NATIONAL CRITICAL INFRASTRUCTURE PROTECTION
REGIONAL PERSPECTIVE

Belgrade, December 2013

[ФБ]
УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ
UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

NATIONAL CRITICAL INFRASTRUCTURE PROTECTION
REGIONAL PERSPECTIVE

Belgrade, December 2013

Editorial

Zoran Keković, PhD, University of Belgrade – Faculty of Security Studies
Denis Čaleta, PhD, Institute for Corporative Security Studies, Ljubljana
Želimir Kešetović, PhD, University of Belgrade – Faculty of Security Studies
Zoran Jeftić, PhD, University of Belgrade – Faculty of Security Studies

Reviewers

Dr Želimir Kešetović, PhD, University of Belgrade – Faculty of Security Studies
Marina Mitrevska, Ss. PhD, Cyril and Methodius University in Skopje – Faculty of Philosophy
Zoran Jeftić, PhD, University of Belgrade – Faculty of Security Studies
Bojan Zrnić, PhD, Ministry of Defence of the Republic of Serbia

Publisher

University of Belgrade – Faculty of Security Studies
Institute for Corporative Security Studies, Ljubljana

For the Publisher

Radomir Milašinović, PhD, Dean of the Faculty of Security Studies
Denis Čaleta, PhD, Institute for Corporative Security Studies, Ljubljana

Proofreading

Dragoslava Mićović, Academy of Criminalistic and Police Studies, Belgrade

Graphics Design, and Cover Page

Branislav L. Valković, University of Belgrade – Faculty of Security Studies

Print

Čigoja štampa, Belgrade

Edition

200 copies

ISBN 978-86-84069-84-1

Note

The authors opinions expressed in this book do not necessary reflect the views of the institution in which they are employed.

Editors
Zoran KEKOVIĆ, PhD, Denis ČALETA, PhD,
Želimir KEŠETOVIĆ, PhD, Zoran JEFTIĆ, PhD

NATIONAL CRITICAL INFRASTRUCTURE PROTECTION
REGIONAL PERSPECTIVE

УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ
UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

ICS
Institute for Corporative Security Studies

2013

CONTENTS

EDITORIAL 9

SECTION I:
CONTEMPORARY SECURITY THREATS AND CRITICAL INFRASTRUCTURE

Teodora Ivanuša, Matjaž Mulej, Iztok Podbregar, Bojan Rosi
TOWARD REQUSITE HOLISM OF CONTENT
OF THE TERM CRITICAL INFRASTRUCTURE 15

Veerle Pashley, Marc Cools
THE POWER OF CREATIVE THINKING IN SITUATIONS
OF UNCERTAINTIES: THE ALMOST IMPOSSIBLE TASK OF PROTECTING CRITICAL INFRASTRUCTURES 27

Goran Matić, Milan Miljković
CRITICAL INFRASTRUCTURE PROTECTION IN CYBERSPACE 41

Denis Čaleta, Aleš Kotnik
CYBER THREATS AND DILEMMAS
OF CRITICAL INFRASTRUCTURE PROTECTION IN SMALL STATES:
COMPARISON BETWEEN ATTACKS IN GEORGIA AND ESTONIA 51

Goran Mandić, Ozren Džigurski, Mladen Milošević
CRITICAL INFRASTRUCTURE SECURITY
AND SOCIAL NETWORKS AND SOCIAL ENGINEERING 65

Marjan Marjanović, Ivan Nađ
ASSESSMENT OF THREATS TO CRITICAL INFRASTRUCTURE
FACILITIES FROM SERIOUS AND ORGANIZED CRIME 77

Saša Mijalković, Vladimir Cvetković
VULNERABILITY OF CRITICAL INFRASTRUCTURE
BY NATURAL DISASTERS 91

SECTION II:
REGIONAL AND NATIONAL PROTECTIVE POLICY AND OPTIONS

Ernst-Peter Döbbeling

PROGRAMS AND TRENDS
IN CRITICAL INFRASTRUCTURE PROTECTION IN THE EU.....105

Momčilo Milinović, Zoran Jeftić

CHALLENGES OF NATIONAL DEFENCE IN INTERNATIONAL STATE
AND PRIVATE CORPORATIVE MANAGEMENT OF INFRASTRUCTURE PROTECTION 119

Želimir Kešetović, Nenad Putnik, Marko Rakić

POSSIBILITIES OF IMPROVING CRITICAL INFRASTRUCTURE
PROTECTION IN COUNTRIES IN TRANSITION 131

Predrag Marić, Zoran Jeftić, Sanja Žugić

EXPERIENCES IN THE OPERATION OF NEW PROTECTION AND
RESCUE SYSTEM IN SERBIA.....143

Branko Mihaljević, Ivan Toth, Alen Stranjik

IMPACT OF CRITICAL INFRASTRUCTURE OWNERSHIP
ON THE NATIONAL SECURITY OF THE REPUBLIC OF CROATIA.....155

Dragiša Jurišić

CRITICAL INFRASTRUCTURE PROTECTION IN BOSNIA
AND HERZEGOVINA AND ROLE OF THE MILITARY.....167

Marjan Đurovski

NATIONAL PLATFORM OF THE REPUBLIC OF MACEDONIA
FOR REDUCING THE RISKS OF CATASTROPHES EFFICIENCY MECHANISM.....179

Ivana Simović-Hiber

THE ROLE OF THE CRIMINAL LAW
IN PROTECTING INFORMATION SOCIETY 189

Zoran Keković, Sandra Vučić, Radosav Despotović, Nenad Komazec

COMPLIANCE OF EDUCATION PROGRAMS WITH THE NEED OF
PROTECTION NATIONAL CRITICAL INFRASTRUCTURE 201

SECTION III:
RISK AND CRISIS MANAGEMENT APPROACHES

Nasir Hussain

USING GENERAL MORPHOLOGICAL ANALYSIS FOR DEVELOPING SCENARIOS AND STRATEGIES FOR EMERGENCY PREPAREDNESS IN CRITICAL INFRASTRUCTURE PROTECTION 217

Milica Bošković, Violeta Ivković, Nenad Putnik

RISK MANAGEMENT IN PUBLIC-PRIVATE PARTNERSHIP OVER CRITICAL INFRASTRUCTURES 231

Dragan Trivan, Vladimir Radović

CORPORATE SECURITY ROLE IN PROTECTING CRITICAL INFRASTRUCTURE 243

Ivica Đorđević, Zoran Pavlović

CRITICAL INFRASTRUCTURE PROTECTION IN HUMAN SECURITY CONCEPT 255

Ljubinka Katić

EDUCATION AS THE CRITICAL INFRASTRUCTURE PROTECTION FACTOR 267

Vesela Radović, Husam Majeed Hameed

THE IMPORTANCE OF CRITICAL INFRASTRUCTURE DURING DISASTERS: THE GREAT CHALLENGE FOR THE FIRST RESPONDERS 279

Dane Subošić, Dragan Mlađan

MAIN FEATURES OF FIRE FIGHTING INTERVENTIONS CARRIED OUT BY BELGRADE FIRE AND RESCUE BRIGADE 289

SECTION IV:
TECHONOLOGIES RELATED TO CRITICAL INFRASTRUCTURE PROTECTION

Bojan Zrnić, Veljko Petrović, Branko Medan

ASPECTS OF CRITICAL INFRASTRUCTURE PROTECTION IN THE DEFENCE INDUSTRY 303

Dragana Nikolić, Ana Kovačević, Srboljub Stanković

THREAT ASSESSMENT FOR THE DESIGN OF THE EFFECTIVE PROTECTION SYSTEM OF NUCLEAR FACILITIES 315

Dejan Radović, Ivica Radović, Vladimir Jakovljević, Zoran Čvorović, Boban Tomić
IMPLEMENTATION OF GIS TECHNOLOGIES IN THE MANAGEMENT OF NATURAL PROTECTED AREAS: CASE STUDY NP TARA (SERBIA) 337

Dejana Jovanović-Popović, Zoran Keković, Miroljub Milinčić, Dejan Šabić
NANOTECHNOLOGY AND FOOD SAFETY: APPLICATIONS AND EMERGING OPPORTUNITIES 353

Mitar Kovač, Nenad Dimitrijević, Brankica Potkonjak-Lukić
SECURITY ASPECTS OF THE "SOUTH STREAM" AS A CRITICAL INFRASTRUCTURE ELEMENT OF THE REPUBLIC OF SERBIA* 363

Kristina Radojević, Zoran Dragišić
A MODEL OF SECURITY MANAGEMENT SYSTEM FOR TRANSPORTATION SYSTEMS 379

Momir Ostojić, Željko Ivaniš, Vladimir Ajzenhamer
CRITICAL INFRASTRUCTURE IN AIR TRAFFIC MANAGEMENT SYSTEM 391

Ana Juzbašić
INTEGRATED PROTECTION OF CRITICAL TRANSPORTATION INFRASTRUCTURES: AIRPORT EXAMPLE 403

Ljubodrag Ristić, Bojana Miljković-Katić
BORROWING FOR CONSTRUCTION OF RAILWAYS AND PROTECTION OF CRITICAL INFRASTRUCTURES IN THE KINGDOM OF SERBIA (1881–1895) 415

EDITORIAL

The strenghtening of national capacity and regional cooperation in relation to the critical infrastructure protection is a common goal of Southeast European countries according to their national security strategies and contemporary security threats to the critical infrastructure protection. This objective is in line with the European perspective of the countries of Southeast Europe, as well as the Critical Infrastructure Protection Programme of the European Union.

The dependence of modern society on the technological development and complex systems is in direct proportion to the threats to these systems. Natural and technological threats, terrorism, crime and other dangers face individual countries with challenges and dilemmas in defining and protecting the critical infrastructure, the disruption of which can cause serious disturbances in the functioning of both economy and society. New risks and threats to the critical infrastructure - social engineering and cyber threats have become reality. On the other hand new technologies (information technology, nanotechnology, nuclear technology, GM etc.) enhance the capabilities of facing those threats, but can also be considered as threats per se. The tremendous development of information and communication technology, revive the question of using social network as a part of the solution, but a part of the problem, too. The application of new tools in the protection of the CI from unpredictable threats (morphological analysis, automatization of processes) is necessary.

The challenges and policies of the national critical infrastructure whose boundaries are rather vague can be considered as a network of interrelationships, as follows: public sector - private sector; the state – the state; the state - the group of states.

The relationship between the public and private sector is being observed from the national and international perspective. A key challenge arises from the relationship between the public and private sectors and protecting the segments of critical infrastructure owned by the private sector. From economic point of view , there is no will to invest in an adequate infrastructure protection without the financial support from the state. The problem of harmonizing the daily operational activities and corporate security policies on the one hand, and the defense and security policy and legislation of the states on the other hand is even more complicated due to the fact that a large number of critical infrastructures are managed by multinational corporations that often operate beyond national protection policy and legal constraints. Protection is also compromised due to the race for competitive position in the economic, technological and financial environment, which has increased the flexibility in the free market of goods and services and makes critical infrastructure even more vulnerable.

The complexity of public-private partnerships within the critical infrastructure protection is especially multiplicate on the level of international and regional cooperation, taking into account the different national, political and security interests of individual countries, restrictions of financial resources and constraints influenced by the legislation. With the exeption of nuclear energy sector which is well-regulated both on national and international level, the issue of ownership and public-private partnership is expected to be solved by the delineation of responsibilities in terms of safety and security and the protection of public interest.

The relationship between a state and a group of states reflects through an integrated approach based on the need to adopt common policies and international standards for the critical infrastructure protection, and the fact that all Southeast European countries are

not members of the EU, regardless of the common European perspective. The EU Directive on critical infrastructure protection is not applied comprehensively in the national critical infrastructure protection as it does not cover certain areas but knowledge and protection tools and processes can be transferred and implemented among the sectors.

Due to the aforementioned, this book aims to open discussion between experts in different fields. In addition to knowledge in the field of security, economy, legal and organizational matters, engineering and other finding are also presented, including their imlplementation into practise (Bologna system has a solution, but the question is how to implement it).

The authors of the book try to make a step forward in order to find solutions for the needs and capabilities of critical infrastructure protection from different disciplinary theoretical and professional points of view.

From the scientific point of view: Differences in defining the critical infrastructure have negative effects that affect the integrity of the protection system. The differences originate primarily from the lack of a unique definition of terrorism and other criminal threats to infrastructure, which interferres with effective communication in information exchange. In addition, the differences in the perception of the importance of infrastructure are apparent among the certain stakeholders, including the differences between the business community and government authorities. Two extremes are presented: underestimating the importance of critical infrastructure or overestimating the criticality of certain critical infrastructure sectors in order to gain a monopoly in the critical infrastructure protection. It is necessary to gain the theoretical and scientific consensus on the definition of critical infrastructure, with the application of two main approaches: critical infrastructure is determined by the symbolic importance that it has for the community or system, and on the basis of structural position that it has within the overall infrastructure.

From the technical point of view: articles are focused on considering the problems of critical infrastructures protection from different perspectives, including risk management, business continuity management and crisis management. These perspectives emphasize the importance of protecting those segments of the critical infrastructure that enable the exchange of security information. Special attention is paid to the development of specific risk management approaches in certain critical infrastructure sectors, especially in the energy sector end nuclear energy sector, including the monitoring mechanisms of organizations and agencies that manage the critical infrastructure protection.

Articles indicate not only the importance of the exchange of ideas and best practices between the countries in the Region in the area of public-private partnership in the management of critical infrastructure, but also interoperability between human and technical resources. A comprehensive risk management approach based on national and international experiences is required, but there are no universally applicable solutions.

From the legal point of view: Since the modern society faces an expansion of cyber attacks on the critical infrastructure, and those attacks are becoming more sophisticated and more dangerous, the legal aspects of critical infrastructure protection are primarily focused on the protection of information technology from cyber attacks. The grounds for the escalation of these attacks is increased by the standardized protocols to be applied in the field of critical infrastructure protection, which make information systems more vulnerable and susceptible to the mentioned threats like never before.

From the economic point of view: Critical Infrastructure protection is considered both from the aspect of business operations and processes and economic feasibility of investment in a certain field.

From the aspect of social responsibility: Attacks on the critical infrastructure can have significant consequences for public health. Therefore, the application of appropriate standards of social responsibility within the business community in conjuction with the government support in terms of investment in security is required to provide minimum public interest in the critical infrastructure protection.

From the defence policy point of view: In order to perfom the third mission of the army, the authors consider the concept of domestic legislation and need to customize the contemporary approach based on the principle of OSA (open structure architecture). This concept involves the organizational structure of military forces as security forces.

The scientific contribution of the book reflects in highlighting regional cooperation between the experts from the academic and business environment, expanding the network of knowledge and experience in the field of risk and crisis management related to the critical infrastructure. We hope that this would contribute to facilitating the transfer and application of scientific knowledge in the practice of critical infrastructure protection. It should be added that higher education programs need to be aligned with the requirements of the practice, which will ensure that academic society provides an appropriate education to professionals who will monitor the complex requirements of the security environment based on the results of scientific research.

A specific goal of the book is the theoretical con¬ceptualization of the topics covered, and professional discussion in the field of critical in¬frastructure protection, with the focus on the exchange of experience not only from the Southeast Europe, but also from other European and non-European countries. With this in mind, the International Scientific Book is designed in a manner which allows authors from more experienced countries to give their perspec¬tives first, to be followed by the experience of representatives from the Southeast European countries.

The main focus areas of the book are: 1) Contemporary Security Threats and Critical Infrastructure, 2) Regional and National Protective Policy and Options, 3) Risk and Crisis Man-agement approaches, and 4) Technologies related to Critical Infrastructure Protection.

Belgrade, December 2013.

Zoran KEKOVIĆ, PhD, Full Prof.
Denis ČALETA, PhD, Assist. Prof.
Želimir KEŠETOVIĆ, PhD, Full Prof.
Zoran JEFTIĆ, PhD, Assist. Prof.

SECTION I

CONTEMPORARY SECURITY THREATS AND CRITICAL INFRASTRUCTURE

UDC 726.9:75.041.5
ID 176374796

Teodora Ivanuša
University of Maribor, Faculty of Criminal Justice and Security
teodora.ivanusa@fvv.uni-mb.si

Matjaž Mulej
University of Maribor, Faculty of Economics and Business,
mulej@uni-mb.si

Iztok Podbregar
University of Maribor, Faculty of Criminal Justice and Security
iztok.podbregar@fvv.uni-mb.si

Bojan Rosi
University of Maribor, Faculty of Logistic
bojan.rosi@fl.uni-mb.si

TOWARD REQUSITE HOLISM OF CONTENT OF THE TERM CRITICAL INFRASTRUCTURE

Abstract: The concept of critical infrastructures is not holistic enough to cover all potential threats by safety measures, as they are traditionally foreseen. The executive summary of EU Chemical Biological Radiological Nuclear Explosive Ordnance Disposal Doctrine (CBRN EOD) for Multinational Operations includes in its enhanced points "to protect personnel, materiel, infrastructures and environment and to maintain or restore operational capabilities..." The CBRN EOD risk potential (as a rule large danger areas with the possibility of extremely negative effects on the mission, population, infrastructure and environment due to contamination) causes the CBRN EOD tasks to never be autonomous/isolated, but interdependent tasks; the allocation of responsibilities is a necessary applied national routine in which the essential imperative is to avoid individual/one-sided unauthorized action! It is complex enough to require systemic thinking, which enhances interdisciplinary creative co-operation, like the Dialectical Systems Theory does more than the others in Encyclopedia (François, 2004) in order to attain the requisite holism and hence success rather than failure. In the light of nowadays threats (i.e., CBRN Devices) that differ rapidly and nearly on a daily basis, the term critical infrastructure is not requisitely holistic. The critical infrastructures are more or less determined, providing mutual and essential course of action for the command and control and the execution of multinational CBRN EOD operations. However, we fear ambiguity of the definition of the critical infrastructures due to natural or intentional outbreak of the highly contagious diseases. Proper planning often prevents poor performance; therefore, threat analysis, high readiness, tasking, coordination and prioritization remain the major factors, when immediate strategic definition of a critical structure must be appointed, i.e. activities must be done requisitely holistically. This is why the dialectical systemic thinking is crucial.

Key words: *critical infrastructure, strategic definition, CBRN devices, dialectical systemic thinking, requisite holism*

1. INTRODUCTION

There is no doubt that nuclear power plant and other common critical infrastructures are issues of the highest national strategic framework. For instance, the Republic of Slovenia as an EU (European Union) and NATO (North Atlantic Treaty Organization) member possesses its nuclear power plant. This is one of the commonly recognized critical infrastructures. In addition, Slovenia is surrounded with 50 other power plants with 109 reactors; 32 of these are within a radius of 500 km from Slovenia (Podbregar, 2005a; Podbregar, 2003). Plead for constantly existing nuclear threat is anticipated and represents one of the central strategic points. Are they worked on with requisite holism of human monitoring, perception, thinking, concluding, decision making, and action (Mulej et al., 2008; Mulej, Kajzer, 1998, and earlier, since 1974)? Total holism is impossible; limitation to a single profession/viewpoint makes holism fictitious causing oversights and hence dangers of failures:

←----------→

Fictitious holism (inside a single viewpoint and special profession causing oversights of attributes visible from other aspects)	Requisite holism (a dialectical system, i.e. synergetic network, of all and only essential interdependent viewpoints/professions/sciences/experiences)	Total = real holism (a system, i.e. synergetic network, of totally all viewpoints)

Figure 1: The selected level of holism of consideration of the selected topic between the fictitious, requisite, and total holism

Critical infrastructure is well defined – from the authors' selected viewpoints (NATO, EDA, and EU). What about other aspects? Alliance's (NATO) critical energy is assumed to be delivered from the Alliance's energy supply structure based on four forms of energy. All threats are focused on energy security, which is a serious tasking complexity (Podbregar, 2000a; Podbregar, 1999; Podbregar, 2000b). The facilities, which are employed in the production, transfer means or storage of and processing of energy, would have a debilitating impact on Allies security and/or economy, if incapacitated or destroyed. The probability of conventional or asymmetric attacks that could lead to indirect or even deliberate disruption of critical energy flows with serious impact over Allied security and economic stability includes any risk of attack or disruption by hostile forces or by terrorists (Podbregar, 2004; Podbregar, 2005b); again inside the selected viewpoints.

NATO might add defining other viewpoints to safeguard the security interests of the Allies and assist national and international efforts. It is of immense importance that EDA (European Defense Agency) and its CBRN EOD Project Team offers plead able Doctrine (EDA CBRN, 2006) focused on the operational level providing a feasible approach on the operational requirements. In addition, giving the nature, it is important that EU Member States verify their coherence with similar NATO concepts to ensure full/requisite compatibility. It seems that national, regional and international interoperability and "know how" are covered, but again inside the selected viewpoints. Are all essential viewpoints and their interactions and synergies covered? Is each and every of them prepared requisitely holistically?

The term critical infrastructure and consecutive strategic documents cover four forms of energy. Vandals, saboteurs, criminals, physical attacks, natural disasters, and misfortune

(human error) are therefore manageable – but are they so one-sidedly, with requisite holism, or even perfectly? The mitigation options are well known: Intelligence fusion and sharing; Projecting stability; Advanced EU – NATO and regional cooperation; Support to the protection of national critical infrastructures; Surveillance and protection of ungoverned spaces (i.e. International waters): from "point" defense to "area" defense; Counterterrorism; Consequence management; Military cooperation. Are they networked in totally or requisitely holistic synergies, too? Is each and every of them prepared requisitely holistically? Requisite variety differs from requisite holism, which addresses the level of holism of monitoring, perception, thinking, emotional and spiritual life, decision making, and action; success depends on the requisite holism, if too small it fails to cover everything essential, if too complete it takes too much time and too many resources; there is mathematical way to determine it, but feed-forward judgment, an interdisciplinary creative cooperation makes the basis for it.

The executive summary of the EU Chemical Biological Radiological Nuclear Explosive Ordnance Disposal Doctrine (CBRN EOD) for Multinational Operations includes the enhanced points "to protect personnel, materiel, infrastructures and environment and to maintain or restore operational capabilities..." (EDA CBRN, 2006). Are they networked in totally or requisitely holistic synergies, too? Is each and every of them prepared requisitely holistically?

NATO forces routinely operate as expeditionary forces engaged in Allied joint operations, which occur both within and outside of the NATO area and responsibility. The operational environment may have no discernable "front lines" or "rear area" and an adversary may be expected to target Allied vulnerabilities anywhere with a wide range of capabilities. Security, one of the principles of operations, and protection, a key component of security, should assure, but it cannot without requisite holism and even higher importance in such environments. Force Protection (FP) is therefore defined as: "Measures and means to minimize the vulnerability of personnel, facilities, materiel, operations and activities from threats and hazards in order to preserve freedom of action and operational effectiveness thereby contributing to mission success." (NATO Standardization Agency, 2007). Thus, the fact is that NATO has admitted that forces are vulnerable throughout the deployment, reception, staging, and onward movement, execution and redeployment phases of an operation – especially when infrastructure is not yet in place and information on the situation is incomplete (Podbregar, 1999). Are they networked in totally or requisitely holistic synergies, too? Is each and every of them prepared requisitely holistically?

So, if kinetic threats, which are physical in nature and may require either proactive or reactive military actions, are eliminated on time, 'our people' are no longer threatened and at least one of four forms of energy will remain an intact critical infrastructure. Additional neutralization of possible non-kinetic threats, e.g. cyber-attack, will accomplish the preventive actions in preserving strategic infrastructures tackling the four forms of energy. Are these actions networked in totally or requisitely holistic synergies, too? Is each and every of them prepared requisitely holistically?

If answers about requisite holism are questionable, the Alliance and its forces remain vulnerable to a wide variety of hazards and threats. Hazards include occupational hazards, such as road traffic accidents, fire, and exposure to environmental hazards, such as (contagious or noncontiguous) disease and Toxic Industrial Materials (TIM). A threat may be

described as a state's/coalition's perception that is to some degree of danger based on the assessed capabilities, intentions, and actions of another state/coalition or group (NATO Standardization Agency, 2007). Such threats may exist even in benign environments, such as unit's home-station or base. At best, an Improvised Explosive Device (IED) environment – or an environment that may involve Chemical, Biological, Radiological or Nuclear (CBRN) agents – may deter or delay the timely deployment of some national forces and undermine Alliance resolve. At worst, it may result in significant casualties and severely hamper or thwart mission accomplishment (NATO Standardization Agency, 2007).

Survivability is therefore a principal consideration in strategic planning and decision-making – with implications that extend well beyond the military mission and into issues such as public support, political cohesion, and other areas. It can hardly be attained without requisite holism of single actions and their synergies. FP is based on risk management, not risk elimination. Casualties, deliberate or accidental, are a reality of military operations and the desire to avoid them totally may impact adversely the achievement of the mission. Although it is not possible to protect every asset against every threat all the time, the assets previously identified as "critical to the mission" must be protected. As a part of FP, a comprehensive risk assessment process is essential to guide risk management decision-making prioritization (Podbregar, 2003; Podbregar, 2000a; Podbregar, 2000b). Are all of them networked in totally or requisitely holistic synergies, too? Is each and every of them prepared requisitely holistically?

From the scientific point of view and simultaneously using a pure common sense the serious question arises: "How vulnerable are we actually?" while NATO considered its vulnerability and pointed out such statement in its highly weighed strategic documents... Are they requisitely holistic?

If they are not so, adversaries may be expected to capitalize on perceived Allied weakness and vulnerabilities, giving rise to the need for a comprehensive and resilient strategy for the protection of forces. FP is essential to operations, and therefore a clear responsibility of command is to ensure that all military units are able to defend and to protect themselves appropriately, i.e. requisitely holistically, against prevailing threats throughout the range of military operations. Hence, NATO's operational needs and the increased global threat of terrorism prompted an urgent review (Podbregar, 2003; Podbregar, 2000a; Podbregar, 1999).

It seems that national, regional and international interoperability and "know how" are covered, but is this true without requisite holism, including resilience, both of people and of the organization to new impacts, including the future ones?

Restitution to solidly defined critical infrastructure, "Four forms of energy", has grounded reason. We will try to offer some prudent reasons where the concept of "Four forms of energy" as an ultimate critical infrastructure has its weak points and hence the scenario can be diametrically different from the general expectation. We will also tackle terrorism as the number one phenomenon threatening the global security arena. Terrorism has already been scientifically described and defined to a certain level and any additional "invention" can diminish the major message we would like to launch to the wider audience (Podbregar, 2005a; Podbregar, 2004; Podbregar, 2005b; Podbregar, Slapar, 2007; Podbregar, 2006). But has terrorism been defined and worked on scientifically and strategically, e.g. as an extreme protest against the privileged part of the current humans (Bourg, 2007)?

In the light of nowadays threats (i.e. CBRN Devices) that differ rapidly and nearly on a daily basis, the term critical infrastructure calls for a detailed reconsideration. The critical infrastructures are more or less determined, representing mutual and essential principles for the command and control and the execution of multinational CBRN EOD operations. However, we see ambiguity of the current definition of the critical infrastructures in, for e.g. its relation to natural or intentional outbreak of the highly contagious diseases. Therefore, the major course of action declares: "It is about an ambition to use both, the infrastructure and human resources in order to achieve the highest level of security possible" (Meško, 2004; Meško, Lobnikar, 2005). This aim can hardly be attained without requisite holism.

2 SOME FACTORS INFLUENCING STRATEGIC AMBIGUITY OF THE TERM CRITICAL INFRASTRUCTURE

Applying the term "know-how" into the "grey area" of humankind's rationality and emotion has an infinitive possibility to become a complete absurd, without the requisite holism, in the strategic definition of the critical infrastructure. Despite such serious possibility of scientific disqualification of the present paper, we will remain in the "grey area" trying to provide some points of departure starting with "scientific achievements, which may belong to victims of a too one-sided approach to transforming novelties to innovations, so far." Authors, Mulej et al (Mulej et al., 2006; Mulej et al., 2003; Mulej et al., 2004; Potočan, Mulej, 2006; Mulej et al., 2008; Mulej, Kajzer, 1998) brief what the dialectical system thinking and requisite holism actually is based on:

- Interdependences, Relations, Openness, Interconnectedness, Dialectical System; rather than one-sidedness;
- Complexity (& Complicatedness: Descartes this is a correct definition and in its essence it leaves interactions of part and emerging synergies aside, which requires complexity to be added for requisite holism with no crucial oversights to be attained) ; rather than simplicity or complicatedness alone with no synergies;
- Attractors; rather than oversight of connecting forces causing emergent process leading to synergies;
- Emergence; rather than expectation of no or linear changes with no new attributes showing up;
- Synergy, System, Synthesis; rather than sums of old attributes of the feature under consideration;
- Whole, Holism, Big Picture, Holon; rather than parts with no attributes of the whole which do not exist in parts as isolated phenomena alone;
- Networking, Interaction, Interplay; rather than isolated analysis per isolated parts alone.

Thus, the dialectical system approach is obviously supposed to enable people to think along the mentioned notions rather than to oversimplify and make dangerous oversights and resulting mistakes, including World Wars, and World Economic Crises, the climate change problem, etc., but also a number of mistakes with less broad consequences (Mulej et al., 2006). However, "law of requisite holism describes the natural fact, that humans do not have capacity to be totally holistic" (Mulej, Kajzer, 1998). "On the other extreme, people hardly can do a good job, if they limit themselves to a single viewpoint, e.g. of a single profession with no co-operation with people who see the same processes differently. The right way, also in this case, is the middle way, but people must take responsibility

for choosing a dialectical (i.e. interdependence-based) system of viewpoints of one kind rather than of another kind"; Figure 1 (Mulej et al., 2008). There is no simple mathematical formula applicable once for ever.

What on earth have the alleged scientific facts of authors Mulej et al to do with the ambiguity of the term critical infrastructure? Almost everything!

The currently solid definition of critical infrastructure, "Four forms of energy", calls for re-consideration, especially when bio-agents (BA) dictate a new, requisitely holistic, style of thinking. Who will be the major target of potential biological warfare? The perfidious way of biological attack is simple, but the reality of such kind of attack is far more complex than most humans are ready to face. It is not just about an intentional outbreak of the highly contagious disease. Humans are highly vulnerable to a non-hostile natural outbreak. World Health Organization (WHO) finally admitted that antigenic shift of H5N1 had happened and the human-to-human transmission has engulfed the humankind (Reuters Health Information, 2007). The "minority report" exceeded the doorstep where naive civilian population has been hypocritically misled that possible future pandemic is just an illusion, or worse, a delusional theory of some isolated scientists (Podbregar, Ivanuša, 2007). The latter persons lacked requisite holism.

A case:

In 2007 the Swine Plague has engulfed the Republic of Croatia. The major outbreak of the disease affected the geographic areas extremely close to the Slovenian national border. The quick and requisitely holistic communication has failed: Slovenia was exposed to a threat very close to a major disaster in which no single animal could survive: stamping out method is the only acceptable strategy in the case of such endemic. So, the national border with the Republic of Croatia became a critical infrastructure of a highest national priority. In addition, critical factors consist of each Slovenian veterinarian who crossed the border then (prior to Croatia's official announcement of the outbreak of Swine Plague) and offered the vet-medical services to Croatian breeders; and vice versa (which is possible and a quite common illegal act in border areas), each single swine that had been in contact with any particular veterinarian in the Slovenian husbandry, any civilian person, any civilian cloth, any civilian footwear, any civilian vehicle that crossed the affected area, any transport in both ways, the entire nutrition chain, export and import et cetera was a critical factor. Was Slovenia "lucky"? Fortunately no case of Swine Plague has been officially confirmed in Slovenia yet. Perhaps Slovenia was prepared on a requisitely holistic level, or was just lucky.

Another case:

Slovenia faced (in 2007) the quite unexpected natural outbreak of Q-fever, a highly communicable disease, where animal-to-human transmission is a well-defined routine. This is just a foretaste of what Avian Influenza, Swine Plague, Q-Fever, Foot and Mouth Disease and other highly contagious diseases (bio agents) can and will demonstrate to the humanity of the 21st century. Soft - "Non Military targets" are nowadays target area of interest to adversary human beings and their organizations.

Therefore, the hypothetically doubtless and solid definition of critical infrastructure: "Four forms of energy" has another "side of the coin", or even several of them. If some (intentionally anonymous) non-state actors provoke the intentional outbreak of the highly

contagious disease to humankind, the "Four forms of energy" will remain perfectly intact. Covert release of BA with delayed effects will turn upside down each existing strategic document and the solid definition of "Four forms of energy" as a critical infrastructure: each course of actions will alter. The public will not notice this type of biological release until people start to become ill. A good awareness of such dangerous position among civilian population will end in panic, which cannot be perfectly predictable and in the vast majority of cases the arriving chaos will govern each security measures taken. Quite a broadly conceived interdisciplinary creative cooperation of quite many crucial professions might offer a better chance for requisite holism to be attained than the military or any other profession alone: it cannot practice dialectical systems thinking alone, like nobody can.

Civilians are those human resources who govern the solidly defined critical infrastructures: "Four forms of energy." Destroying humankind with for e.g. potential biological agent with delayed effects will protect the currently defined critical infrastructure that is vital to each adversary having its own reasons and strategic appetite to take it over. Mass casualties, for which biological weapons are potentially made, are the main focus. No hostile track has the strategic concept, which will allow the end of "Four forms of energy". Such a lack of requisite holism might cause tragic consequences.

FP offers a safety zone on a certain level of course. The members of the Security/Armed Forces are well trained and equipped to protect themselves (Podbregar, 1999). However, they are only human beings. Their final task in the case of biological warfare might become a plain straggle to survive. And they can become ill as well; they can be part of the mass casualties as well. Empty space of the solidly defined "Four forms of energy" can be the final outcome of the potential natural or intentional outbreak of the highly contagious disease of any inhabitant of the world.

That is why we dare to move the term critical infrastructure from nuclear plant, or as defined: "Four forms of energy", to human beings-animals-national borders-general transport, etc. if they do not practice the requisite holism. None of them exists and acts in isolation from each other; they are more interdependent than they look like at first glance. Their dialectical (i.e. interdependence-based) relations must stop being victims of oversights of specialists, who are deep inside their own specialties/viewpoints, but poorly capable of interdisciplinary co-operation, and hence do not attain the requisite holism in such complex processes and situations as tackled here.

3 CONCLUSIONS CONCERNING REQUISITE HOLISM OF THINKING, DECISION-MAKING, AND ACTION

Biological agents are an "invisible front" (Vauhnik, 1941) seriously denying the currently recognized critical infrastructure. To be precise, we agree: "Four forms of energy" make a critical infrastructure. But this definition is somehow too decisive and one-sided rather than requisitely holistic. The dialectical systemic style of thinking was offered just to remind or simply add rather than deny the highly strategic definition of critical infrastructure. The authorities should make it more/requisitely holistic. Throughout history, for e.g. infection diseases contracted naturally have had a significant impact on military operations and human lives. The effects of disease introduced to native populations were clearly demonstrated by for e.g. the spread of smallpox in the Americas after the arrival

of the Europeans and illustrated the potential impact of the deliberate use of BA (NATO Standardization Agency, 2005).

The intentional dissemination of disease(s) adds a new dimension to threats that are posed by BA traditionally transmitted only by natural routes. The global security arena is facing already the natural outbreak of virus H5N1, which crossed and it keeps crossing the national borders silently, identically as electricity silently crosses the national borders giving the vital source of energy the absence of which can inflict a crisis of immense extension...

Proper, i.e. requisitely holistic planning, often prevents poor performance, therefore, threat analysis, high readiness, tasking, coordination and prioritization remain the major factors with immediate strategic definition of a critical structure that must be undertaken, and happen in a requisitely holistic manner. In practice, this means planning with requisite holism based on inter-disciplinary creative co-operation. Which level of holism is requisite in the concrete case, must be decided and responsibility for decisions must be accepted; there is no mathematical solution once for ever. And every planning, if it is proper, has to do with some innovation, at least, add to the established routine; the current life is no longer unchangeable or simple like in old times (Mulej et al., 2008). The content of a term is also novelty aimed at becoming innovation, i.e. beneficial to its users in their practice. (Mulej et al., 2008)

"We just tried to demonstrate that holism of thinking, decision-making, and action is very necessary. Also, we would like to show how much more success one could yield in the innovation effort, if one applied more system thinking. The problem lies in mentality very much - in humans' thinking and worldview as well as other values and other emotions." (Mulej et al., 2008).

"Take a look at experience around you and discover (again): Success has always resulted from absence of oversights with crucial impact. And failure has always resulted from crucial oversights, be it in business, scientific experiments, education, medical care, environmental care, invention-to-innovation processes, etc., or wars, all the way to World Wars of 20th century, and all other wars and crises." (Mulej et al., 2008). As a case of reminder of requisite holism about innovation see Figure 2 (based on Ženko, et al., 2008; and Mulej et al., 2008, renewed).

		Phases of users' decision making about a novelty				
VIEWPOINTS TO BE CONSIDERED		1 Awareness	2 Persuasion	3 Decision	4 Applicati-on	5 Reconfir-mation
Novelty customers (potential)	Customers – innovators					
	Early customers					
	Early majority					
	Late majority					
	Laggards					

Potential customers' absorption capacity for the introduced novelty – to-be innovation						
Requisite holism of potential suppliers/ authors of novelty – to-be innovation						
Requisite holism of potential customers of novelty – to-be innovation						
Requisite holism of pressure of market, government and bosses concerning novelty – to-be innovation						
Requisite holism of information system concerning novelty – to-be innovation for suppliers and customers to know enough						
Systemic quality of novelty – to-be innovation (based on requisitely perfect products, processes, leadership and commitment, linked in a synergy by organization, and expressed in the system (= network) price, quality, range, uniqueness, and environmental care)						
Requisitely holistic vision, mission, policy, strategy, tactic, operation, and control of the entire process with suppliers (and users)						
Opinion leaders						
Attributes of novelty	Relative advantage					
Compatibility						
Complexity						
Testability						
Visibility						
Communication channels	Public					
Interpersonal						
Nature of the culture of customers						
Decision type about novelty	Optional					
Group						
Authority						

Consequen-ces of novelty	Desired					
Indirect	Undesired					
Direct						
Anticipated						
Unanticipated						

Legend: the darker the area, more change agents' effort is needed

Figure 2: Matrix of Essential Attributes of Diffusion Process of a Novelty Supposed to become Innovation, from the Viewpoint of Change Agents

REFERENCES

1. Podbregar, I. (2005). Oblikovanje evropske strategije kolektivne varnosti. In: Lobnikar, B. (ed.). 6th Slovenian days of Security Studies. Bled, June, 2.-4. 2005. *Conference Proceedings,* pp. 1-6. Faculty of Criminal Justice and Security, Ljubljana, Slovenia. SI -ID 1060842]
2. Podbregar, I. (2003). Organisational aspect of common security in European Union. In: Florjančič, J. (ed.). 22th International Scientific Conference of Management and Organisational Development. Portorož, March, 26.-28. 2003. *Management and organisation development : collection of papers from international scientific conference on development of organizational sciences,* pp. 61-69. Moderna organizacija, Kranj, Slovenia. SI-ID 3823123]
3. Podbregar, I. (2000). Selection model for participants in peacekeeping operations. In: Jaškova, M. (ed.). ECON '99 : Proceedings Book, selected research papers, Vol. 6, No. 1, pp. 120-124. Technical University, Faculty of Economics, Ostrava, Slovakia. SI-ID 2751507]
4. Podbregar, I. (1999). Vojske prihodnosti. Vojstvo, No. 5, pp. 105-116. SI-ID 2518803]
5. Podbregar, I. (2000). Vloga oboroženih sil danes, jutri. Defensor, pp. 1-67. Defensor, Ljubljana, Slovenia. ISBN 961-6177-04-4.
6. Podbregar, I. (2004). Vloga obveščevalnih služb v boju proti mednarodnemu terorizmu. In: Lobnikar, B. (ed.). Conference of Security Studies, *Conference Proceedings,* pp. 30-34. Faculty of Criminal Justice and Security, Ljubljana, Slovenia. SI-ID 898794]
7. Podbregar, I. (2005). Metode delovanja obveščevalno-varnostnih sistemov v totalitarnem režimu : pregledni znanstveni prispevek na primeru SFRJ. *Slovenian Intelligence and Security Agency*, pp. 1-28. . Slovenian Intelligence and Security Agency, Ljubljana, Slovenia. ISBN 961-91646-0-1.
8. EDA CBRN EOD project Team. (2006). EU Chemical Biological Nuclear Exsplosives Ordnance Disposal Doctrine for Multinational Operation. EU, Brussels, Belgium.
9. NATO Standardization Agency. (2007). Allied Joint Doctrine for Force Protection: AJP-3.14. Third study draft. (2006). NSA, Brussles, Belgium.

10. Podbregar, I. Slapar, M. (2007). Razsežnosti gospodarskega vohunstva v 21. stoletju : primer gospodarskega vohunstva s pomočjo trojanskega konja. In: Lobnikar, B. (ed..) 8th Slovenian days of Security Studies. Bled, May, June, 30.-1. 2007. *Conference Proceedings,* pp. 1-6. Faculty of Criminal Justice and Security, Ljubljana, Slovenia. SI-ID 2750586]
11. Podbregar, I. (2006). Some patterns of industrial espionage. *Varstvoslovje*, Vol. 8, No.. 3/4, pp. 323-331. SI-ID 1324778]
12. Meško, G. (2004). Partnersko zagotavljanje varnosti v lokalni skupnosti- želje, ideali, ovire. *Rev Krim. Kriminol,* Vol. 55, No. 3. pp. 258-265.
13. Meško, G., Lobnikar, B. (2005). The contribution of local safety councils in crime prevention and provision of safety. *Policing*, Vol. 28, No. 2, pp. 353-373.
14. Mulej, M., Potočan, V., Ženko, Z. Ways to make the Goedel's theorem more known to people. (2006). University of Maribor, *Faculty of Economics and Business*. Maribor, Slovenia.
15. Mulej, M., Ženko, Z., Knez-Riedl, J., Potočan, V. (2003). Upravljanje - kdaj je razmišljanje o njem in v njem sistemsko/celovito. *Organizacija,* Vol. 36, No. 7, pp. 443-445.
16. Mulej, M., Potočan, V., Ženko, Z., Kajzer, S., Uršič, D., Knez-Riedl, J, Lynn, M., Ovsenik, J. (2004). How to restore Bertalanffian system thinking. (2004). *Kybernetes,* Vol. 1, No.33, pp. 48-61.
17. Potočan, V., Mulej, M. (2006). Enterprise competitiveness and ethics of sustainable development. In: Kickstarting small island enterprise competitiveness. The University of the West Indies at Cave Hill. *Conference Proceedings,* pp. 299-314.
18. Mulej, M., Fatur, P. Knez-Riedl, J., Kokol, A., Mulej, N., Potočan, V., Škafar, B., Ženko, Z. (2008). Invencijsko-inovacijski management z uporabo dialektične teorije sistemov (podlaga za uresničitev ciljev Evropske unije glede inoviranja). Korona plus d.o.o, Inštitut za inovativnost in tehnologijo, Ljubljana, Slovenia, 285 pages (on CD). In Slovenian.
19. Mulej, M., Kajzer, S. (1998). Ethics of interdependence and the law of requisite holism. In: Rebernik, M., Mulej, M. (eds). *STIQE '98*. ISRUM et al. Maribor, Slovenia.
20. Podbregar, I., Ivanuša, T. (2007). The threat of pandemic is real if not inevitable – Who will protect the Security/Armed Forces in the case of Pandemic. In: TIEMS World Conference, Trogir. *Conference Proceedings,* p.p. 29-36.
21. Vauhnik., V. (1941). Nevidna fronta. *Knjižnica Novo mesto.* Novo mesto, Slovenia.
22. NATO Standardization Agency. (2005). NATO Handbook on the Medical Aspects of NBC Defensive Operations (Biological): AmedP6(C) Vol II. NSA, Brussles, Belgium.
23. WHO Confirms Human-To-Human Bird Flu Case Thursday a single case of human-to-human transmission of the H5N1 avian influenza virus in a family in Pakistan, but said there was no apparent risk of ... News, Reuters Health Information, December 2007.
24. François, Ch., ed. (2004): *International Encyclopedia of Systems and Cybernetics. 2nd Ed.* Saur, Munich
25. Bourg, D. (2007), interviewed by Y. Sciama: Special Report Climate Change – Toward a Planet – wide Ethic. *Research*eu*, No 52, June, 16-17

26. Ženko, Z., Mulej, M., Potočan, V., Rosi, B., Mlakar, T. (2008) A Model of Making Theory as Invention to Become an Innovation. In: Mulej, M., Rebernik, M., Bradač, B., editors, *The 9th International conference STIQE on linking Systems Thinking, Innovation, Quality, Entrepreneurship, and Environmental Care*. University of Maribor, Faculty of Economics and Business, Institute of Entrepreneurship and Small Business Management, Maribor, and SDSR Slovenia Systems Research Society, Maribor

UDC 726.9:75.041.5
ID 176374796

Veerle Pashley
Free University of Brussels
veerle.pashley@vub.ac.be

Marc Cools
Free University of Brussels and Ghent University
marc.cools@vub.ac.be

THE POWER OF CREATIVE THINKING IN SITUATIONS OF UNCERTAINTIES: THE ALMOST IMPOSSIBLE TASK OF PROTECTING CRITICAL INFRASTRUCTURES

'A man who discovers his pants are on fire tends to have very little time to worry about somebody else's box of matches'

(Dexter in Jeff Lindsay, 2005:75)

Abstract: Writing an article on critical infrastructure protection is quite challenging. Scientifically speaking, we ascertain a serious lack of research. A possible explanation could be the fact that in studying critical infrastructure protection one must be able to integrate a multidisciplinary scope. The changing landscape of security (Crawford, 2012) and prevention requires a scientific viewpoint that implements segments coming from several disciplines, i.e. economy, technology, governance, law, sociology and criminology. Evidently, this means a challenge for researchers. Taking these transitions into account, this paper aims at better understanding of critical infrastructure protection. First, we will discuss the conceptualisation of the concepts 'infrastructures', 'critical' and 'protection'. Each word entails a different connotation. We will also focus on the European dimension. Considering the fact that a clarifying definition is currently difficult to realise, we will explore the underlying characteristics and give ideas for new directions. This paper will also reflect on the role of intelligence and private security. Last, we will present criminological reflections regarding the changing landscape of security and its effect on the protection of critical infrastructures. The recent focus on resilience gives an interesting alternative for the encountered challenges.

Key words: *critical infrastructure protection, resilience, intelligence, private security, disruptive events*

1. INTRODUCTION: CRITICAL INFRASTRUCTURE PROTECTION AND THE UNDERLYING CHALLENGES

The protection of critical infrastructures, such as water, energy and telecommunications, is of the utmost importance. If these assets are at risk or destroyed, it will have an impact on the economy, psychology and pride of a nation or society (Lewis, 2006, p. 1). Technological progress and economic shifts emphasize the importance of information, telecommunication and knowledge infrastructures (Thissen & Herder, 2003). Ever since the Cuban Missile Crisis of 1962 the concept of infrastructure security has been evolving. Former President of the United States of America, Kennedy, and former Prime Minister of

the Soviet Union, Khrushchev, had troubles with inadequate telecommunication technology. It was the first sector to be defined as 'critical' (Lewis, 2006, p. 2). Since the nineties, critical infrastructure protection became a main focus of security strategies.

Citizens rely on the proper functioning of certain organisations, e.g. water, energy, telecommunications... If critical infrastructures fail, it can compromise the functioning of society. Today, we ascertain some important technological and institutional changes, which have an impact on critical infrastructures. Also, systems are becoming more and more complex. Our global society obliges us to consider trans-boundary dependencies and an increasing service quality (Thissen & Herder, 2003). These transitions illustrate that the protection of critical infrastructures is a security strategy, which is far from clear.

The first problem scientists and practitioners encounter is the difficulty of formulating an efficient conceptualisation. Both theoretically and practically, current understandings of critical infrastructures are very vague, broad and uncertain. It seems almost impossible to fully understand the underlying structures and meaning of the concept. Subsequently, a second problem arises. In order to protect companies, organisations, sectors and/or key resources, three important aspects are necessary: risk planning, risk management and risk leadership. Yet, critical infrastructures can be huge in size and our global society challenges us to act both locally and internationally. The eruption of the Icelandic Eyjafjallajökull volcano in 2010 illustrates how a local nature disaster can have an enormous effect on technology (non functioning air traffic) and the economy in several countries. Therefore, critical infrastructures can be interdependent. As a result, prevention and repression strategies are extremely difficult because they question the very aim of security. More specific, what does 'security' of critical infrastructures means and how can we respond to threats or disasters if multiple sectors are involved? These questions entail a third problem. In order to protect critical infrastructures we need to have adequate protection strategies that focus on prevention. Moreover, we must reflect on threats or disruptive events that could happen. Considering the changing landscape of security, this almost seems impossible unless we can appeal on our creative thinking. As we will discuss, the focus on resilience (European Commission, 2013) is important and offers another direction in protecting our critical infrastructures.

2. MANAGING UNCERTAINTIES: IT'S ALL ABOUT CRITICAL INFRASTRUCTURE PROTECTION (CIP)

In this section of the paper, we will reflect on the conceptualisation of critical infrastructure protection. Considering the reliability of citizens on certain sectors, organisations and key resources, prevention strategies focus on 'uncertain and disruptive events'. This requires a profound system of intelligence in order to know the possible risks.

2.1. Critical infrastructure protection: a question of conceptualisation

A good and scientific analysis starts with a closer look at the conceptualisation at hand. The definition of CIP is not easy because of its wide range. This paper examines infrastructures that are critical and need protection. Each word entails a specific connotation and is characterized by several components. First, we have to examine the notion 'infrastructures', which are generally defined as organizational structures that are necessary for the operation of a society or enterprise or the facilities and services that are essential for an economy to function (Lewis, 2006).

The assets are divided into sectors (Lewis, Darke, Mackin & Dudehoeffer in Flammini, 2012, p. 4). According to the United States' National Infrastructure Protection Plan of 2006, infrastructures and key resources can be divided into eighteen sectors. These infrastructure sectors are agriculture and food protection, drinking water treatment, energy/power, information technology/telecommunications, transportation systems, defence industrial base, public health, banking/finance, postal/shipping and critical manufacturing. Key resources are national monuments/icons, government facilities, chemical facilities, commercial facilities, hydro-electric dams, emergency services and commercial nuclear reactors, materials and waste (United States' National Infrastructure Protection Plan, 2006).

Second, we have to define the notion of 'critical', which is problematic because if we take a look at the assets, sectors, organisations and key resources we can ascertain that numerous infrastructures are critical. In order to better understand this concept we have to reflect on the reliability of these infrastructures on the functioning of society. Taking a look at the existing literature, we can highlight that critical infrastructures are mostly defined as those assets, systems or functions that can seriously impact national-level public health, the economy, public safety, governance, national security and public confidence (Lewis, Darke, Mackin & Dudehoeffer in Flammini, 2012, p. 4). Critical infrastructures are *'vital and its incapacity or destruction would have a debilitating impact on our defense and national security. It is a network of independent, often privately owned, systems that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services'* (Lewis, 2006, p. 3). Therefore, critical infrastructures must ensemble in a reliable way so they provide a critical need (Dynes in Papa & Shenoi, 2008, pp. 3-4).

Third, we have to highlight the concept of 'protection', which is even more problematic. As we can see, the conceptualisation of 'critical' 'infrastructures' is vague and uncertain. This has consequences on how they are protected. Security and protection are focussed on dealing with threats or disruptive events that can vary in context, i.e. crime related, environmental, system failures... As a result, assessing risks becomes (almost) impossible. Most commonly, CIP is examined within a scope of crime related threats. In this light, the protection of critical infrastructures is about strategies and policies that are necessary to prevent and react to attacks or harms on the aforementioned sectors and key assets (Lewis, 2006, p. 4).

As mentioned in the introduction, three aspects are important in critical infrastructure protection, i.e. risk leadership, risk planning/assessment and risk management. An integrated risk management approach recognizes that both the optimal amount of risk retained and the tools used to achieve a risk level will differ from organisation to organisation. The meaning of integrated is twofold, i.e. integrating risks and integrating ways to manage risks. It emphasizes a systematic approach where risks are evaluated taking into account the multidimensional effects on the organisation coupled with a framework for deciding upon the best implementation strategy (Chew, 2008, p. 74). Each decision leaders make as well as the integration of both risk planning and assessment means that, in turn, another set of risks emerges (Linkov et al, 2007). Dealing with risks means dealing with never ending uncertainties and strategies. Khatta (2008, pp. 81-82) highlights the need for risk impact analysis. This approach emphasizes decision makers to determine the consequences of possible disruptive events. Scenario building that enables us to reflect on 'things that could happen' is a much wanted tool.

Infrastructures vary in size. The bigger the asset, the more complex its protection gets. Each of the aforementioned sectors is extremely large, complex and open to attack by natural or human actors. Also, there is interdependency between these infrastructures and key resources, which make their protection all the more difficult. At the level of the ensemble of critical infrastructures there is a lack of understanding of these interdependencies (Dynes in Papa & Shenoi, 200, pp. 3-4). Also, its protection is difficult because there is an absence of standardized risk assessment schemes. As a result, we cannot compare the existing risks between regions, industries and divisions. Each sector applies its own methods targeting different aspects of critical infrastructure protection (Lewis, Darke, Mackin & Dudehoeffer in Flammini, 2012, p. 4). Researchers come to the conclusion that it is practically and economically unrealistic to fully protect every component or sector, let alone all sectors (Lewis, Darke, Mackin & Dudehoeffer in Flammini, 2012, p. 4). Instead of focussing on the idea that critical infrastructures can be successfully secured as a whole, several authors emphasize the need of a prioritization scheme in order to protect critical infrastructures with limited resources (Flammini, 2012, Lewis, 2006). This means that we must focus on systems instead of sectors and on networks with partners, both publically and privately. In order to prevent supply chain risks or risks due to interdependencies between critical infrastructures, we need better frameworks (Dynes in Papa & Shenoi, 2008, pp. 3-4). Lewis (2006) also emphasizes the necessity of 'asymmetric thinking', which means we have to search for new ways to protect our vast and critical infrastructures from attack, environmental harms and system failures.

Although we have tried to clarify its meaning, we can see that the conceptualisation of critical infrastructure protection remains challenging because of its size and its multidisciplinary components. Our focus is too much aimed at the 'protection' of 'uncertain events' that could happen to 'all critical infrastructures'. In Chapter 4 we will highlight another possible approach, which has become a strategy in Europe and can diminish some of the encountered difficulties.

2.2. Critical infrastructure protection in Europe

In 1999, the Treaty of Amsterdam emphasized the European Union's role in security strategies against terrorism (Van Nevel, 2010, p. 35). Post 9/11, the European Council approved an action plan, which highlights the importance of freedom and security for citizens. Therefore, acts of terrorism should be prevented and tackled. As a result, the European Union created the counter terrorism strategy in 2005 that focuses on prevention and protection.

In 2007, the European Union created a programme called '*Prevention, preparedness and consequence management of terrorism*', a project with a time limit of six years. The aim is to protect citizens and critical infrastructures within the scope of freedom and security (European Union, 2007) in supporting Member States. Although countries are individually responsible for the protection of critical infrastructures, it is important to have transnational guidelines because of the aforementioned interdependence between certain sectors and organisations. The EU also wishes to support its Member States.

In 2004, the European Commission launched a communication with the idea of creating a European Programme for Critical Infrastructures (EPCIP). The aim is to support companies and governments in the EU in their security strategies. It seeks to provide an

all-hazards cross-sectoral approach (www.ec.europa.eu). In 2005, the EPCIP emphasized the need for creating better networks. The Critical Infrastructure Warning Information Network (CIWIN) brings together the specialists from the EU to assist the European Commission in establishing networks programmes to facilitate information exchange on threats, vulnerabilities, measures and strategies (Van Nevel, 2010, p. 37). EPCIP Contact Point meetings are organized in order to exchange information between the EU Member States (www.ec.europa.eu). They also fund and execute multiple studies in order to identify the needs of an adequate critical infrastructure protection.

In 2008, there was an important transition when the EU launched a Directive called '*On the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection*'. Considering the fact that the EU highlights the freedom of each Member State to protect critical infrastructures, the Directive makes a clear distinction between Critical Infrastructures and European Critical Infrastructures. Article 2 of the Directive (2008) defines a critical infrastructure as *'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'*. A European Critical Infrastructure, on the other hand, has a different connotation. It a critical infrastructure that is located in the EU and its disruption or destruction must have a significant impact on at least two Member States. Article 2 of the Directive (2008) states that the impact must be assessed in terms of *cross-cutting criteria* (interdependencies of infrastructures). This means that when critical infrastructures have essential or vital services in several countries of the EU, security strategies obtain a European dimension.

In 2012, the European Commission launched a staff-working document called *'On the review of the European Programme for Critical Infrastructures Protection (EPCIP)'*. Based upon research results, they highlight several conclusions on critical infrastructure protection. All Member States have legally implemented the Directive of 2008 and have identified the European Critical Infrastructures. Also, they underlined that even though the Directive seeks to improve a better protection, there is no indication that the security of energy and transport sectors is improved. Another viewpoint of the staff-working document is the fact that European strategies should focus on systems instead of sectors (critical infrastructures are often too huge and complex). We also need a European Forum for decision-making and a critical infrastructure risk management policy with more specific guidelines and recommendations (European Commission, 2012, pp. 18-19).

In 2013, a very important document was launched that has new and interesting insights on the protection of critical infrastructures. The European Commission staff-working document '*A new approach to the European Programme for Critical Infrastructure Protection: making European critical infrastructures more secure'* (2013) highlights alternative directions. The interdependency between organisations, the variety and complexity of certain sectors as well as the uncertainties of transnational security strategies were points of discussion, which advocated the need of other focal points. The document stimulates the need of resilient critical infrastructures (we will discuss this in Chapter 4) and interdependent systems. Furthermore, a new approach will be implemented. In order to have a more focussed approach EPCIP selected four critical infrastructures that have a European dimension in order to optimise their protection and resilience. These sectors are Eurocon-

trol (EU Air Traffic Management Network Manager), Galileo (global satellite navigation system), the Electricity Transmission Grid and the European Gas Transmission Network (European Commission, 2013, pp. 7-8). The selection was based on their cross-border dimension, representativeness and interest in piloting and sharing best practices. The aim is to set up tools for prevention (risk management and risk assessment), preparedness (increasing consideration for resilience and preparation) and response (long-term recovery of critical services).

If we compare this document to other papers of the European Commission, we ascertain an increasing focus on specific strategies. The uncertainties of disruptive events made it quite clear that strategies should focus more on resilience and preparedness. This strategic shift offers opportunities to execute studies, which are much more focussed on certain particularities.

3. INTELLIGENCE, PRIVATE SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

Protecting critical infrastructures is an important core business in the framework of protecting the economic potential (Cools, Dassen, Libert, 2005). Intelligence services play a vital role in security strategies regarding CIP.

Intelligence is a process consisting of three characteristics (Shulsky & Schmitt, 2002). First, it is about gathering information regarding actual and potential threats. Second, it evolves around activities that focus on gathering, analysing and processing information as well as countering threats. Third, the organisation of intelligence is important. Often forgotten in literature is the fact that intelligence is also about networking. If you want information about actual and potential threats, you need to have contacts. Intelligence is, as a process, extremely complex. Information is necessary to obtain knowledge on situations, events and changes in society. Intelligence is also about assessing and evaluating risks. This means one must have solid networks and be able to estimate transition of a social, political, economic and technological nature.

The protection of critical infrastructures is an important task for intelligence services, since they provide advice and analysis regarding crime related threats (e.g. terrorism, sabotage). Collecting information regarding risks and possible disruptive events is challenging. We live in a world where a lot of information is available. Intelligence or knowledge gathering must make a distinction between relevant and irrelevant data. Subsequently, information can also be insufficient, undetermined and uncertain (Richards, 2010, p. 40). How can one determine which intelligence must be further explored or not? Protecting critical infrastructures means that scenarios must be created based on reliable information, especially since most problems are linked with indirect risks and immeasurable threats. In order to create efficient scenarios, networking (both privately and publically) is important. Collaboration strategies are important to protect our economic potential. Steenlant and Ven (2005, pp. 324-328) stress out that international commitments as well as meetings with companies are a necessity.

The security and safety of critical infrastructures is the responsibility of the owner of the company or organisation (Van Nevel, 2010). On this level another important partner emerges, i.e. the private security sector. Their foremost input is the provision of training. When organizations or installations, which have a vital impact on the continuous function-

ing of public authorities, the market and society are facing disruptive events or emergencies, it is of the utmost importance to safeguard and secure these critical infrastructures. Since critical infrastructures can be threatened, e.g. terrorist attacks, technological failures and natural disasters, the added value of private security is targeted in specialisation that is aimed at developing sector specific knowhow and market segments (CoESS, 2013, p. 17; Müller, 2012).

Training is an important focal point for private security. Companies and their personnel have to obtain a certification from government authorities and follow training if they want to deliver private security (CoESS, 2011). In most European countries, critical infrastructure protection is evaluated as an important task for private security. Subsequently, the protection of critical infrastructures is generally seen (Davidovic, Kesetovic & Pavicevic, 2012) as a responsibility that must be organized between the public and private sector.

Private security takes part in larger security strategies, which is mostly explained as 'governance of security'. This theory focuses on the pluralisation of security in certain areas or 'nodes' and examines how these 'nodes' relate to one another (Johnston & Shearing, 2003). However, a very recent study conducted by Adam White (2011) sheds new light on the matter. He claims that a broader interdisciplinary scope is needed, i.e. the integration of the 'new political economy'. His main critique of contemporary studies on private security is that they fail to integrate both the administrative context and the economic context (White, 2011). Indeed, scientists in general and criminologists in particular often overlook to integrate both pillars in security research. However, contemporary studies need to find a way to implement both the administrative and the economic context. This would allow us to fully understand the underlying process and practical organisation of security related private – public collaboration strategies.

We already discussed the conceptualisation of critical infrastructure protection and the role of intelligence. The question arises: what is the role of private security companies in critical infrastructure protection? In order to give an appropriate answer we must take a look at the field and consult the existing working documents. The Confederation of European Security Services (CoESS), which is the representative organisation for private security services, has created interesting white papers and guidelines that give a general overview of the current situation. Considering the aim of this paper, it is necessary to discuss certain aspects of these documents. The sector emphasizes the '*explicit allocation of roles and responsibilities for protection along with common standards of risk assessment to be adopted so that best practice is used to apply appropriate levels of security'*(CoESS, 2012a, p. 4). Taking into account the importance of accountability and responsible decision-making (Davidovic, Kesetovic & Pavicevic, 2012, p. 70) the private security sector advocates the need of a special license regarding critical infrastructure protection (CoESS, 2012a).

The main issue of contemporary public – private partnerships in security strategies is that private security is often called upon as an afterthought. As a result, the effectiveness of such a collaboration is somewhat eroded. In order to improve effective partnerships, the private security sector should be included from the beginning, i.e. in the design (conceptualisation of approaches) and the operation (possible as well as applied strategies) of critical infrastructure protection (CoESS, 2012a). Considering the fact that the private security industry consists of corporations, the sector is more than familiar with the structural components of risk assessment, identifying security threats and sector specific training.

4. NEW DIRECTIONS IN THINKING ABOUT CRITICAL INFRASTRUCTURE PROTECTION: THE INTRODUCTION OF RESILIENCE

The new European focus on resilience is quite exciting because it narrows the gap in critical infrastructure protection. But what does this precisely mean? Taking a look at other international documents, we conclude that this shift is detectible in other regions as well. In the United States of America, the National Infrastructure Advisory Council or NIAC supplies advise concerning the aforementioned eighteen critical infrastructure sectors and key resources. They also give feedback to lead federal agencies having responsibilities regarding CIP and industry coordinating mechanisms. Their aim is twofold. First, they want to search for strategies which enhance public-private cooperation. Second, they encourage the private industry to frequently perform risk assessments of critical information and telecommunication systems (http://www.dhs.gov/national-infrastructure-advisory-council).

In 2009, the NIAC released a study report called "Critical Infrastructure Partnership Strategic Assessment Study", which highlighted some interesting results. It focuses on the importance of resilience for the public and private sector in creating their risk assessment strategies. Infrastructure resilience is '*the ability to reduce the magnitude, impact and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to and/or rapidly recover from a potentially disruptive happening*' (NIAC, 2009, p. 8). Risk management should therefore focus on the resilience of a critical infrastructure.

Resilience aims at the enhancement of three capacities. The absorptive capacity is the ability of the system to endure a disruption without significant deviation from a normal operating performance. The adaptive capacity is the ability of systems to adapt to a shock to normal operating systems. Recoverability is the ability of a system to quickly recover from disruptive events (NIAC, 2009).

Three features characterize critical infrastructure resilience (NIAC, 2009). These features are robustness (maintain operations and functions in the face of a crisis), resourcefulness (prepare for, respond to and manage a crisis or disruption as it unfolds) and rapid recovery (return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption).

It is important to stress out some of the recommendations of the NIAC report (2009), since they are specific and coherent with scientific research on critical infrastructure protection. A first focus should be on further exploring the conceptualisation of critical infrastructure protection and resilience. As other studies highlight (Goetz & Shenoi, 2010; Flammini, 2012; Hokstad, Utne & Vatne, 2012), our current knowledge remains very general and there are many difficulties in clarifying the main focal point. The main problem is the fact that several infrastructure sectors can be viewed as 'critical'. Also, the possibility of a 'chain reaction' if a disruptive event occurs is a vast reality, e.g. the effects of the Eyjafjallajökull volcano in Iceland impacted the economy, technology... Risk management is often restricted to specific sectors and organisations. The interdependency between critical infrastructures, nationally and internationally, challenges an integrated approach. Therefore, public-private cooperation strategies are of the utmost importance. As scientific research emphasizes (Goetz & Shenoi, 2010), the roles and responsibilities of critical infrastructure partners should be clarified and implemented in risk management. Since the protection of critical infrastructures challenges partners to 'think about the unthinkable' (Gosselin, Leysen & Verbeke, 2007), we must focus on alternative viewpoints and

working procedures. In this scope, the focus on resilience should be encouraged because it is the first step towards an adequate protection. As mentioned, private-public collaboration strategies are of the utmost importance. This focus was made very clear in the NIAC report. Europe's strategy is somewhat comparable with the US.

Three main strategies are linked with the European viewpoint on critical infrastructure resilience, i.e. prevention, preparedness and response (European Commission, 2013, p. 8-9). The aim of the European Commission is to work on each of these characteristics. Prevention will be aimed at the creation of tools for risk assessment and risk management. In doing this, the private sector should be included more profoundly. The idea is to create best practices on a European level, which highlight several recommendations, scenario scenes and guidelines. Considering the fact that intelligence plays a vital role, the EU Intelligence Analysis Centre (INTCEN) will also be included in further planning. The preparedness and response strategy is aimed at training, awareness and exercises.

In our opinion, what is missing in the document is the vital role of risk leadership and coordination. Since European Critical Infrastructures are crosscutting and interdependent, how will these strategies be coordinated? This remains unclear and since a multitude of partners is involved, a profound risk coordination scheme is of the utmost importance.

Although these transitions are interesting, several questions still remain unanswered. First, the importance of preparedness is still very vague. As mentioned, disruptive events that can threaten critical infrastructures are uncertain. All things considered, numerous threats could occur. Also, we do not know if and when such events will take place. We have to deal with a lot of uncertainties. We can ask the same question for the factor 'response'. How can we prepare an efficient recovery if we do not know what could happen? Scientifically speaking, there are several challenges tangible and we lack a proper theoretical framework that could clarify the underlying difficulties. Criminological research produced several security studies that focus on strategies and governance. They mostly focussed on direct threats. However, we lack insight that deals with uncertain events. The following chapter will provide a criminological framework that will highlight these uncertainties more profoundly.

5. CHALLENGES FOR THE CRIMINOLOGICAL RESEARCHER: THINKING ABOUT UNCERTAINTIES AND VAGUE EVENTS THAT COULD HAPPEN

As mentioned, scientific studies regarding critical infrastructure protection and resilience are not common. A possible explanation for the current lack of research could be the difficulty of an alternative scope and the wide range of critical infrastructures. Therefore, it is important for scientists to focus on two realities.

First, we have to be able to study uncertain threats, i.e. disruptive events that have not occurred but could happen. This means we have to be able to widen our theoretical framework, both nationally and internationally. Subsequently, the concept of 'risk management' should be integrated in security studies. Second, we must take into account the changing landscape of 'security'. Critical infrastructure protection is not a 'new' phenomenon, however the actual conceptualisation is. This is mainly due to societal transitions and the changing landscape of 'security'.

If we take a look at literature regarding security and thinking about the unthinkable (Gosselin, Leysen & Verbeke, 2007), we can conclude that most ideas are formulated from a

perspective of criminal threats such as terrorism and war. Critical infrastructure protection is therefore mainly studied within this scope. Intelligence and security services are also focused on these threats. However, environmental events and technological failures can also have disastrous effects on infrastructures. Subsequently, 'thinking about the unthinkable' for organisations, firms and society has never been so challenging, especially since we live in a global society where boundaries are becoming more and more blurred.

The focus on resilience offers new opportunities. Also, the importance of systems instead of entire sectors offers more hand-on working procedures. Gosselin, Leysen & Verbeke (2007) conducted research related to the question 'What can threaten our prosperity?' In answering this question we must study our weaknesses. Culture, institutions and democracy have an important position among intangible assets (e.g. corporate culture, ethics, consultation...) of highly developed industrial countries (Kay, 2004, p. 37; Gosselin, Leysen & Verbeke, 2007, p. 4). This means that several invisible characteristics are associated with protection of our economic potential and the protection of critical infrastructures. This knowledge is often overlooked. Nevertheless, if the interdependency between infrastructures is a priority, these elements should also be included.

Let us examine the different aspects of security, which will clarify the difficulties critical infrastructures are facing. Our society faces potential and existing threats that can be characterized on several levels (Crawford, 2012). First, we emphasize crime-related risks and threats. These can be acts of terrorism, organised crime ... Second, technological threats are becoming more and more apparent. Third, economic risks are a vast reality. Fourth, environmental threats often remind us of our vulnerability. Fifth, we are also facing scientific risks, since certain inventions and study results can be much wanted items. All these events occur both locally and globally.

The problem of this changing landscape of security is that criminology studies mostly focus on the first characteristic. However, we can ascertain blurring boundaries between all these levels. The 9/11 terrorist attacks are a perfect example of how all these security facets can be intertwined. Criminologists should ask themselves two important questions: 'Is our knowledge of security still applicable in this global and multidimensional reality?' and 'Shouldn't we be focussing more on this changing landscape and aim at multidisciplinary security studies that focus on an evaluation of disruptive events, both global and local?'

In our opinion these questions should be discussed amongst scientists and practitioners. If we want to search for new directions, interplay between empiric science and applied science is of the utmost importance.

6. CONCLUSION

If we want to increase our knowledge on critical infrastructure protection, we need to increase academic research. The concepts of critical infrastructures, protection, resilience, preparedness and response need to be further defined. We must also focus on alternative methodologies (Pashley & Cools, 2013) in order to examine the underlying characteristics of uncertain disruptive events. Subsequently, a theoretical framework should be developed, based upon empirical studies. Security and protection in the 21st century require an alternative and a broad scope. Uncertainties can seem unmanageable. However, creative thinking can help change old directions into new opportunities.

REFERENCES

1. Chew, D.H. (ed.) (2008). Corporate Risk Management. *Journal of Applied Corporate Finance*. Columbia: Columbia University Press.
2. CoESS – APROSER (2013). *The socio-economic value of private security services in Europe.* Fourth White Paper on Private Security. Wemmel: CoESS.
3. CoESS (2012a). *Critical infrastructure security and protection: the public-private opportunity.* White Paper and guidelines by CoESS and its working committee. Wemmel: CoESS.
4. CoESS (2012b). *Critical infrastructure private guarding company requirements checklist.* Wemmel: CoESS.
5. CoESS (2011). *Private security services in Europe: facts and figures.* Wemmel: CoESS.
6. Cools, M., Dassen, K. Libert, R. & Ponsaers, P. (eds.) (2005). *De Staatsveiligheid: essays over 175 Veiligheid van de Staat.* Brussel: Politeia.
7. Crawford, A. (2012). *The evolving concept of security: mapping the dynamics of security in Europe.* Leeds: unpublished document.
8. Davidovic, D. Kesetovic, Z. & Pavicevic, O. (2012). National critical infrastructure protection in Serbia: the role of private security. *Journal of Physical Security* 6(1). pp. 59-72.
9. European Commission Staff Working Document. A new approach to the European Programme for Critical Infrastructure Protection: making European critical infrastructures more secure. Brussels. 28/08/2013.
10. European Commission Staff Working Document. On the review of the European Programme for Critical Infrastructures Protection (EPCIP). Brussels. 22/06/2012.
11. European Commission, Critical Infrastructures, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm, 20/06/2013, 15h30.
12. European Union Council Directive. On the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union. 23/12/2008.
13. European Union Counter-Terrorism Strategy, Brussels 30th November 2005, http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf, 20/06/2013, 16h55.
14. European Union (2007-2013). Specific programme: prevention, preparedness and consequence management of terrorism (2007-2013), http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33262_en.htm, 20/06/2013, 17h15.
15. Flammini, F. (ed.) (2012). *Critical infrastructure security: assessment, prevention, detection, response.* Billerica: WIT Press.
16. Goetz, E. & Shenoi, S. (2010). *Critical infrastructure protection.* New York: Springer.
17. Gosselin, P.G., Leysen, J. & Verbeke, T. (2007). Protecting a nation's economic potential: proposal for a scientific research agenda. *European Journal of Intelligence Studies* (1), pp. 3-21.

18. Hokstad, P., Utne, I. & Vatne, J. (eds.) (2012). *Risks and interdependencies in critical infrastructure protection.* London: Spinger-Verlag.
19. Homeland Security, National Infrastructure Advisory Council, http://www.dhs.gov/national-infrastructure-advisory-council, 20/02/2013, 15h24.
20. Johnston, L., & Shearing, C.D. (2003). *Governing Security: Explorations in policing and Justice.* Londen: Routledge.
21. Kahn, H. (1980). *Thinking about the unthinkable in the 1980s.* New York: Hudson.
22. Khatta, R.S. (2008). *Risk Management.* New Delhi: Global India Publications Pvt Ltd.
23. Kay, J. (2004). *The truth about markets: why some nations are rich but most remain poor.* London: Penguin Books.
24. Lavoy, P.R., Saga, S.D. & Wirtz, J.J. (2000). *Planning the unthinkable.* Cornell: Cornell University Press.
25. Lewis, T.G. (2006). *Critical infrastructure protection in Homeland Security: defending a networked nation.* New Jersey: Wiley Interscience.
26. Lindsay, J. (2005). *Dearly Devoted Dexter.* New York: Doubleday.
27. Linkov, I., Wenning, R.J. & Kiher, G.A. (eds.) (2007). *Managing Critical Infrastructure Risks*. Dordrecht: Springer.
28. Lopez, J. Setola, R. & Wolthusen, S.D. (eds.) (2012). *Critical infrastructure protection: information infrastructure models, analysis and defence.* Berlin Heidelberg: Springer-Verlag.
29. Müller, J. (2012). Schutz kritischer Infrastrukturen. In: Stober, R., Olschok, H., Gundel, S. & Buhl, M. (eds.). *Managementhandbuch: Sicherheitswirtschaft und Unternehmenssicherheit.* Stuttgart: Richard Boorberg Verlag, pp. 366-375.
30. National Infrastructure Advisory Council (2009). *Critical Infrastructure Resilience.* Research Report. USA.
31. Papa, M. & Shenoi, S. (red.) (2008). *Critical infrastructure protection 2*. New York: Springer.
32. Pashley, V., Cools, M. (2013), Breaking boundaries. Collapsing the dark side of researching criminology. In Beyens, K., Christiaens, J. et al (ads), *The Pains of Doing Criminological Research*. Criminological Studies. Brussels: VUBPress, pp. 161-180.
33. Presidential Policy Directive, Critical Infrastructure Security and Resilience, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, 21/06/2013, 14h24.
34. Richards, J. (2010). *The art and science of intelligence analysis.* Oxford: Oxford University Press.
35. Shulsky, A. N. & Schmitt, G.J. (2002). *Silent Warfare: understanding the world of intelligence.* Virginia: Potomac Books.
36. Steenlant, J. & Ven, C. (2005). Het belang van de inlichtingendiensten voor de bescherming van het economisch potentieel van onze bedrijven. In: Cools, M., Dassen, K. Libert, R. & Ponsaers, P. (eds.) (2005). *De Staatsveiligheid: essays over 175 Veiligheid van de Staat.* Brussel: Politeia.

37. Thissen, W.A.H. & Herder, P.M. (2003). *Critical infrastructures: state of the art in research and application.* Kluwer's International Series: Operations Research & Management Science. Dordrecht: Kluwer.
38. United States' National Infrastructure Protection Plan 2006.
39. Van Nevel Hannes (2010). De bescherming van kritieke infrastructuren: een publieke of overheidstaak? Een casestudy in de Zeebrugse Haven. Master Dissertation. Ghent University.
40. White, A. (2011). The new political economy of private security. *Theoretical Criminology 16*(85), pp. 85 – 101.
41. White, A. (2010). *The Politics of Private Security: Regulation, Reform and Re-legitimation*. New York: Palgrave Macmillan, 216 p.

UDC 726.9:75.041.5
ID 176374796

Goran Matić, Milan Miljković
Office of the National Security Council and Classified Information Protection of the Government of the Republic of Serbia
goran.matic@nsa.gov.rs
milan.miljkovic@nsa.gov.rs

CRITICAL INFRASTRUCTURE PROTECTION IN CYBERSPACE

Abstract: Massive application of information and communication technology has brought about new risks and threats represented by physical and software related dangers to critical information infrastructure and cyberspace of relevance to the nation and its security. The leading countries in the world as well as international organizations show growing awareness of the need to take action to raise the security level in cyberspace. In this context cyberspace itself constitutes the critical infrastructure, or more precisely, the critical information infrastructure due to which the concepts of protection of critical infrastructure and cyberspace are closely linked. When protecting critical infrastructure the public sector, i.e. governments cannot act on their own and have an imperative need to cooperate with representatives of the corporate sector, non-governmental organizations and specialistis in particular areas (the public-private partnership concept). The protection of a highly vulnerable system, such as the national critical information infrastructure also includes handling of classified information as one of its components by which individual segments of the organization and the functioning of the system are safeguarded. In organizational terms, crisis management in cyber defense implies engaging the capacities of the relevant Ministry of Justice and Public Administration, Ministry of Tansportation, Ministry of Defense, Ministry of Foreign Affairs, Ministry of Finance, Ministry of Internal Affairs and the security and intelligence community. Their activities as well as the overall cyber policy are coordinated and guided by organizations of the executive branch, for example the National Security Authority (NSA), as a body responsible for the coordination of the national security policy or steered by a ministerial committee.

Key words*: threats in cyberspace, critical information infrastructure, information security, classified information, crisis management in cyber defense, CERT, national cyber defense council.*

1. INTRODUCTION

Massive application of information and communication technology has brought about new risks and threats represented by physical and software related dangers to critical information infrastructure and cyberspace of relevance to the nation and its security. Cyberspace has become the determining feature of modern-day life and the key area of world economy. Tens of thousands more or less hazardous attacks are registered in cyberspace on the daily basis and the leading countries in the world, as well as international organizations which show growing awareness of the need to take action to raise the security level in this domain. Many of them already have their own cyber security strategies and established cyber defense systems.

Thus the Cyber Security Strategy for Germany (2011, p.14) defines cyber as virtual space for all information and telecommunication (IT) systems connected at the level of databases on a global scale. This strategy makes the point that the internet is a core prerequisite for the existence of syberspace, as a universal and publicly accessible network that can be further expanded and upgraded by adding networked databases. It also argues that in the isolated virtual space IT systems are not part of cyberspace. On the other hand, the UK Cyber Security Strategy (2011) puts forward that cyberspace implies the internet, although it is not the basic condition for its existence. In this context, the question arises why defining the basic terms relating to cyberspace challenges is so complex and difficult. The experiences gained so far suggest that the core of this problem lies with different angles of looking at this problem, distinct political and legal approaches to this problem by the world's leading countries which stem from their particular interests in connection with the use of cyberspace for achieving goals on the national and international level. It follows from the above that every security problem has the following three dimensions: 1) Political (strategic), 2) Legal, and 3) Technological.

2. THREATS IN CYBER SPACE - CLASSIFICATION

For more than a decade now, analysts have been speculating as to potential consequences of threats coming from cyberspace. In the meantime, there is no generally accepted definition that identifies and classifies these and other cyber incidents. At this point there are two predominant albeit different pro-governmental concepts of understanding and defining a scale of threats from cyber attacks, one being propagated by the US Government and the other one by the Shanghai Organization of Cooperation headed by Russia and China (O.A. Hathaway, R. Crootof, 2012, p.8).

On the other hand, after analyzing the views presented in the cyber strategies of the developed countries, cyber activities can, in principle, be divided into four groups:

Cyber crime 2) Cyber terrorism 3) Cyber espionage, and 4) Cyber warfare.

It should be stressed that physical forms of cyber terrorism, cyber warfare, cyber espionage and cyber crime often look alike or identical. Lech J. Janczewski and Andrew M. Colarik illustrate this point with the example of an individual breaking into the hospital databasis to prescribe a medicine to a patient who is allergic to its ingredients. As a consequence of that, the patient dies. If the attacker's intention were to harm or kill the patient for some personal reasons, then this event would constitute a criminal offense committed by means of computer technology, i.e. an act of high-technology or *cyber crime*. In case the attacker made it known later on that he was ready to commit more offences along these lines, in case his/her conditions had been fulfilled, then such conduct would be described as an act of *cyber terrorism*. Moreover, if the above offender was also an agent of the adversary structures and there also occurred a theft of classified information relevant to the national security, that act would be qualified as *cyber espionage*. So, the attacker's intention is one of the factors that influences the classification of malicious activities in cyberspace into cyber terrorism, cyber espionage or cyber crime.

Malicious activities in cyberspace can also be carried out by state or non-state actors; they involve active conduct of attackers and are aimed at jeopardizing the functioning of the victim's computer network with a view of accomplishing political or national security objectives. In this sense, in our attempt to give an approximate definition of *cyber war,*

we can say that this terms implies only cyber attacks with state actors behind them whose impact is equivalent to a conventional "armed assalt" or alternatively that it entails cyber attacks that occur in the context of an armed conflict and develop into a cyber war (O.A. Hathaway, R. Crootof, 2012, p.17).

For the prupose of further clarification of malicious activities in cyberspace, we shall put forward one of the several classifications as outlined in the Table 1 below. Although it only explains the relation between cyber attacks, cyber crime and cyber warfare, it is important in the context of assessment that the critical infrastructure will be the object of activities that would probably evolve to a cyber attack or be carried out within an armed conflict.

With regard to the defense of the critical infrastructure in cyber space it is important to highlight the difference between the terms that denote similar defense activities in cyber space. In this sense, we shall set out the classification below:

1. Cyber defence - relates to defense of the critical infrastructure that may be publicly or privately owned;
2. Informatical assurance – relates to the protection of cyber space used for the functioning of the state authorities, and
3. Information security (infosec) – relates to work on classified information peformed on the network owned by the state authorities.

Table 1: Relation between cyber attack, cyber crime and cyber warfare
(Source: O. A. Hathaway, Rebecca Crootof,
The law of cyber attack, California Law Review, 2012)

Types of malicious activities in cyber space	State actors involved only	Must be liable to prosecution and carried out by computer devices	Objective must be to incapacitate the functioning of computer network	Must have political or national security related purpose	Impact of such act must be equivalent to armed attack or must occur in the context of armed attack
Cyber attack			+	+	
Cyber crime	+	+			
Cyber war			+	+	+

3. CRITICAL INFRASTRUCTURE AND RELATED SECTORS

Definitions of *critical infrastructure* generally refer to resources, systems, physical or virtual networks, whose destruction or incapacitation may undermine the national security, economic stability and affect other aspects of normal functioning of a society (D.Vuletic, 2012, p.1).

Critical information infrastructure is a narrower term than critical infrastructure and constitutes its integral part. It can be located in both public and private sectors. Critical inormation infrastructure involves services, computer networks and other ICT-based systems of relevance to the functioning of a given country from the economic, security and other aspects (D.Vuletic, 2012, p.1).

In the last decade significant steps have been made to identify and analyze *critical infrastructure elements* from the aspect of risk and preparations for the events that may impede their operation. The mere existence of related strategies aimed at effective prevention of extremely negative scenarious (terrorist attacks or large-scale natural disasters) does not necessarily mean that optimal resources have been allocated for the protection of critical infrastructure. This rather complex issue poses a great challenge for the adequate planning of responses to natural disasters or other hazards.

Based on the survey of foreign reference literature (J. Moteff and P. Parfomak, 2009), the following key sectors of the national critical infrastructure can be identified:

- Information and communications (telecommunications, network and the internet)
- Electrical power
- Transport
- Oil and gas (supply, transport, refinement and distribution)
- Banking and finances
- Water supply and emergency services
- Government and armed forces.

4. CRITICAL INFRATRUCTURE PROTECTION IN CYBERSPACE

The critical infrastructure protection can be defined (Lewis G, 2006, p. 4) as strategies, policies and readiness necessary to deter, prevent and respond in case of an attack on critical infrastructure. More precisely, critical infrastructure protection comprises the following three aspects: political, organizational, and implementative.

The political aspect covers the adoption of appropriate policies and laws on cyber defense, informatical assurance, critical infrastructure and other rules necessary for legal regulation of detterence, prevention and response in case of cyber defense on critical infrastructure. The above documents generally set out the following state mandates: 1) military activities, 2) suppression of high-tech crime, 3) intelligence and counterintelligence activities, 4) critical infrastructure protection and crisis management, and 5) cyber diplomacy.

When discussing *the legal aspect of cyber defense* of critical infratructure, the following relevant cyber defense rules should be mentioned:

1. Rule of territoriality, which means that information infrastructure located on the territory of one state is subject to its territorial sovereignty;
2. Rule of responsibility, which means that a given state bears responsibility for a cyber attack made from the information system located on its territory;
3. Rule of cooperation, which implies that the state from whose territory such an attack has been made is obliged to cooperate with the affected country, and
4. Rule of self-defense, which means that everyone has the right to self-defense in case of apparent and impending danger and with respect of the law governing armed conflicts.

The protection of a highly vulnerable system such as the national critical infrastructure also includes as one of its components the handling of classified information in the state communication network figuring as an important critical infrastructure facility The said classified information helps safeguard individual segments of the organization and the functioning of the system and is classified according to the provisions of the Law on Clas-

sified Information. For access to classified information, the individual needs to hold an appropriate security vetting certificate (Law on Classified Information, The Official Gazette of the RS, No.104/2009). The protection of classified information in information and telecommunication systems is regulated by separate legal arrangements and by-laws.

In *organizational terms*, crisis management in cyber defense implies the engagement of capacities of the Ministry of Justice and Public Administration, Ministry of Transport, Ministry of Defense, Ministry of Foreign Affairs, Ministry of Finance, Ministry of Inernal Affairs and the security and intelligence community. Consequently, over the last two years the developed countries have made important steps to identify the existing civilian and military capacities and set up new ones to be responsible for cyber defense, as well as efforts to define interdepartmental cooperation and roles of the private sector in this area. In organizational terms, it very important to identify a coordinating body, which is most often derived from the executive branch, to take over the role of coordinating and directing the overall policy in the area of critical infrastructure cyber defense in the public and private sector alike. In many countries this task is often assumed by the National Security Authorities (NSAs), responsible for coordination of national security policies or carried out by a ministerial committee.

When discussing the executive phase of *the critical information infrastructure protection* – CIIP, it should be underlined that it rests on four pillars given below (Suter M., A, 2007, p. 1):

- Prevention and early warning;
- Detection;
- Reaction, and
- Crisis management.

When protecting critical infrastructure the public sector, i.e. governments are unable to act on their own and have an imperative need to cooperate with representatives of the corporate sector, non-governmental organizations and specialistis in particular areas (the public-private partnership concept). For that reason the private sector must be considerably involved in the critical infrastructure protection. Hence, the public-private partnership is considered an important pillar of the critical infrastructure policy.

Various forms of CERT related organizations are set up in order to establish efficient early warning mechanisms that perceive threats. They operate as points for sharing and analyzing information about threats coming from cyberspace (ISAC – Information Sharing and Analysis Centers, WARP – Warning, Alerting and Reporting Points and the like). The exchange of information is carried out, not only in connection with the content of such threats, but for each individual critical infrastructure sector.

4.1. International experiences in the critical information protection in cyberspace

Critical infrastructure protection in cyberspace has become the subject of activities of numerous international and national organizations and institutions which is conducive to better awareness and understanding of this societal danger.

The Geneva based International Telecommunication Union (ITU) with over 190 member states is a specialized United Nations agency responsible for information-communication technologies. It undertakes various activities to improve telecommunication infrastructure, develop international standards, exchange ideas, knowledge and technology (D.Vuletic, 2011).

The EU has its track record of activities on the critical infrastructure protection which started at the beginning of 2004 when the European Council initiated the elaboration of the programme for its protection *(European Programme on Critical Infrastructure Protection –EPCIP).* In the next years, the following documents were adopted: The European Programme on Critical Infrastructure Protection (2006), Directive 2008/114/EC (2008) and the EU Internal Security Strategy (2010). In the course of 2012 the EPCIP and Directive 2008/114/EC were reviewed. Council Directive 2008/114/EC (2008) constitutes an integral part of the above programme. In February 2013 the EU adopted its Cyber Security Strategy. In addition, the Council Security Rules (doc. 10086/13) defined the responsibilites of National Security Authorities (NSAs) or other competent security organizations in connection with cyber defense. Moreover, at the beginning of 2013 the European Commission decided to include the review of activities on the development of cyber defense related legal framework and pertinent structures in the progress reports on EU candidate countries for 2013.

In Germany, the overall cyber policy at the national level is coordinated by the National Cyber Security Council, as a body of the German government composed of several Bundesware members. The National strategy for the critical infrastructure protection (CIP strategy) sums up the Government's objectives and intentions and outlines its political and strategic approach. It is included in the National plan for information infrastructure protection (NPSI). The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI), which operates as part of the Federal Ministry of Interior is a leading authority in the area of cyber security. The German Federal CERT (CERT-Bund) is a section of the 12 BSI divisions (acting as the central "point of contact" for resolving computer and network security problems on behalf of the federal agencies. BSI operates by elaborating a threat assessment and making an analysis, as well as by developing a protection concept along with the Federal Office of Civil Protection and Disaster Assistance (BBK), the Federal Criminal Police Office (BKA), the Federal Police (BPOL) and the Federal Institute for Technical Support. The operational group for CIP (AG KRITIS) was established to coordinate related activities with the competent Ministry and subordinated agencies. The strategic development and implementation are also coordinated with other Federal ministries, especially the Federal Ministry of Economy and Technology, the Office of the Chancellor, Federal Ministry of Justice, Federal Ministry of Foreign Affairs, Federal Ministry of Defense and other relevant agencies, such as the Federal Network Agency. In addition, strategic partners from private sector are consulted in connection with cyber security issues.

In Finland, cyber security is perceived as administrative data security and addressed as an issue of economic importance closely linked to the development of the Finnish information society. There are three main governmental agencies dealing with the critical information infrastructure protection (CIIP): the Finnish Communications Regulatory Authority (FICORA) at the Minsitry of Transport and Communications which promotes the information society and works on technical regulations and standardization; the Central Authority for overall security of supply for Finland (NESA) which analyzes threats and risks to critical information infrastructure (CII), and the Government Information Security Management Board (VAHTI), which elaborates political guidelines and practical guides for the security of IT systems (Finland's Cyber security strategy, 2013).

4.2. National aspect of critical infrastructure protection in cyberspace

As for the political and legal aspect of cyber defense of the critical infrastructure in our country some important steps forwards have been made in criminal and security legislation. The Serbian National security strategy classifies high-technology crime and threats to information and communication systems as important security risks. The National defense strategy identifies cyber threats as new security risks, and advocates continual development of technological protection of defense system components. In 2009 the Republic of Serbia ratified the Council of Europe Convention on cyber crime and made provision for incriminating high-technology offences by its Criminal law. However, although the draft law on information security was finished in 2012, the activities on its adoption have been discontinued.

The critical infrastructure is mentioned in the national reference documents only once in Chapter 6.2. of the Strategy for the information society development in the Republic of Serbia until 2020, which reads as follows: "It is necessary to develop and enhance protection from attacks by applying information technology to critical infrastructure systems; in addition to ICT systems they may include other infrastructure system administered by applying ICT, such as the electric power system. In this context, there is a need to further regulate criteria for designating the critical infrastructure from the aspect of information technology, set rules for evaluating such attacks through application of information technology on such infrastructure in relation to traditional forms of attacks and determine conditions for ensuring adequate protection in this area."

However, the other relevant national documents, such as the National strategy for the protection and rescue activities in contingencies and the Law on Emergency Situations do not even make references to issues of critical infrastructure. It should be pointed out that the institutional framework for defining the critical infrastructure is in place in the form of the Division for Contingencies, relevant ministries and regulatory bodies.

4.3. System of fight against cyber threats in the Republic of Serbia

The problem of critical infrastructure protection in the Republic of Serbia and the neighbouring countries is reflected in the following facts: absence of a national organization for coordination of critical infrastructure protection in cybespace; shortage of skilled personnel; lack of necessary technical tools for response in case of attack on the critical information infrastructure; non-existent mechanism for contact with relevant institutions in the country and the region; absence of a national cyber defense strategy.

Taking into account the above drawbacks and topicality of this thematic area, the Office of the National Security Council and Classified Information Protection (the NSC Office) communicated towards the end of 2012 a letter to all ministries and public authorities concerned requesting their views and suggestions in connection with a need to develop a national cyber defense concept.

Having reviewed the proposals put forward by the relevant ministries and public authorities, we feel that the Republic of Serbia should take the following key actions in this area: adoption of the draft Law on Information Assurance, drafting of a national strategy for cyber defense, identification and designation of the critical infrastructure and formation of a national center or team for proactive management of computer incidents equivalent to the above CERT bodies. Once the above cyber strategy and the draft Law on Informa-

tion Assurance are in place, the Serbian government bodies whose remits may include or already cover the fight against computer threats are as follows: the Office of the National Security Council and Classified Information Protection; the prospective national CERT (nCERT), and the Division for high-technology crime of the Ministry of Internal Affairs. Moreoever, the Ministry of Defense and the Serbian Armed Forces Headquarters, the Ministry of Foreign Affairs, security structures, Administration for Provision of Services to Governmental Bodies, *Telekom Srbija* mobile operator, *PTT Srbija* postal services, *NIS* oil industry, *EPS* electric power industry, private sector and banking sector also have capacities for the fight against individual types of cyber attacks which constitute an adequate core for further enhancement of national cyber defense capabilities.

5. CONCLUSION

In spite of the absence of a specific system for critical infrastructure defense in cyberspace within the existing national legislation, it can be assessed that the Republic of Serbia has provided its defense mainly thorugh the implementation of IA measures which need to be further elaborated on once the above cyber defense strategy and the draft Law on Information Assurance have been adopted. In the light of the foregoing tendencies perceived in the international community concerning the legal and organizational aspects of cyber defense, we propose the following actions:

1) initiating an expert debate within the governmental structures to identify and examine cyber challenges, risks and threats; 2) launching the procedure for supplementing the National Security and Defense Strategies, as well as drafting a cyber defense strategy; 3) undertaking activities to identify and designate the critical infrastructure and build capacities for the critical infrastrucutre defence in the Republic of Serbia cyberspace, and 4) international cooperation and permanent interpartmental interaction in that area.

REFERENCES:

1. Cyber Security Strategy for Germany, Federal Ministry of Interior, 2011. Available at, http://www.cio.bund.de/.../css_engl_download.pdf? Accessed 05/11/2012
2. Cyber Security Strategy of the United Kingdom, UK Office of Cyber Security, 2009. Available at, http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf. Accessed 15/01/2013
3. Decree on special measures for the protection of classified information in information and telecommunication systems (Official Gazette of the RS, 53/2011). Available at http://www.nsa.gov.rs. Accessed 12/08/2013
4. Finland's Cyber security strategy, available at http://www.yhteiskunnanturvallisuus.fi. Accessed 15/07/2013
5. Hathaway A., Rebecca Crootof, The law of cyber attack, California Law Review, 2012. Available at http://www.californialawreview.org/assets/pdfs/100-4/02-Hathaway.pdf Accessed 10/07/2013
6. J. Moteff and P. Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification," Congressional Research Service, The Library of Congress, 2004. Available at http://www.fas.org/sgp/crs/RL32631.pdf. Accessed 10/09/2012
7. Lewis G., Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation, John Wiley & Sons Inc. Hoboken, New Jersey (USA), ISBN-13: 978-0-471-78628-3 (2006) Accessed 20/08/2013
8. Law on classified information (Official Gazette of the RS, 104/2009) A*vailable at* www.paragraf.rs/propisi/zakon_o_tajnosti_podataka.html. Accessed 10/08/2013
9. Murray A.T., T. Grubesic., "Critical infrastructure protection: The vulnerability conundrum," *Telematics and Informatics,* vol. 29, no. 1, February 2012.
10. "National Infrastructure Protection Plan," Homeland Security, 2009. A*vailable at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.* Accessed 20/08/2013
11. NSA acronyms, available at http://www.nsa.gov/about/faqs/terms_acronyms.shtml, accessed 04/01/2011
12. Suter M., A Generic National Framework for Critical Information Infrastructure Protection, Center for Security Studies, ETH Zurich, 2007, p. 1. Available at http://www.itu.int/osg/spuold/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf. Accessed 28/08/2013
13. UK Cyber Security Strategy, Protecting and promoting the UK in a digital world, November 2011. https://www.gov.uk/government/.../uk-cyber-security-strategy-final.pdf. Accessed 28/08/2013
14. Vuletić D., Defense against threats in cyberspace, ISI, Belgrade 2011, p. 57, Available at www.isi.mod.gov.rs/.1328179353_Odbrana%20od%20pretnji%20u%. *A*ccessed 05/03/2012
15. Vuletić D., Critical infrastructure protection – global and national aspect, Information Assurance Conference Proceedings, 2012. Available at http://*www.bisec.rs/global/zbornik_full_v01.pdf* . Accessed 05/07/2013

UDC 726.9:75.041.5
ID 176374796

Denis Čaleta, Aleš Kotnik
Institute for Corporative Security Studies, Ljubljana
denis.caleta@ics-institut.si
ales.kotnik@ ics-institut.si

CYBER THREATS AND DILEMMAS OF CRITICAL INFRASTRUCTURE PROTECTION IN SMALL STATES: COMPARISON BETWEEN ATTACKS IN GEORGIA AND ESTONIA

Abstract: Major changes in the international political, security, defence, social, environmental field and globalization in the 21st century brought new opportunities and challenges in the security field. We are today faced with threats in both the real and virtual world, which are quite real, dangerous and can have potentially deadly consequences. There have been examples in our surrounding area, where cyber threats have become real and have had a serious impact on critical and other infrastructure, like in Estonia 2007 and Georgia 2008. Those two examples will be analyzed in more detail. This paper is intended to identify threats and vulnerabilities that threaten critical infrastructure from cyber space. The main research question is: Is the vulnerability of critical infrastructure and cyber space for small countries greater than for big countries?
Keywords: *critical infrastructure, cyber threats, cyber attacks, Estonia 2007, Georgia 2008*

1. INTRODUCTION

The main reason and motivation for dealing with cyber threats and their impact on national security is the rapid development of cyberspace, which is increasingly integrated into the life of an individual and a society. The current situation is characterized by major changes in international relations in the politics, security, defense, society, environment and globalization, which is mainly the result of the development of cyberspace in the 21st century. The international security environment is becoming more unpredictable and challenging, where especially asymmetric threats in cyberspace represent a major threat and challenge to freedom and security.

Examples of where cyber threats become real, dangerous, and have a serious impact on the critical and other infrastructure in our surrounding area like in Estonia and Georgia in 2007 and 2008, remind us that the threats posed in cyberspace are serious and those two examples will be analyzed in more detail. We would like to make a contribution aimed at identifying the contemporary threats and consequent vulnerability that threaten countries in cyberspace. The main research question in this paper is: is the vulnerability of critical infrastructure and cyber space the greater threat to small countries than for large countries?

Most important in this is that we understand concepts and processes that have occurred in recent years in the field of protection of critical information infrastructure and how it can be at risk from cyber space. The main contribution primarily leans on the results of high-quality and comprehensive research, which was performed by researchers Tikk, Kaska

and Vihul from Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn in Estonia and of course on the analysis of domestic and foreign literature in the field of cyber security. Finally, we will show what the situation was and what the actual consequences were of the attacks from cyberspace in Estonia and Georgia. Their comparison will give us a better understanding of international cyber incident and what the possible solutions in the field of risk management are when it comes to cyber attacks on a country.

2. INTERNATIONAL CYBER INCIDENTS

In the international environment it is difficult to identify and define the type and extent of cyber threats and incidents. This makes it difficult to recognize when there is a threat to individual countries and attacks from cyberspace. The greatest difficulty is in the study of incidents causing all the technical details, but the purpose of this paper is less important from a technical than from a sociological point of view, where we will focus on the political, sociological and other reasons, which led to the incident.

Modern countries increasingly rely on information systems, because on the one hand with the development of information society in the country there is also increasing advantage over other countries, and on the other hand, these countries are becoming much more vulnerable and at risk.

Far-back countries and the Alliance did not give a strong focus on threats from cyberspace, which might endanger the national security of each country. Cyber threats were mostly seen as a threat to individuals or organizations and were identified primarily as a criminal offense. For a watershed in terms of threats from cyberspace is true in 2007. At that time, there had been one of the first high-profile cyber attacks that hit the country and its national security - Estonia. In the Estonian case, we can see that it is possible to undermine the country and its national security and its critical and other infrastructure at a distance from cyberspace. The analysis of this incident shows us roughly that in the case of Estonia we had a combination of several negative factors. The attack is the result of an internal dispute between the Estonians and the Estonian citizens of Russian nationality. The cyber attack on Estonia was initially the result of patriotism, which was later used by criminals. For this reason, it is necessary to address this very seriously because it is a multi-faceted and complex example of cyber threats. The cyber attack on Estonia was first uncoordinated but later on the attacks were temporal and organizationally well-designed. The attackers used retention and attrition tactics, on the Estonian side there were defenders, who at first did not know how to act.

The attacks caused partial and total information blockade, which caused delays and inability to organize the defense. In addition to critical infrastructure this has also raised questions about the need to protect other sensitive parts of the civilian infrastructure. Even "non-critical" infrastructure is important, and through it each country is vulnerable. Consequently, the view of the recent past is even more important and necessary. Was Estonia attacked at all, and what was actually going on? At the same time, it is necessary to consider the willingness of country's legal system to deal with cyber threats and to draw attention to the strengths and weaknesses in national legislation (Tikk, Kaska, Vihul 2010, p. 11). Cyber conflict in this case is already defined as a fifth dimension of warfare, which will be needed to pass the Law of Armed Conflict in the cyberspace and require the writing of new rules and laws (Wingfield 2011). This of course means a new era of legal inter-

preting of cyber incidents which may lead to a meaningful application of the law of armed conflict in cyberspace. Of course, it is not easy to carry and use it in cyber space. In this case cyber-space represents imaginary space where different rules apply as in the physical space. Extensive legislation, non-compliance with safety standards and inadequate protocols further weaken the protection against cyber attacks (Lukman, Bernik 2009, p. 10). This can lead to the black scenarios, which ultimately lead to the physical destruction of critical components of information communication technology. Therefore, we can say that the greatest concern in cyberspace is caused by cyber attacks on state law. The examples of such attacks are:

- In June 2010, China launched cyber attacks on companies that have been involved in the U.S. defense industry. At that time the confidential information about the project of the new U.S. fighter F-35 were stolen.
- In July 2009, North Korea carried out a massive attack on the United States and South Korea. It then attacked several websites, including the White House website, information systems NASDAQ, American Stock Exchange and South Korea's financial institutions and other important websites in the USA and South Korea.
- Stuxnet case in 2010 actually represents the first international cyber attack with broader impacts on the nuclear critical infrastructure. In that case, it comes to sophisticated attacks that bypass a series of security barriers in cyberspace. Studies never officially confirmed who was behind it. Some studies have shown that in this case there was not only the temporary neutralization of targets, but also the physical destruction of targets (Concordiam, 2011, p. 10). Due to the sophisticated worm in information systems it is supposed that some of the national governments stand behind it, because only they have enough information and resources. One of the foreseeable Stuxnet targets were Iranian nuclear facilities with the aim of gaining control over all nuclear systems for the implementation of sensitive operations (SCADA). In this case, it was difficult to determine whether a Stuxnet managed to end the destructive action, which it was intended for. The damage to nuclear systems is caused only in Iran, which leaves open the following question: was the target of the attack on the international level or only in Iran? Here arises the question of retaliation or whether Iran can carry out retaliatory measures that could affect critical infrastructure in the USA and its allies, which Iran was accused of to have caused such an incident. One study concludes that Stuxnet was created as a powerful psychological weapon while it was probably very successful (Preliminary Stuxnet report, 2010).
- Even the case of Burma, which was organizing the elections in 2010, experienced a massive scale cyber attack which cut off their citizens from the internet and thus the information, indicates the severity of cyber threats. The attack in Burma was much larger than the attack in Estonia.

All information and various activities from the personal information, information about companies and state institutions to financial transactions and other services that are performed daily in cyberspace, poses a valuable wealth.

Cyber threats require a multifaceted approach to solve the problem. In addition to the security of information systems there is a need to include other areas from the organizational to financial resources, which must be available. For this reason, it is necessary to look in more detail individual incidents and understand the causes that led to cyber-attacks and

the consequences that occurred during and after the attacks. The characteristics of modern cyber incidents are rapid changes in unpredictable environments, which are often the result of political decisions. Everything is accompanied by barriers that are reflected in the lack of national and international laws, the lack of authority for the control and prosecution of cyber crime and the lack of international cooperation, which is not consistent and depends on the "goodwill" of each country. In the current cyber incidents it was not clear how some of the individually suspected countries were involved in the incident.

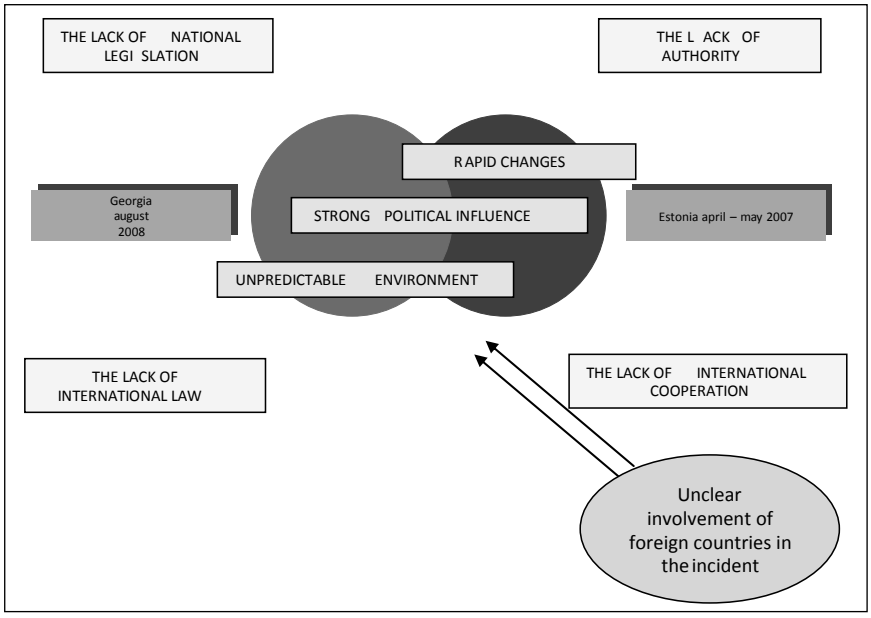


Figure 2: Characteristics of cyber incidents (Source: Own)

In the following we will find the features of cyber incidents that have occurred at the country's level. Good results in this field resulted from the research carried out by Tikk, Kaska and Vihul in 2010, where they explored the cyber attack on Estonia in April and May 2007, the cyber attack on Radio Free Europe/Radio Liberty in Belarus in April 2008, the cyber attack on the Lithuanian online network in June and July 2008 and the cyber attacks on Georgia in August 2008. Estonian and Georgian case will be completed and upgraded with some new insights and reflections. In all cases, we can speak about new incidents, which have a common denominator that took place around the same time period in the wider European area and showed the vulnerability of countries in our immediate vicinity. All incidents have the following common denominators:

1. Rapid change – sudden and rapid changes occurred at incidents, which hampered investigators working on counter-measures.
2. Strong political influence - the incidents destabilized highly domestic and international political environment.
3. Unpredictable environment - all consequences could not be foreseen.

All incidents can be compared due to the same time components. Comparison is also possible because of other identical characteristics, where in addition to policies there are a lot of determined historical facts. Such threats can be classified as asymmetric or asymmetric cyber, if cyberspace is treated as a new dimension, which is entirely man-made. In our opinion, not so far away, we are not too burdened with asymmetric threats, like falling meteors and other cosmic objects, and of course, information and network warfare the threats of which are increasingly switching from imagination into reality.

The development of new technologies is enabling the transfer of major conflicts into the digital environment. Cyber attacks make use of individuals, groups and countries. For this reason, there is an increasing danger of cyber attacks which are not just a problem of individuals and organizations, but the problem of states and alliances.

This is best shown in Estonia, where in 2007 one of the most well-known and high-profile cyber attacks in recent years occurred. And only the incidents in Estonia in summer 2007 finally attract all the political attention to this growing source of threats to public safety and stability of the country.1 Three-week wave of massive cyber attacks showed that NATO States are also very vulnerable from the cyber side. The cyber attacks over a period of three weeks resulted in denial of service to most government and banking websites. Because of these attacks, NATO has recognized that they must put cyber security at the forefront of new security challenges, which will require more work in the future.

2.1 Comparison of incidents in Estonia and Georgia

In 2008, Russian hackers carried out simultaneous attacks on Georgian websites supported by the Russian army in southern Ossetia. When we compare those attacks to the attacks on Estonian websites in 2007, Georgian servers were attacked with much greater intensity, but in short time (Lukman, Bernik, 2008).

2.1.1 The incident in Estonia in 2007

In 2007, Estonia became the first country in the world to be targeted by a large-scale co-ordinated international cyberattack (Kalev, 2013). Estonia, as a member of NATO and the EU at the end of April 2007, experienced an outbreak of violence in the capital city of Tallinn, caused by particular groups of Russian ethnic origin. Unrest caused the decision of Estonian Government to remove from the city center the Soviet monuments from the time of the World War II, which symbolizes the victory of the Soviet army against Germany. Such a decision is then strongly opposed by the Russian side that threatened Estonia and compared it to Nazi Germany. Seemingly insignificant monument immediately became the center of attention of Russian extreme groups in Estonia, which showed open hatred to the Estonian state. In the beginning there was a peaceful protest in Tallinn and other cities across Estonia. But, protests have escalated - there had been looting, destruction of buildings and other violence. One person died, about 100 people were injured, and 1,300 people were imprisoned, which was a big task for the Estonian security forces. The result was also considerable material damage which was estimated at 4.5 million EUR. Because of these events, the Estonian government made a quick decision to remove the

1 "Cyber-attacks are getting more common, more complex, and more dangerous. They come without warning. From anywhere in the world. And they can have devastating consequences." (Anders Fogh Rasmussen – Secretary General of NATO).

statue to an unknown location before it was announced. This decision resulted in protests outside the Estonian Embassy in Moscow. The violence from the streets of Tallinn altered in a "riot" and instigated the attacks in the virtual world, when in the evening of Friday, 27 April 2007, the website of Estonian government institutions came under a wave of cyber attacks. The attacks on public and private websites lasted more than 3 weeks, when the political tensions between Russia and Estonia eased. The violent protests and cyber attacks on Estonia had severe internal and broader international implications.

Estonia is characterized by a small number of residents, low population density and limited resources. For this reason, the Government of Estonia in the early 1990s decided to try by the Internet to ensure the functioning of the country for its citizens. The development of information and communication technologies has been very successful, so that a large proportion of revenues from banking to public transport result from the use of this one. All this provided innovative and comfortable living environment for the Estonian nationals. At the beginning of 2000, there was an online business equivalent to a written document in the administrative proceedings and digital signatures had the same legal effect as handwritten.

Coverage of the Internet was 98% in 2007, and coverage of mobile telephony was practically 100%. The information systems and databases developed national system of information and access to services by the principle of "one-stop-shop". National Information System enabled more than 1,000 different electronic services, the number of individuals with a digital signature reached 70,000. Estonia was the first country in the world to allow voting via the Internet. Old forms of business paper for the citizens of Estonia were the past. All this has made Estonia vulnerable in cases of loss of information and communication resources.

2.1.2 Phases, the main targets and the origin of attack

The cyber-attack was launched on April 27, 2007, parallel with the unrest in the streets of Tallinn. The target of cyber attacks was the IT infrastructure and electronic services of Estonian government institutions. The intensity of the attacks was reduced until the end of May, when a political agreement between Estonia and Russia on the issue of the monument and the interpretation of history started.

The attack had two completely different stages and each stage had more intensity levels. The first phase of the attacks lasted until April 29, 2007. This period is characterized by emotional motivation, the attacks were not coordinated. They were conducted in a relatively simple manner (with simple commands – "pinging" was able to verify the availability of the targeted computers), so they can be referred to as a "cyber riot", which could be easily mitigated. The instructions for the attack were mostly simple and did not require any special technical knowledge to participate in the attack. It was enough to have a computer with an Internet connection. On the first list of possible computers from which they carried out attacks, unexpected countries were found such as Egypt, Vietnam and Peru. They predicted that development in these cases to less protected personal computers that have been abused.

This next stage followed on April 30, 2007, and these attackes were coordinated and much more complex and lasted in four waves until May 18, 2011. The sites became unavailable or denied access to electronic devices, computers, servers, networks and Internet resources

for the target users. The escalation of the intensity of attacks against critical public and private information infrastructure led to the collapse of the network because traffic was at the peak of attacks almost 400 times higher than its normal rate.

The main assets and types of attacks included the denial of services or access to facilities, attacks on servers, disruption, intrusion, breaks and raids on the website, large quantities of unwanted comments and spam, which contained negative propaganda messages, spreading instructions for carrying out the attack. Easy targets for attacks were government mail servers and individual e-mail accounts of public officials, as they were made public for all public servants since 2001. The effects of attacks were seen outside of Estonia. There were disabled queries and foreign users did not know why the normal traffic with Estonia was disrupted.

The main targets of attacks were governmental and private information and distribution channels and websites of the private sector, where the banks were most affected. Vital databases, systems and registers of the public and private sector were not fully blocked, but we can say that it was a direct attack on the national internet infrastructure. The target of attacks was also the 112 Emergency Calls that was blocked for a short time. The attacks can roughly be classified as attacks on servers that support Estonia's Internet infrastructure. The main targets of attacks were:

1. Governmental and political targets, where the websites of the Prime Minister, the President of the State Parliament, the National Audit Office and all ministries, the Estonian border police and some political parties were attacked.
2. Services offered by the private sector, where the websites of Estonian electronic banking of two largest banks were attacked: Hansapank and SEB Eesti Ühispank, which together dominate at 75-80% of the banking market in Estonia. That had serious consequences for the Estonian economy at home and abroad, because in 2007 the share of e-commerce with banks in Estonia ranged from 95 to 97%.
3. Personal and random targets.

However, the information systems, which support the transport and energy systems and represent a conventional part of critical infrastructure, were not targeted by the attacks. The attacks came primarily from abroad. The data collected by Arbor Networks suggest that the attacks were conducted from computers in 178 countries. A substantial part of the attackers were emotionally and politically motivated. When the tension around the monument eased, attacks eased too, although this was not the case for all. In the second stage of attacks the elements of the central management and control were seen, the attacks occurred at specific time intervals, which required large financial and intellectual resources. In the early stage of the attacks many IP addresses were discovered that were coming from Russia and moreover, some of the IP addresses belonged to the Russian state institutions. However, the Russian government denied any involvement, some cyber security experts pointed to the lack of evidence that the official Moscow supported attacks.

During the attacks, Estonia engaged the best experts in the field of information technology in the public and private sectors, who worked 24 hours a day. The coordination in response to the attacks was taken by the CERT[2] organization.

2 Computer Emergency Response Team.

2.1.3 International cooperation in attacks

International co-operation and support during the attack on Estonia was taken by the Ministry of Defence. The EU and NATO were kept informed on the progress of cyber attacks. More nations offered help to limit the attacks on Estonia from their area. The U.S. CERT observers visited Estonia in order to observe the situation and provide assistance and advice in the defense. The U.S. government offered help Estonia to find resources and close the attack. The Finnish CERT observers offered help in providing contacts and finding service providers. When the attackers knew that Estonia cooperated with foreign authorities in order to identify "cyber criminals" and that this would lead to the court, the number of spontaneous attacks decreased.

2.1.4 Effects of attacks

The cyber-attacks on Estonia had a wider social impact and direct impact on their economy. Many sectors ranging from trade to industry were on a daily basis depending on the information and communication channels, so the attacks affected large sectors such as government institutions, banks and media corporations as well as small and medium-size enterprises, which seriously hampered the functioning of the domestic economy. The social impact of attacks was found in dealings between the state and citizens, who were increasingly looking for information on e-government communication channels. The citizens no longer used any channels to search for information other than the Internet. Due to the unavailability of government websites normal communication between government and citizens was affected. Nevertheless, it was estimated that cyber attacks on government websites were not particularly critical, because in a relatively short period of time the attack did not cause major damage to population. Most damage was in tax returns and applications for social assistance and subsidies, so the actual damage was difficult or impossible to determine.

Finally, it is necessary to mention the damage that is incurred by Estonia in the flow and exchange of information with foreign countries. The first piece of information that permeated the rest of the world was about the riots in Estonia and demonstrations against the Estonian embassy in Moscow, so the rest of the first piece of information about the cyber-attack stayed in the background. It was difficult or impossible to assess the damage caused by it.

2.1.5 Legislation and Legal Aspects of the attacks

The cyber-attacks on Estonia were quickly getting wider international attention. In the context of the existing legal acts the Estonian politicians sought parallels with terrorism and conventional forms of warfare. Soon, the Estonian authorities knew that cyber attacks should be considered only as a cyber crime under the applicable Penal Code and researched in accordance with national legislation and international agreements. Cyber crime is certainly one of the most complex forms of crime which is constantly evolving and progressing (Šepec 2010). This is also reflected in Estonia.

The question of Article 5 referring to the Washington Treaty has never been seriously considered. Identifying of the attackers depended on the measures and procedures that have been legally allowed, which excluded the possibility that the ISPs or CERT would try to identify the attackers. According to The Criminal Procedure Act, evidence may be

collected by surveillance in criminal proceedings, if the collection of evidence in other procedural acts is excluded or if it is a criminal offense which is punishable by at least three years imprisonment. The majority of crimes committed in the Estonian cyber incident did not reach the criterion of three-year imprisonment. At the time of the incidents in Estonia the penalty prescribed by law for computer crime was maximum one-year imprisonment or a fine.

The cooperation with Russia, which based on mutual legal assistance beetwen Estonia and Russia in the agreement of 1993, did not yield any results, because the Russians refused to identify the requirements of the IP addresses on the Russian territory on the grounds that the agreement does not define such procedural actions. There was a problematic interpretation of the agreement and the lack of will to cooperate.

The cyber-attacks on Estonia were a great experience in the field of criminal law. Notwithstanding the fact that these attacks were persecuted as "ordinary cyber crime", in these cases it was more than just a series of individual crimes. Estonia changed the form of "cyber" crimes, so they changed the law. Due to the complications that arose in the prosecution, the Ministry of Justice of Estonia established a comprehensive amendment to the Penal Code, which entered into force in February 2008, which listed in detail the provisions relating to attacks on computer systems and data, added new provisions on cybercrime and imposed higher penalties. Among terrorist offenses interference in computer data or disruption of computer systems and threats of such acts are also included, if this was done with intent to compel a State or an international organization to act or omission or to seriously disrupt or destroy the political, constitutional, economic or social structure of the country or seriously disrupt or destroy the functioning of international organizations, or seriously intimidate the population. Estonian law currently deals with cyber crimes, if they are motivated by terrorist targets such as terrorist offenses.

The cyber-attacks have resulted in the adoption of a new cyber security strategy, since they are highly prejudicial to their national security. The strategy was adopted for the period 2008-2013 and is managed by the Ministry of Defence in cooperation with other ministries. The strategy provides a concept and an action plan for the implementation and emphasizes the importance of understanding the security risks posed by asymmetric threats of cyber attacks and the vulnerability of the global cyberspace.

The final result of the attacks on Estonia indicated the ineffectiveness of the regulatory system. Despite the international support and engagement of the entire state apparatus, only one person was sentenced: a student who was praising about these activities at the local forum. All other domestic and international investigations have remained without result.

2.1.6 The incident in Georgia in 2008

The cyber incident in Georgia falls within the timeframe of the armed conflict between Georgia and the Russian Federation, which erupted in August 2008 because of a territorial dispute around the province of South Ossetia. South Ossetia became independent from Georgia in 1991, but the international community still regarded South Ossetia as an integral part of Georgia. For this reason, the OSCE[3] deployed peacekeepers which were comprised of Russian, Georgian and Ossetian armed forces under the Russian command.

3 OSCE – Organization for Security and Cooperation in Europe

After constant provocations by the Ossetian separatists, Georgian armed forces carried out a sudden attack on separatist forces in South Ossetia. The Russian armed forces were quick and forcefully responded to the attack. They had referred to the obligation to protect Russian citizens abroad and occupied the territory of South Ossetia and other parts of Georgian territory. Georgia informed the international community that they were in a state of war and that launched massive mobilization of all forces and other measures to protect national security and sovereignty of Georgia. Such was the state-of-affairs which marked the legal framework for the treatment of cyber attacks on Georgia.

Before the Russian armed attack on Georgia on August 8, 2008, the cyber attacks against a large number of Georgian websites were also launched. The military conflict ended after four days with an agreement on a cease-fire, while cyber-attacks continued until the end of August. Georgia as the information society at that time was not considered to be among the developed countries. Stats of this period show that the Internet was used by only 7% of the population, which is significantly less than in the developed European countries. The major part of the Internet infrastructure has been dependent on Russia, the smaller ones from Turkey and Azerbaijan. Because of this, the potential for dispersal of Internet traffic was very limited. Georgia was at that time a good target for a coordinated cyber attack.

2.1.7 The main targets and the origin of attack

The aim of cyber attacks was to isolate Georgian government and the population of the rest of the world. Tensions in the Georgian-Russian relations were evident in the Georgian cyberspace a few weeks before the Russian attack on Georgia. At that time the website of the President of Georgia was not accessible for a day. The majority of attacks began on August 8, 2008, when the targets of simultaneous attacks were the websites of Georgian President, government websites and the website of the Ministry of Foreign Affairs and the Ministry of Defence. Georgian and other news portals and forums were also attacked. The next day the largest commercial bank of Georgia – TBC was attacked as well. The Georgian government was at that time in the information blockage. Georgia got help from Poland and Estonia, where they transferred a part of their websites and they also got assistance from the experts in the field of information security. On August 10, 2008, the website of Georgian Parliament, the President and other non-governmental websites were attacked again. This time the attack came from the territory of Turkey. Government websites have been blocked for two days, and the website showed the Georgian President Saakashvili equal to Hitler. Georgian Ministry of Foreign Affairs has issued a press release on the Russian cyber attack on Georgia. The last major cyber attack on the Georgian site was launched on August 27, 2008. The main target of the attack was the Ministry of Foreign Affairs. The attacks were successfully blocked until the next day. The cyber attacks on Georgia can be compared with the cyber attacks on Estonia, where similar means and targets of attacks were used. The attacks were aimed at:

- Political and governmental websites – the websites of presidents of state and parliament, the Ministry of Foreign Affairs, Ministry of Science and Education and other;
- Financial websites – the website of the National bank of the Republic of Georgia and the websites of largest commercial bank TBC;
- Public media web sites;
- The Website “Community of Georgian hackers”.

Statistical analysis of the attacks, carried out by Arbor Networks, indicated that in Georgia there were high-intensity attacks, which had an average duration between two and six hours. To attackers were also distributed a list of Georgian politicians and their e-mail addresses to send them spam and targeted attacks. A part of the flow of information and transactions between government and citizens was blocked or interrupted.

Also in the event of cyber attacks on Georgia, there was no evidence of who organized the attacks. Russia is suspected because the attacks took place under the direction and they coordinated with the events in the Georgian-Russian armed conflict. It was confirmed that Russian hacker community was involved in the attacks because of the Russian language and Russian forums. However, there was no evidence to suggest that the Russian government was involved in the attacks, which denied all allegations. A research conducted by the Swedish National Defence College also suggests a link to organized crime with Georgian cyber incidents. In Georgia, there emerged a variety of criminal activities such as forgery of passports and credit cards. Based on the research by Grey Goose Project, the cyber attacks on Georgia held in five phases:

1. Dissemination and promotion of cyber attacks on Georgia;
2. Publication of a list of targets and Georgian websites for access;
3. Selection of types of malicious software for attacks on websites;
4. Start of attacks and attacks;
5. Results and assessment of attacks.

There is no doubt that the attacks that took place were organized and coordinated. Countermeasures implementation is carried by Georgian Group for Information Emergency Incidents (CERT). Georgia also cooperated with international community and moved certain media portals on to hosting world service platform (www.servage.net). Georgia news portal was covered directly by Google. The website of the President and the Ministry of Defence moved to Tulip Systems, Inc., which is located in Atlanta in the USA, the website of the Ministry of Foreign Affairs moved to Estonia. Help was also offered by Poland, where they gave a separate part of its web sites available to the Georgian Government.

The effects of cyber attacks in Georgia were different in comparison with the attacks in Estonia. The effects in Georgia were largely limiting the spread of information on the progress of the Russian military operations, when most Georgians needed the free flow of information. The attacks prevented the implementation of certain public utilities and services. For 10 days the National Bank of Georgia halted the operations of all banks that offered online services. In this context, it should be pointed out that cyber attacks caused significant damage even though they did not have the objective of long-term destruction of the ICT infrastructure.

It was difficult to assess the damage in the case of Georgia, especially since the cyber-attacks took place simultaneously with the armed conflict, which also caused a lot of damage. Precisely for this reason, it was impossible to assess the damage.

Searching for answers at cyber incidents and in accordance with national and international law, we may look at different areas of regulation such as:

- Information and communications regulation,
- Criminal law,
- Law of armed conflict.

International media at this time of the cyber attacks on Georgia quickly dubbed as the cyber war against Georgia. It is necessary to look Georgian cyber incident from the view, when Georgia had a difficult situation, where its territorial integrity was threatened as well as its political independence (use of force, cyber attacke of military targets - the website of the Ministry of Defence). In this case armed conflict cannot be linked with cyber attacks. Not one country currently has "cyber force" that could be used against another country and Russia denied any connection and involvement in the cyber attacks. This makes the application of the Law of armed conflict in cyber attacks on Georgia very problematic, as the case is too vague and does not meet the criteria of government involvement and the severity of the impact.

Another issue that was raised concerning the cyber attacks on Georgia is whether the countries that hosted the Georgian website (Poland, Estonia, and the USA) violated the principle of neutrality of the international law in the Russian-Georgian conflict. The answer is that a neutral State may authorize the use of their telecommunications infrastructure and equipment, and that this does not constitute a violation of the neutrality of the country. Therefore, it appears that it is the question of whether we can use the criminal law to address cyber incidents in Georgia. In terms of dealing with cybercrime, the Council of Europe adopted the Convention on Cybercrime in 2001, which contains both substantive and procedural aspects of the investigation of cyber crimes. Georgia signed the Convention on Cybercrime in April 2008, but by August 2008 it had not ratified it. For this reason, they can only rely on the existing national and procedural laws of Georgia. However, even in this case there was no international cooperation because Russia has not signed the Convention on Cybercrime.

3. CONCLUSIONS

Finally, from both cases we can see that the national security was threatened due to the attacks from cyberspace. Cyber security has become one of the core issues for Estonia and Georgia and also for the international community. States, especially small ones, should identify the threats and vulnerabilities that can threaten the information critical infrastructure. The continuity of functioning of information and communication technology has a decisive impact on the functioning of critical infrastructure as we have seen in these cases.

Small states must take care of information critical infrastructure protection and adopt the legislation which deals with the issue of cyber security. In those terms, legislation should be supplemented or amended at least on a lower level. Many cases show us that the information critical infrastructure of small states is more vulnerable and at risk from cyber space, so they should consider the choice and training of personnel, appropriate information and communication technology and organizational and security measures.

REFERENCES

1. Hanganu, M. (2011). Martime and Fluvial Critical Infrastructure Security, Obtained 13.9.2011 in http://www.ceeol.com.
2. Kalev, A., (2013). The poster child for cybersecurity done right: How Estonia learnt from being under attack, Obtained in http://www.zdnet.com.
3. Lukman, M., Bernik, I. (2009). Threats to critical infrastructure from cyberspace, 10th Slovenian days of criminal justice, UM, College of criminal justice, Ljubljana.
4. Šepec, M., (2010) Changes and innovations in the field of IT/cyber crime in the new Penal Code (PC-1).Obtained in http://www.fvv.uni-mb.si/dv2010/zbornik.
5. The Cyber Security Forum Initiative, (2010). Preliminary Stuxnet report ver. 1.16. Obtained in http://www.csfi.us.
6. Tikk, E., Kaska, K., Vihul, L., International Cyber Incidents: Legal Considerations. Cooperative Cyber Defence Centre of Excellence (CCD COE) Tallinn, Estonia, (2010).
7. Wingfield, C. T. (2000). The Law of Information Conflict: National Security Law in Cyberspace. Aegis Research Corp.

UDC 726.9:75.041.5
ID 176374796

Goran Mandić, Ozren Džigurski, Mladen Milošević
University of Belgrade, Faculty of Security Studies
gmg381@yahoo.com
odzigurski@gmail.com
mladen.milosevic@gmail.com

CRITICAL INFRASTRUCTURE SECURITY AND SOCIAL NETWORKS AND SOCIAL ENGINEERING

Abstract: The systems of Critical Infrastructure (CI) belong to the category of socio-technical systems. Generally, the CI of one state includes the following business and industrial sectors, such as energy systems, transport and distribution networks, telecommunication and information systems, chemical industry and technological systems, agriculture and food industry, banking and financial management systems, public health systems, public administration, etc. Given the significance of the CI systems for the functioning of the state and its business entities, the CI system is very susceptible to various eminent threats imposed by both external and internal factors. Knowing the operational and functional characteristics, as well as their complex functional interdependence, these infrastructure systems require a special approach in defining and implementing their safety and protection.

This paper addresses three aspects of security of CI: the security of SCADA systems as key technology components for the management of CI, social engineering as an important component of security threats to CI and the influence of social networks on the safety of CI, as a higher level of threat and protection of the CI.

Key words: *critical infrastructure, SCADA security, social engineering, social networks*

1. SCADA SYSTEMS AND CRITICAL INFRASTRUCTURE

Industrial Control Systems (ICS) are devices, systems, networks, and controls used to operate and/or automate industrial processes. These devices are commonly found and used in nearly every industry sector, transportation systems, output and transmission of energy, as in many other areas of critical infrastructure systems.

SCADA (Supervisory Control and Data Acquisition) represent systems and/or networks that communicate with the ICS for the purpose of the collection of the necessary data for process monitoring and control units that control processes. As automation continues to evolve and becomes more and more important in the world, the use of ICS/SCADA systems becomes widespread. ICS/SCADA systems are particularly applied in all areas of CI containing process control, such as energy and transportation systems, production and distribution of food and water, chemical industry, etc.

In the domain of CI system, in terms of safety performance, ICS/SCADA systems represent a major problem. Because of the way they are implemented, ICS/SCADA systems are very susceptible to various kinds of physical and logical attacks, that is, the attacks such as unauthorized access to the data and devices in these systems. The reason for this is that the ICS/SCADA systems are usually implemented with a very large number of components that can be distributed over a large area, connected by wires or wirelessly. Within this framework, the SCADA systems are practically the Achilles heel of these categories of CI systems given that they are located in the appropriate places for the purpose of direct collection of data necessary for process control, and can carry out the direct management of individual executive procedural devices. Because of their spatial distribution, these places may be insufficiently secured by various types of unauthorized access and criminal attacks. The Central Control System ICS is usually physically secured enough; however, it is mainly because of the control system that it is endangered by the attacks on unauthorized access to process data for the purpose of process control.

The issues of security and the protection of the SCADA systems, as critical components are investigated for a long time in a period of time, and even though almost all the problems are known and all the best practical solutions in this area have been applied, it is still not possible to achieve the maximum safety of the operation of these systems. One of the crucial reasons for this is the architecture of these systems and their spatial distribution (Krutz, 2006, pp. 7-10).

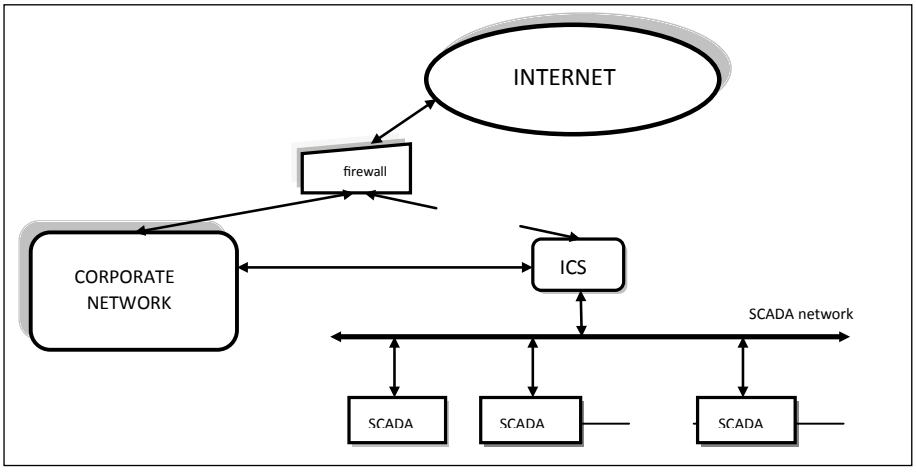


Figure 1- The architecture of the ICS/SCADA system.

The paper further presents possible solutions and recommendations for achieving a high level of security of SCADA systems, as well as the possibility to analyze the achieved level of security and the protection of ICS/SCADA system.

The following specific actions should be taken to increase the security of SCADA networks:

1. Identify all external connections to the SCADA networks;
2. Turn off the unnecessary ties to the SCADA network;
3. Assess and improve the safety of all remaining connections to the SCADA network;

4. Improve the operation of SCADA networks by removing or disabling the unnecessary operational service;
5. Do not use standard protocols for data transfer in order to protect the ICS/SCADA system;
6. Implement the security features that are enabled by the devices recommended by the manufacturer;
7. Establish firm control over all media used for a systematic approach to SCADA networks;
8. Establish a system for the detection of internal and external intrusion in the ICS/SCADA system and establish a continuous monitoring of incidents;
9. Perform technical review of SCADA devices and networks, as well as any other associated networks to identify security problems;
10. Establish physical and technical (FT) control and perform security assessments for all remote devices and systems connected to the SCADA network;
11. Establish SCADA expert teams to identify and evaluate possible attack scenarios on the ICS/SCADA system.

There are also many organizational activities that are mandatory in order to establish an effective cyber security program of ICS/SCADA system.

As can be inferred, a high level of ICS/SCADA systems can be achieved by applying complex activities, systems and security measures and protection. These activities include organizational measures, the implementation of measures to protect access to data via the appropriate logical protection measures, and establishing a system of physical and technical security with multiple levels of protection. In addition, a continuous monitoring of security and functioning of the ICS/SCADA system is necessary. For the analysis of the achieved level of protection of ICS/SCADA system, the penetration test (pen-test) is used. Penetration tests are an integral part of the complete audit (auditing) security system.

Penetration testing belongs to a domain of ethical hacking where appropriate information security experts are hired to perform security attacks to various levels of ICS/SCADA systems, with the aim of discovering all vulnerabilities and gaps in the protection of these systems. The level of protection and all discovered security weaknesses are then recorded and submitted to those responsible for the security of ICS/SCADA system. Effective penetration tests will incorporate the information obtained from the tests with the assessment of potential safety threats to ICS/SCADA system, to carry out a series of technical and procedural countermeasures to reduce security risks.

Despite the intensive application of these recommendations and technical means for the protection of ICS/SCADA systems, there is very little evidence showing the insecurity of ICS/SCADA systems and devices. More important, this trend of uncertainty continues to grow as more and more of these systems and devices are connected to the Internet. Using the internet, you can easily search and find the built-in ICS/SCADA systems that are exposed to the Internet. In addition to Google and other search engines, the attackers can use other websites for this purpose. All this is especially true for ICS/SCADA systems implemented in the past that were and are exposed to the Internet, and did not have any built-in security mechanisms. In addition, these systems, which are numerous, especially in critical infrastructures, are usually not later upgraded in terms of security and protection against unauthorized access, so they become an easy target for the attackers.

For the analysis of vulnerability of ICS/SCADA systems, an IT trap can be applied - a honeypot to detect the attacks on the system. In computer terminology, a honeypot is a trap to detect, deter, or otherwise oppose the attempts of unauthorized use of information systems. Generally, it consists of a computer, data and networks that look like they are part of the core network, but in fact represent their imitation and are monitored in isolation, and seem to contain information or resources of value to the attackers. Honeypot works like intrusion to detection systems (IDS), which are implemented in each instance of ICS/SCADA systems, but in this case virtual and not actual address is used. Honeypot architecture is implemented to fully emulate the real ICS/SCADA system and is used to collect the data on who, when and for what purpose attacks the real ICS/SCADA systems.

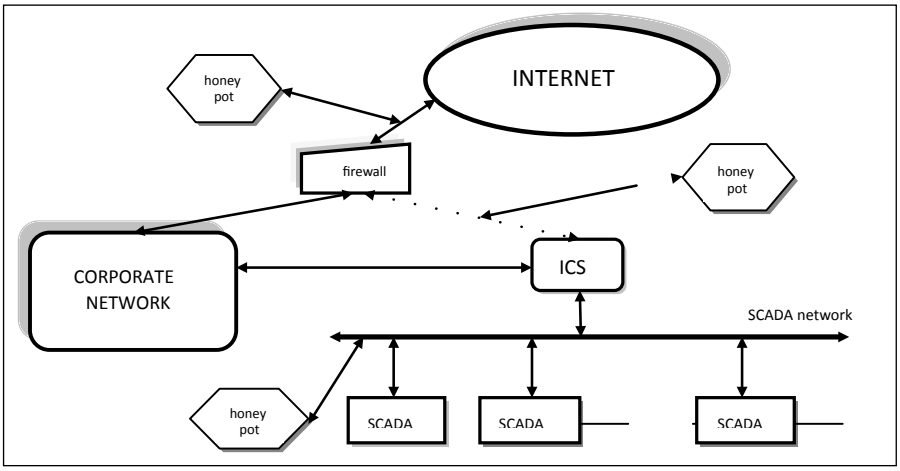


Figure 2 - Honeypot architecture

A research example that can show the effectiveness of this architecture, realized on the Amazon EC2 cloud web service with three instances (Wilhoit, 2013) is used to illustrate the usefulness of honeypot architecture.

As implied, the ICS/SCADA systems exposed to the Internet are relatively an easy target for the attackers. Until adequate security of these systems is implemented, these types of attacks are likely to become very common and destructive in the years to come. However, the origin of the attack and the attacker motivations are not questionable. Continued research must be focused on the motives, the sources of the attacks, the improvement of security techniques and the increasing sophistication of ICS/SCADA system. It is expected that the trend will continue in the area of the attacks on ICS/SCADA system, with possible far-reaching consequences. With continuous efforts and the use of computer-security techniques, the ability to defend from these attacks will help increase the safety of all organizations in the field of critical infrastructure.

2. SOCIAL ENGINEERING AND CRITICAL INFRASTRUCTURE SYSTEMS

Critical infrastructure systems belong to the category of socio-technical systems that can be classified into two main categories. One category is based on the operation using the ICS/SCADA control and process systems. This group contains all the CI systems whose

many components are distributed over a large area in order to manage and control. It primarily relates to energy, transport, industrial and similar systems. The second category of CI systems includes other CI systems whose functioning is not based on the principles of process control, i.e. without the use of ICS/SCADA system. This group is made out of financial systems, medical systems, public administration, etc.

Common to both categories of the CI systems is that they do their operation based mainly on the use of information - communication technologies. Therefore, the security of both categories of the CI system is primarily based and depends on the implementation of the principle of security of information - communication technologies. In terms of protection from security threats in these systems complex physical-technical (FT) protection devices, networks and systems are applied, as well as sophisticated logical protection against unauthorized access to data and all the components of the CI system. However, despite the establishment of a high level of quality, the application of modern FT and logical protection still has certain shortcomings, which leads to the fact that the absolute safety of the CI system cannot be achieved.

The next level and one of the sophisticated ways of security threats of the CI system is the use of social engineering.

Social engineering is based on the application of appropriate procedures that mislead people who are somehow involved in the functioning of the CI system to collect data and information that enable attackers to the system, input and access data and information-communication components of the CI system. In short, social engineering is a form of manipulation of individuals in order to indicate that they do something they normally would not do, and refers to the fulfilment of certain requirements set by the attacker.

Critical infrastructures are vulnerable to the attacks from many angles, including the physical access attacks and attacks carried out over the network. Co-dependence between the infrastructures puts all at risk, so that a successful attack on one part of the system is likely to affect the other parts of the system that are not directly attacked, but are mutually connected (Parker et al., 2004, p. 229).

The attacks of social engineering use human interactive communication, where communication skills are used so that the victim is cheated into doing a compromising thing, such as the disclosure of personal information, or opening e-mail messages that contain malware. Social engineering can be combined with many other methods in order to compromise the security of computer systems. While social engineering attacks are simple and low-tech, they can be surprisingly effective if performed well (Kanellis et al., 2006, p. 16).

The ways of conducting social engineering can methodologically be divided in relation to the presence or absence of communication and contact between the attacker and the attack on:

- The execution by contact;
- The execution without contact, and
- The combined method of execution.

Each mode of execution of social engineering has its advantages and limitations, and a person who successfully uses social engineering achieves their goal by using different methods and procedures. If he feels that his victims are becoming suspicious about testing and access, the person who uses social engineering methods also changes the attack. In the

attack of social engineering, the techniques are often combined (Janczewski et al., 2008, p. 183).

The common techniques (methods) of misleading by Mitnick are:

- Impersonating a colleague;
- Posing as an employee in a service provider company, partner companies or Enforcement Section;
- Posing as someone who is in a higher position;
- Impersonating a new employee who needs help;
- Offers help if it comes to a problem, then causes the problem, which leads to the victim asking help from the attacker;
- Sending the victim a free software or upgrades to install;
- Sending viruses or Trojan horses attached to an e-mail;
- Recording the victim's typing on the keyboard using the computer system or program;
- Leaving the diskettes or compact discs with malicious software at the workplace;
- Use of internal terminology of a specific internal organizational unit in order to gain the person's trust, and ... (Mitnick et al., 2003, p. 334).

All of these techniques can be classified into three main groups:

- False impersonation technique;
- A technique of exploiting negligence, carelessness and ignorance of targets, and
- Technique of reverse social engineering.

It should be noted that the techniques are rarely used alone and that it is usually a combination of two or more techniques. When it comes to CI systems, the use of social engineering is not simple because the CI system structure is usually very complex and the operation is based on expert knowledge and high technology (Gonzalezet al., 2006, pp. 79-90).

Today, after the 11th of September 2001, social engineering is a part of a well organized cyber attack aimed to cause panic with physical attacks on critical infrastructure and facilities, such as companies, water and energy systems (Janczewski et al., 2008, p. 183).

An interesting classification was implemented in the U.S., where they studied and analyzed specific types of groups or organizations that could possibly attack the critical infrastructure of the state or government computer networks. It was found that at the national level, over 100 countries have technology and information prerequisites for this type of attack. At least 20 countries have targeted the United States in the past, and some of them have the same features of information technology and knowledge as the United States (Parker et al., 2004, p. 220).

According to this classification, the following groups are identified as threatening:

- National governments (the rarest threat, but in the case of an attack the biggest damage can be made);
- Terrorists;
- pies, including corporate espionage;
- Organized Crime;
- Insiders, and
- Hackers (the most common threat, but the slightest possibility of damage).

According to this classification, an insider is a person who is not necessarily employed in the legal entity that is under attack. In the context of these threats, insiders are those who have access to computers and computer networks, and have knowledge of the value of the information contained in the legal entity. This group comprises a majority of the employees, but may also include the family members of employees, business partners, customers, suppliers, and, in rare cases competitors.

In terms of threats made to CI with this method, apart from the usual methods and techniques of social engineering, it is necessary for these attackers to have highly professional and practical knowledge of the corresponding domain of critical infrastructure (electronics, IT, telecommunications, technology, energy, etc.). For this reason, this threat is most effectively carried out by a combined approach in the form of synergies of external and internal sources of danger, that is, the employees and the attackers who have no employment relationship with the target of attacks.

However, the attackers first need to learn this expert knowledge, and then to gather further information about the components and entities, which are necessary for the implementation of social engineering. All this requires a very large amount of time, measured in months and years, or requires a serious commitment of teamwork.

In what way is it possible to speed up the preparatory work for the implementation of social engineering? One way is to attempt to insert malicious software, and if it is accepted and activated, it provides the access to CI. Here the technique of exploiting the negligence is used, carelessness and ignorance of targets as well, including: eavesdropping in public places, looking over the shoulder, examining the offices, reviewing the contents of a computer, monitoring an employee entering in the restricted-protected area, looking at waste, installation of malicious programs , phishing...

In addition to phishing, a new term appears, that represents the combined performance of social engineering - Vishing. English title is the abbreviation of Voice (voice) and phishing (phishing). Vishing indicates a criminal activity that uses a combination of voice (actual social engineering contacts) and phishing (the execution of social engineering without contact), where the use of voice makes the targets go to a fake web address (Humphreys, 2008, p. 253).

Because of the complexity of these attacks all the above is usually not enough to speed up the intrusion.

Another way to help speed up these procedures is hiring an insider, someone who works within the CI system and is in some way familiar with the information and operating of the CI system. This person, who has access to system components, may install the malicious software that allows an attacker to enter the system. In case they do not have access, or enough privileges to install the software, an insider can attempt to use social engineering to obtain confidential information for that purpose, an approach to familiar faces from the surroundings is used if those familiar faces are in charge of the operation of the CI systems and in some way can carelessly provide the necessary information about the system.

If an insider does not have access to familiar faces, he/they may try, together with the external source of danger to bring the technique of reverse social engineering.

It is believed that a reverse social engineering attack is the most complicated of them all because it takes a lot of preparation and skills in order to be successfully performed (Gregg,

2006, e-book). Reflected in the fact that the person who carries out social engineering is in their views, knowledge and action, according to the targets, a positive and legitimate person, someone they are looking for information from (Granger, 2001). This technique is the most difficult to detect because the target is contacted by the attacker without doubting his identity as an expert in a particular area (Kee, 2008).

The premise of this technique is in a nutshell reflected on the creation of a problem with the targets by the person who carries out the social engineering or by an insider that is later on invited by the target to resolve the troubleshooting. Of course, in addition to solving the problem the attacker uses the position in which he found himself, moving to locate and retrieve information that were the main target of the attack.

The attack involving these techniques must be well planned and consists of the following three phases:

- Sabotage,
- Promoting of the attacker, and
- Assistance (Nelson, 2001).

Sabotage can be a real problem that exists or suspicion of the targets that there really is a problem. The real problem and the doubt are created by the attackers using other techniques.

Promoting essentially means that the attacker in the first place has the knowledge and skills to solve the problem. For targets that belief can be achieved by previous contacts with the attacker when he assured the target that he was well suited to address these problems, therefore, the targets would address the attackers for help. An attacker can call the target presenting as an employee of the company that supplied hardware or software in question, and give their phone to contact him in case of any problems. Another way of promoting is to make a false report for the target to see on their monitor, saying that an error in the system occurred and to contact the persons who is suitable for the problem solving.

And finally, help providing, when the person who executes the social engineering, in order to solve this problem asks for information from the employee. Since the problem is resolved quickly and professionally, everyone is generally satisfied that the attacker got the information he needed.

Given that there are many examples of successful attacks on CI systems through social engineering, the basic protection from the attacks is by a method of staff training and learning about the methods and techniques of social engineering. This is especially significant for the CI systems implemented in the past, with older generations of technology and the application of simpler safety and protection measures. A particular problem represents the fact that people who now manage the CI systems are not sufficiently familiar with the way of functioning of these systems in the past.

3. SOCIAL NETWORKS AND SYSTEMS OF CRITICAL INFRASTRUCTURE

Another way to speed up the process of coming to confidential information about the CI system is by collecting and analyzing the information from the relevant social networks using the methods of social engineering by contact through social networks and internet chat rooms. Certain people carelessly put confidential information on social networks about themselves, their business, and even about some functional characteristics of ICS/SCADA and other technical systems.

Enforcement of social engineering through social networks is a particular risk for two main reasons. The first greatest danger threatening the execution of this method of social engineering is its variety and changeability. The attacker can falsely present himself through private messages and mislead the target into giving the information he requires. If, however, the attacker estimates that this technique alone will not be effective, he may misrepresent first, then use the target's emotions such as empathy, and make him take a malicious program that will allow him access to all required information. However, if there is not enough time available, the attacker may decide not to waste time on the misrepresentation, but to send a web address with a multimedia content and by its activation the installation of malicious software is initiated. By these examples we can see that this method of execution of social engineering techniques can include all categories, individual or combined, and that all forms of its expression cannot be strictly and precisely predicted. Therefore, the mechanisms of defence (protection) must be flexible, and must include a very detailed training that provides a good understanding of all the aspects of these threats and the ability to recognize it regardless of the method the attacker uses.

Another reason that makes the execution of social engineering through social networks particularly dangerous is the characteristics of users of social networks. A large number of users of these networks present ignorance of the basic rules of personal precautions, and disregard for their own safety, and above all the neglect of the safety of the organization they work for. As a result, the users are highly prone to releasing personal information, disclosure of accurate information about the place of employment and job description, they use the same password for a social network account, as they use for their e mail accounts and work related accounts, etc. These mistakes make it so much easier for the attacker to act, as they allow him to require most of the information, or at least the information necessary for the execution of social engineering, by simple searching through some of the general search engines or social networks. These mistakes also increase the damage when it comes to the attack, because after the execution of social engineering, the attacker has a free passage to all the sites, services and applications that the user is using. Another important characteristic of the users of social networks is that they are by definition open to contact with other users. Communicating and getting to know other people is basically the purpose of social networks, which makes it easy for the attacker, as it excludes the need for finding a way for the target to accept the contact.

The advantage of this method of execution of social engineering is reflected in the minimal cost, failure to discover the identity of the attacker, a great flexibility in the choice of techniques and cooperativeness of the target.

The number of users of social networks, and the number of potential targets, is growing rapidly, which is why the enforcement of social engineering is increasing, and there is no end to it at this moment.

However, the social networks can also have a significant role in the protection of CI in crisis situations, in case of floods, nuclear accidents, epidemics, etc... The social networks and related software can further help in overcoming the major organizational deficiencies, as well as updating and replacing command and control structures, where they are vulnerable to crises.

In addition, the social networks can minimize the impact of crises and speed up the recovery of CI after accidents.

On the other hand, the social networks can be a critical part of the same infrastructure that must be protected. The social networks can be one of the good ways for sharing and gathering of information useful for the operation of CI, and for organizing various activities and engagement of resources to supplement the features of the CI (e-government can be used as an example). The new reality is that more and more connecting of physical networks of CI and social networks are realized, which can lead to security threats due to their interdependence, and due to the impact of various factors, requirements and restrictions (major energy and telecommunication systems can be used as an example).

However, the problem may appear if when the crisis occurs, the social networks which in the function of infrastructure are dangerous for the society and the economy (and dependent on each other), were attacked or disabled. The lack of information, the submission of false information and the loss of contacts from the social network may impair their ability to respond in emergency situations and lead to the delays in the operation of CI. In these situations, methodologies and techniques that have been developed for "traditional" critical infrastructure are not usually able to deal with the crisis of social networks. One reason may be that, in this case, it is not possible to organize emergency procedures for the recovery of social networks.

Particular problems when it comes to the security of the CI are anti-social networks that are created for the purpose of destabilizing the system CI (Chai et al., 2008, pp. 256-273). The founders of these networks can be a variety of criminal and terrorist groups, and even individual states that want disempowering the CI of other hostile countries, although this is usually not easily proved. Within these networks an exchange of information is performed in order to attack the CI systems, their security flaws, vulnerable targets, functioning, responsible individuals, etc. Also, the development of Cloud network infrastructure for the support of social networking has enabled the availability of command architecture and control servers that coordinate these malicious attacks. The nature of such architecture makes it more difficult to determine who owns and who controls these systems.

Here are some of the ways that the social networks increase the safety of CI. This is primarily related to:

- Risk assessment - identify vulnerabilities of CI and categorize social networks as a new security threat;
- Monitoring - monitoring the social and anti-social networks that are potential sources of attacks on CI;
- Early warning – the use of social networks for monitoring of potential targets of CI and respond to early warnings and signs of an attack;
- Forensic analysis – the analysis and decision making in real time on recognizing the signs of a distributed attack on CI; and,
- Information sharing - sharing of information and exchange between the actors involved in functioning and safety of CI, the public and private sectors and others about previous accidents, vulnerabilities and protection options of the CI system.

Based on the previously stated possibility of threats and the protection of CI through the social networks, it can be concluded that this security aspect of co-depending of CI and social networks, has not been sufficiently studied and applied in regards of the protection of CI. For this reason, in the future research, in addition to security threats, it is necessary first of all to identify the safety measures that will minimize the threat to the future secu-

rity of the system CI, and are caused by the "dark side" of the social networks. The reason for this may be a sudden development, dissemination and use of social networks in all directions and areas, and therefore, their impact on the security of the system CI is obvious.

REFERENCES

1. Krutz, R. (2006). *Securing SCADA Systems*, Wiley Publishing Inc, USA
2. Wilhoit, K. (2013). *Who's Really Attacking Your ICS Equipment*?, Trend Micro Incorporated, Research Paper
3. Gonzalez, J., Sarriegi, J., Gurutxaga, A. (2006). *A Framework for Conceptualizing Social Engineering Attacks*, First International Workshop, CRITIS 2006, Samos, Greece
4. Chai, C,-L, Liu, X., Zhang, J.W., Liu, D., Dyachuk, D., Deters, R. (2008). *Social network analysis of the vulnerabilities of interdependent critical infrastructures*, International Journal of Critical Infrastructures, Vol. 4, No. 3
5. Kanellis, P., Kiountouzis, E., Kolokotronis, N., Martakos, D. (2006). *Digital crime and forensic science in cyberspace,* Idea Group Publishing (an imprint of Idea Group Inc.), Hershey – London
6. Janczewski, J. L., Colarik, M. A. (2008). *Cyber Warfare and Cyber Terrorism,* Information Science Reference, Hershey - New York
7. Mitnik, D. K., Sajmon, L. V. (2003). *Umetnost obmane*, Mikro knjiga, Beograd
8. Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management, Information Security Technical Report, Volume 13, Issue 4, November 2008.
9. Kee, J. (2008). *Social Engineering: Manipulating the Source*, April 28th 2008, http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-manipulating-source_32914, Accessed on 22.07.2013.
10. Nelson, R.: *Methods of Hacking: Social Engineering*, http://sodaphish.com/files/ebks/try2innovate.com/downloads/E-books/Hacking/Methods%20of%20Hacking%20-%20Social%20Engineering.pdf, Accessed on 25.04.2012.

UDC 726.9:75.041.5
ID 176374796

Marjan Marjanović
Security Guard Montenegro
marjan@securityguardmn.com

Ivan Nađ
University of Applied Sciensis, Velika Gorica
ivan.nadj@vvg.hr

ASSESSMENT OF THREATS TO CRITICAL INFRASTRUCTURE FACILITIES FROM SERIOUS AND ORGANIZED CRIME

Abstract: From social and economic perspective the protection of critical infrastructure is the basic element for maintaining vital social functions. The need for the selection of optimal and appropriate measures of protection and security requires a necessary setting of the frame for the estimate of protection of a critical infrastructure and the estimate of the risk of this action. In the present time, when it comes to most of the objects with critical infrastructure, there are still not enough measures of protection taken against serious and organized crime, as one segment that should be dealt with in the analysis of risks and the evaluation of data for it. The basic forms of possible endangerment of facilities which can result in bigger or smaller damages, and which are in the immediate domain of physical and technical protection are different forms of terrorist action, sabotage, diversions, explosions, fires, breaking-and-entering and robberies, larceny, and industrial espionage. Confronting all forms of serious and organized crime includes, based on the data gathered by the actions of criminal and intelligence agencies, defining the most efficient strategies for opposing masterminds of serious and organized crime. The model of evaluation of these threats is presented in this paper which is developed in the EU under the name of "SOCTA", as well as two key methods of data analyses – PESTLE AND SWOT, which can be one of the possible models for evaluation of endangerment of objects with critical infrastructure. The authors in the article put special emphasis on the fact that the evaluation of endangerment of critical infrastructure from serious and organized crime is, in their opinion, a neglected segment of preventive actions in literature. Therefore, in that context, they are suggesting a more active approach to the study of this matter with the goal of improving the protection of objects with critical infrastructure.

Key words: *evaluation of endangerment, critical infrastructure, serious and organized crime, threat evaluation, data gathering, intelligence analysis, data evaluation, evaluation of sources, SOCTA, PESTLE, SWOT, analyses and analyses of concurrent hypothesis.*

1. INTRODUCTION

The development of events affecting international security sector has led to an increased number of challenges and threats. The changes and events that have a high degree of uncertainty, unpredictability and discontinuity dominate. Most countries depend on critical infrastructure such as energy, water supply, banking, commercial communications, manufacturing and transportation. The vulnerability of critical infrastructure is demonstrated through ratio of possibility of real threat to critical infrastructure components and the system's ability to deal with these threats.

The analysis of factors of endangerment is based on the mutual understanding of different dangers which could have serious consequences on the functioning of elements of the system and their interaction. In accordance with the guideline EC 114/2008 from December 8th of 2008, "Risk analysis represents an analysis of the scenario of significant threats, in order to assess the endangerment and potential impact on critical infrastructure". The elements of infrastructure are now more often subjected to human error, weather conditions and natural causes, physical attacks and cyber attacks. Each of these threats, caused at some point, has a potential to cause serious and long term consequences. Potential threats can be materialized in a wide range of threats, such as international terrorism, serious and organized crime or pandemic. Globalization, climate changes, urbanization, current economic crises, as well as the demographic growth and its socio-economic consequences, are raising potential present threats which represent a security risk for critical infrastructure (Cornelis, 2004). There is a realistic assessment that frequency and severity of incidents on critical infrastructure will rise in the future (Maliszewski, 2008).

The fact that modern society today entirely depends on technology makes it more vulnerable from the perspective of security, and risks and threats to the uninterrupted functioning of critical infrastructure are therefore multiplied and it definitely increases the high expenses of proper security for CI. The protection of critical infrastructure requires the ability to identify and follow critical elements and to determine when and if the elements of CI are under attack, or whether they are subjected to a destructive natural occurrence. A possible methodology which helps in the identification of the necessary capacities needed to confront the special threats includes (Smedts, 2011):

- The identification of basic infrastructure, which is of key importance for the uninterrupted functioning of society;
- Threats evaluation: proactive identification of elements of critical infrastructure (CI), as well as taking into consideration the future trends. In this phase an analysis of proper intelligence information is necessary;
- Endangerment evaluation: determining the effects of an incident on CI, taking into consideration the vulnerability of existing facilities;
- Risk evaluation: it is necessary to create a list of existing credible risks, depending on potential risks in terms of their cause, nature, potential targets, as well as an evaluation of influence.

Economic subjects are always a target and they are exploited by professional criminals. Potential losses are measured in billions of dollars each year. While some criminal groups specialize in certain criminal activity, a significant number of criminal groups, especially larger and more stable, are involved in two or more profitable criminal activities. The evaluation of threats from serious and organized crime (SOCA) deals with serious and organized crime which influences Europe and its citizens.

2. SOCTA METHODOLOGY

SOCTA Methodology was developed by Europol in cooperation with the expert group SOCTA (consisting of the EU member states (MS), EUROPOL third partner countries and organizations, the European Commission and the Council General Secretariat), on the basis of pre-determined SOCTA user requirements (SOCTA 12983/1/11 REV 1.). Based on user requirements, Europol has determined the purpose and scope of SOCTA,

and they have been adopted by COSI in October 2011. SOCTA provides an overview of current and future threats posed by SOC. In addition to current and future threats, it contains a limited analysis of future trends, which may be taken into account for the assessment and lead to the "Watch List" of likely threats to follow.

The methodology within SOCTA is generally the synthesis and simplification of several similar methods used in police work. The traditional intelligence cycle has five main stages that are used as the basis for a step-by-step approach. During the SOCTA analysis process, the goal is to provide a complete assessment of SOC threats, including:

- The factors that are relevant to the SOC;
- the impact of SOC;
- The groups and networks operating in the SOC;
- Intelligence deficiencies/gaps, and
- The recommendations from the key threats.

Intelligence analysis and assessment differ from scientific research. In scientific research, the main objective is to gain knowledge on the chosen topic. The intelligence analysis objective is to find out what happened, what is happening now or might happen in the future. Also, as opposed to scientific research, in intelligence analysis the speed, confidentiality and professional confidence are extremely important. This has an impact on the assessment in the identification and interpretation of indicators for specific situations and events.

The concept of threat assessment of serious and organized crime, based on intelligence data, must be clearly defined and agreed on:

- Methods for registering received information
  - information should be given a unique reference number (URN), which is recorded in some form of a register or database
  - Methods for storing information
  - information should be recorded and stored in a safe manner
  - electronic databases, or even several interconnected databases
- Methods for downloading important information
  - to ensure that all the relevant information can be quickly reached
  - information should be found by the major identified categories, for example human trafficking, corruption, legislation, etc. It is quite possible that one document can and should be selected in several categories.
- Methods for recording, classification (Council Framework Decision 2008/841/JHA of 24 October 2008) and distribution of information
  - that all received information is handled properly in accordance to relevant, national data protection legislation
  - information should be recorded and limitations imposed by labels for Classification or Manipulation should be respected
- Methods of evaluating information
  - assessment of information sources, and accuracy of information itself
- Terms, to avoid controversial interpretations and disputes.

SOCTA methodology consists of four steps: focus, tools, analysis and assessment and result.

2.1. SOCTA Analysis

SOCTA analysis is based on the following three points: OCG, SOC areas and environments on which they have effect, and in which they have facilitated access. These three points are also starting points for data collection.

2.1.1. Organized criminal group (OCG)

For the purposes of SOCTA, Framework Decisions on Organized Crime dated 24 October 2008 (Ibid) should be used, which defines "criminal organization" as "*a structured association, established during a certain time period by more than two persons acting together in order to commit criminal offenses which are punishable by imprisonment or a detention order of at least four years or more, to obtain, directly or indirectly, a financial or other material benefits*."

Structured association means "*an association that is not randomly formed for the immediate commission of a criminal offense, or it needs to have formally defined roles for its members, continuity of its membership or a developed structure"* (Ibid).

In accordance with this definition, the following list of criteria is applied to OCG[1]:

- Cooperation of more than two persons;
- Longer or indefinite period of time;
- Suspected or convicted of a serious criminal offense (*punishable by a prison sentence of at least four years or more* - for organized crime);
- *Acquiring, directly or indirectly, financial or other material benefits, and*
- Operates/works at the international level in and/or out of the EU member states.

Severe form of criminal offense refers to criminal activities which are considered serious and worthy of reporting, and do not meet the definition of OCG from 2008 Framework Decision of criminal conspiracy, and practically also apply to lone actors or individual actions.

2.1.2. Areas of serious and organized crime (SOC areas)

SOC areas are specific sets of criminal activities[2], committed by the OCG as well as sets of criminal activities which are serious because of international dimension, or their impact. Europol Council Decision provides a wide (but not exhaustive) list of serious criminal activities.[3]

In addition, the criminal offenses that should be treated are all forms of organized crime, covered by organized criminal groups and networks of all kinds and may include also individual criminals.

---

1 OCG structures vary significantly and a large number of groups is divided between strickt hierarchy and loose web of criminals. For the use of SOCTA, every type of OCG are analysed providing that they correspond to the definition stated above.

2 Criminal area includes criminal markets.

3 Europol council decision: illegal drug trafficking, illegal activities of money laundering, crime including nuclear and radioactive materials, smuggling of illegal immigrants, human trafficking, vehicle crime, homicides, serious bodily injuries, illegal trafficking of human organs and tissue, kidnapping, illegal deprivation of liberty and taking of hostages, organized robbery, unauthorized trafficking of cultural goods, including antiquities and works of art, deception and fraud, racketeering and extortions, forgery and piracy, forgery of personal documents and its trafficking, forgery of money and others means of payment, computer crime, corruption, illegal trafficking of arms, amunition and explosives, illegal trafficking of endangered animal species, illegal trafficking of endangered plants, environmental crime, unauthorized trafficking of hormonic substances and other growth promoters.

2.1.3. The environment

For a better understanding of future threats, it is essential to consider the wider environment. Criminal activities are embedded in larger environments and changes in the OCG and SOC areas often reflect adjustment of leaders/helpers, vulnerability and/or opportunities in the immediate or wider environment and these changes are tracked as relevant crime factors (RCF).

Systematic analysis of the environment determines what is constant and what has changed, what is changing and what can be changed in the future, and thus helps in detecting early signs of potentially important events. Detailed scan of the environment provides a basis for the development of recommended priorities and strategies for the fight against TOC.

In order to assess the threats in the environment, three types of indicators are being used:

- OCG indicators (16);
- The indicators of SOC areas (11);
- Effect indicators (6).

In addition to these three types of indicators, relevant factors of crime (RCF) are also being analyzed. RFK are mitigating factors and vulnerabilities in the environment that have an impact on current and future opportunities and barriers to the OCG and the SOC areas. RCF is analyzed through scanning the horizon, which aims to identify future trends in society and the future threats from crime.

Current and future threats are being evaluated by using indicators and RCF. Combined, indicators and RCF help us to answer the following four questions:

- What OCG (or OCG types) are the most dangerous and why?
- What SOC areas are progressing, and why?
- Where have these activities and their effects been noticed?
- Which changes in the environment affect the SOC, and why?

2.2. Analysis and assessment of operational information

The evaluation of sources reliability and data accuracy is the weakest link in the operational information analysis. This fact creates big issues for persons who work with operational information in terms of doubts about the reliability and accuracy of the information, and hence possible errors in reaching conclusions or decisions.

2.2.1 Data Collection

Data collection must be focused and accomplished by public and secret funds and by using all available resources. Data collection depends on defining of the set task and information request analysis. One of the key skills in the analysis is to identify and find the right kind of information, or information that will contribute to assess the scale and impact of serious and organized crime on society.

Baseline:

- Available data within Europol: Europol database content (AWF)[4] for SOC. The information is combined with SCAN Europol on new and innovative trends of threats, assessments of specific threats and other strategic reports developed by Europol.

4 AWF: AWF is a database of specific criminal area which is inextricably linked with specific forms of operating support provided by Europol. AWF is the only existing legal instrument in the area of Europe for storing, processing

- Open sources intelligence (OSINT) for scanning the crime environment.

This analysis will provide an immediate, but not a complete picture of the state of SOC. The results of this preliminary analysis will identify intelligence gaps and help develop specific intelligence requirements.

In the first phase of data collection the sources are being defined (type of information and available information resources vary from country to country):

- The law enforcement authorities and related agencies;
- Public Administration and Local Self-Government;
- Open sources;
- The academic community;
- Private companies;
- Non-governmental organizations (NGO);
- International organizations (IO);
- Subject matter experts.

2.2.2. Data Sources

SOCTA is using data available within Europol, provided by Member States through a questionnaire and from third countries and organizations. In addition to these, it uses materials available from open available sources, except dubious sources, tabloid press or similar articles. OSINT that is inconsistent with the information provided by the MS is compared to other included members. Open sources are:

- Reports of public organizations, primarily NGOs;
- Feedback from the private sector;
- Scientific reports;
- Other sources, including journals, magazines, news agencies and newspapers;
- EU and other official (government) documentation (e.g. decisions, declarations, general reports and newsletters, minutes and supporting documents).

The reference list of all sources used for the purposes of SOCTA must be in the annex to the report.

2.2.3. Data and sources evaluation

In general, the information is evaluated by using the "Four x Four (4x4)" matrix, where the source and information are being evaluated independently, and to each combination of source and its information is assigned a value within the range from A1 to X4.

and analysing information ("hard" data) and especially "intelligence" (or "soft" data), including, at the same time, personal data of delicate nature. All data are available for analyses.

Figure 5: Information assessment matrix (Own source, 2013)

A where there is no doubt about the authenticity, reliability and competence of the source, or if the information is obtained from sources that in the past had been proved to be reliable in all cases	A4	A3	A2	**A1**
B source from which information is obtained in most cases proved to be reliable	**B4**	**B3**	**B2**	**B1**
C source from which the information is obtained in most cases proved to be unreliable	**C4**	**C3**	**C2**	**C1**
X reliability of the source cannot be estimated or there is suspicion in the reliability, authenticity and competence of the source	**X4**	**X3**	**X2**	**X1**
	4 Information for which the source is unknown and cannot be supported by other reliable information. Information not known personally to the source and cannot be substantiated by other already verified information.	**3** Information source is unknown, but it is corroborated by other already verified information. Information is not personally known to the source but it is supported by other already verified information.	**2** Information source is known, but not where it came from. Information is personally known to the source, but it is not known to the police officer.	**1** Information the accuracy of which is not questionable. The police officer knows for a fact that the information is true. Personally known to the police officer.

After using the 4x4 matrix, the data sources used for SOCTA are ranked:

- A1, A2, B1, B2 are considered as “confirmed” information,
- While all the others are “unconfirmed” and “unverified” information.

Information deemed as "unconfirmed" and "unverified" need to be further verified in order to raise their accuracy rank or to confirm them as unfit for evaluation.

However, Europol does not use this method to evaluate all received data. Some partners are considered sufficiently reliable to provide information that they consider being of the highest quality and they automatically evaluate them as such. That includes: "Europol information: A1" MS information: A1 (exception may be made if there is an explicit reason to reduce the status of the resources and/or information, e.g. the investigation is ongoing, and all information has not been verified); "Information from the EU Institutions (EUROJUST, FRONTEKS): A1; automatic acceptance of information from the Member States and EU agencies provides a way for unproved or unreliable data to become accepted as "A1" as Europol has no authority to investigate whether the assessment process at the national level or in EU agencies meet the required standards.

Other sources are being carefully examined: "status of information from gray literature and other open sources can be anything between A1 and X4" and there are no "sources that are immediately rejected, except tabloids and other news articles or similar."

Information that can be used for SOCTA must have grade B3 or higher (A1, A2, A3, B1, B2, B3), this means that the source material which does not even meet the standards for "confirmed information" is being used.

Data classified as A3 (source is unknown, but there is no doubt about the authenticity, reliability and competence of the source, and their information is corroborated by other sources), or B3 (source of the information is unknown, but it is corroborated by other already verified information and the source from whom the information was obtained in most cases has proved to be reliable) can be used in preparation of the "threat assessment" document, which will be the basis for a coordinated and operative action by the member States police and EU agencies.

This is stated because exactly those sources serve us as the baseline data and it is our opinion that they should be taken with a certain amount of doubt and they should be checked within the possibilities (what is related to the local problem).

The evaluation of the data is the most sensitive and very important step in making the threat assessment of serious and organized crime, as if our input data are wrong, the analysis results and recommendations may be completely wrong.

By assessment we determine how much the source is reliable and how much the data itself is correct, i.e. we quantify the data and its value to us, because only evaluated, confirmed, indexed and classified data makes information usable.

During the evaluation process, we must follow two basic principles:

- The assessment must be based solely on an objective professional judgment, i.e. the assessment should not be affected by personal attitudes, prejudices or emotions.
- Evaluation of reliability of sources is always done separately from the assessment of the data accuracy, and these are actually the steps of the assessment process.

It is very important that the assessment of the reliability and accuracy of the source is done only by a person who found out certain information (law enforcement official, undercover agent), because only he can know who is the source and what is its previous reliability and how accurate the obtained information is. We must be aware that the personal assessment is a double-edged sword, but we still have to rely on their integrity, professionalism, impartiality and morality.

Examples:

1	
Information	**I saw Marko Markovic takes the package that he was handed by an unknown person, whom I did not get a good look at, from the car Audi with unknown plates**
Source	Police officer P. P.
Assessment	A1 . Source is reliable (policeman) and information is obtained **by direct observation of the source.**
2	
Information	We have information that members of the Belgrade clan visited their close associates in Bar.
Source	Daily newspaper Vijesti
Assessment	X 3. The information comes from an open source that cannot be easily assessed, but the information can be verified from other sources.
3	
Information	Unknown criminal group uses encrypted phones to communicate with other gang members. I know, because I've seen these phones.
Source	Mister Pero Perić (most frequently unreliable source)
Assessment	C2. The source is unreliable. Information is personally known to the source.
4	
Information	Unknown criminal group uses encrypted phones to communicate with other gang members. I know, because I've seen these phones.
Source	Mister Miro Mirić (most frequently reliable source)
Assessment	B2. The source is reliable. Information is personally known to the source.
5	
Information	Fifty-six people were prosecuted for trafficking criminal offenses in 2010, which is an increase of 25 percent compared to 2009.
Source	Annual report of the Prosecution
Assessment	A1 or B2. The source is the annual report of the Prosecution which is as some claim fully accurate source (A), while others argue that it is most often the correct source (B). Given information, therefore, can be considered as true, without a doubt (1) or known personally to the source but not to the official operator (2).
6	
Information	An organized group of Pero Peric is preparing a bank robbery in the shopping centre Camellia in Kotor.
Source	Police informer AO22

Assessment	B3. The source is most often accurate (B) source from which the information in most cases proved to be reliable; the information is assessed by (3). Information is unknown personally to the source, but is already supported by other reliable information, because they have information about the activities of an organized group led by Pero Peric.

From these examples we can conclude that the source and data assessment is not an exact science, but the experience, knowledge and opinion play and will always play a significant role in this process.

The above examples are pieces of simple and unambiguous information. If the information is of a complex type and refers to the number of segments or faces, each piece of information is separately evaluated.

Example of border police report:

On August 21st 2010, on the border crossing "NN" between country X and country Y car brand Volkswagen with license plates abcd123 was stopped and searched. In a hidden compartment beneath the rear seat four AK-47 automatic rifles with 10,000 rounds were found. A1

By checking the car it was found that it is registered to associate of a known drug trafficker, who is a member of an organized criminal group NN (OCG), which operates from the country Z. B2

This OCG is suspected to control a number of corrupt police and customs members in the country Z. X4

This report has been assessed in three parts and to each part a rank was assigned.

The analysis represents establishment of the connections and interpretation of information and/or intelligence information from various sources to detect pattern and meaning (Andrews and Peterson, 1990). Data analysis and indicators assessment is the essence of the analysis process. The goal of the analysis is to develop the most accurate and most valid possible conclusions based on the information and thus come to the key threats.

In fact, some analyses have already been conducted during the process of defining the task, by accepting the terms of reference and the beginning of collection, processing and evaluation. However, in this fourth phase of the intelligence cycle, analysis method is fully implemented.

For a complete analysis we need to scan the environment, and that is the process of collecting factual and subjective information on the environment we analyze. Two analysis techniques that complement each other are PESTL and SWOT. We also need to know that each country has its own key environmental factors.

2.3. PESTEL

PESTEL is the analysis of certain environmental factors that can have an impact on crime and law enforcement. The letters stand for political, economic, social, technological, environmental and legislative factors. The method considers each of these areas and identifies the elements that may have an impact on law enforcement.

PESTEL is a method of identifying key environmental factors. They vary from country to country, and as a result some elements can be combined, others can be omitted and new

ones introduced. Thus the key legal factor may be the issue of human trafficking, a key social factor may be demographic issue and one of the most important economic factors can be average earnings of the population.

2.4. SWOT analysis

SWOT environmental analysis is often used as a logical compliment to the PESTEL analysis. SWOT stands for strengths, weaknesses, opportunities and threats. After making PESTEL analysis, analyst will reveal some of the key "initiators" of serious and organized crime. SWOT analysis is applied to help in assessing how serious and organized crime can use these initiators and what can be a barrier in reducing their ability to use them. The part of this analysis - strengths and weaknesses - is focused on the strengths and weaknesses of the organized criminal group (OCG) and the part - opportunities and threats - is focused on the possibilities and threats that the environment provides.

SWOT analysis technique can also be used on the law enforcement authorities, to examine its own internal strengths and weaknesses and the possibilities and threats which exist in the environment, in the fight against serious and organized crime.

Using the above PESTEL and SWOT techniques, analyst will now have the arguments to cover the characteristics of a good inductive analysis that reflects the meaning of the data and goes "beyond the facts" in order to provide insight into the phenomenon.

For example:

Fact: Drago Dragić is linked to known criminals.

Fact: Drago Dragić has no visible income.

Fact: Drago Dragić has a very lavish lifestyle.

Conclusion: Drago Dragić makes money on criminal (inductive reasoning).

This is known as inductive reasoning, where the statement may be true, given the facts from which it was derived. It is possible that Drago Dragić won the lottery, received an inheritance or has rich parents. A number of related conclusions are then used to create the heart of analysis, and hypothesis.

Statement: Drago Dragić makes money on criminal.

Statement: Most of the associates of Drago Dragić are linked to drugs.

Statement: Drago Dragić owns a little yacht which his son regularly uses.

Hypothesis: Drago Dragić organizes import of drugs using yacht operated by his son.

Hypothesis should now be tested in an attempt to prove or disprove its validity, and this may require further data collection. The analyst should attempt to identify alternative hypotheses with the same information. This helps to avoid unnecessary bias considering a single option. This is known as **Analysis of competing hypothesis (ACH)**. The development and testing of a hypothesis is the focus of the analysis and finally all recommendations will be made about the hypothesis that the analyst gives.

The methodological approach is used to make a report on the situation using information from various sources. Brainstorming is used to identify serious and organized crime groups and the type of crime in which they are involved. With PESTEL analysis key national environmental factors are being determined which contribute to the existence of

these criminal groups and types of crime. SWOT analysis, using previously identified criminal groups, common features, and criminal business, combined with market analysis helps in determining conditions that allow the entry of criminal groups in the market.

This is achieved by combining different analytical techniques. Further data collection was conducted by intelligence methods in areas where gaps/deficiencies were identified.

Without quality assessment, source reliability and data accuracy, it is impossible with certainty to consider the collected information, because we do not know whether it is true, and therefore is useless for us. Based on this initial facts it is almost impossible to make a proper conclusion or the right decision on the basis of collected data. The subject of analysis is a wide area, national differences are big, and therefore special analytical skills are necessary so they need to provide detailed training for those who are expected to evaluate and analyze information and make useful reports.

3. CONCLUSION

Systems and infrastructure elements networks earlier were physically and logically independent and separated and had little interaction or connection to other infrastructure sectors. With technology progress, the systems within each sector have become automated and connected to each other via computer and communication facilities. Although this connection of systems and elements, and automation increase efficiency, they also make them more susceptible to interruptions and attacks. This interdependent and interconnected infrastructure is more vulnerable to disruptions. In the past, incident that would be isolated now can cause major disruption due to cascade effects (Givens, 2011).

Organized crime is a serious threat to critical infrastructure, especially for the sectors of finance and communications. Organized criminal groups that acquire specialized skills and professionalized business practices, whether related to theft, hacking or denial of service of vital systems are becoming a very real threat to society. The fight against serious and organized crime requires a multidisciplinary approach to intelligence data in order to identify this global phenomenon and provide effective and long-term results. One of the responses to the SOC is SOCTA.

The methodological approach is used to create report on the situation using information from various sources. Brainstorming is used to identify serious and organized crime groups and the types of crime in which they are involved. By PESTEL analysis key national environmental factors are determined which enable the existence of these criminal groups and types of crime. SWOT analysis, using previously identified criminal groups, common features, and criminal business combined with market analysis helps in determining conditions that allow the entry of criminal groups on the market.

This is achieved by a combination of different analytical techniques. Further data collection is conducted by intelligence methods in areas where gaps/deficiencies have been identified.

Without quality assessment, sources reliability and data accuracy, it is impossible to safely consider the collected data, because we do not know whether it is true, and therefore is useless for us. Based on these initial facts, it is almost impossible to make the correct conclusion or the right decision on the basis of collected data. The subject of analysis is a wide area, national differences are big therefore special analytical skills are necessary, so

they need to provide detailed training for those who are expected to evaluate and analyze information and make useful reports.

Rapid changes and the emergence of non-state actors in the security system contribute to the state's monopoly over the protection of critical infrastructure to be divided between experts, academic community, professional associations and technological community, the business sector and non-profit organizations. Private security companies need to increase the capacity and quality of their products and services. It is the only way for them to become a key part of the public-private partnership in the area of critical infrastructure protection.

4. ABBREVIATION LIST

AWF	Analytical work files
COSI	Committee of operative cooperation for internal security
UD	User demands
CI	Critical infrastructure
RCF	Relevant crime factors
LBS	Legal business structure
EMPACT	Multidisciplinary European platform against criminal threats
IR	Intelligence requests
MS	Member States
OCG	Organized criminal group
OCTA	Organized crime threat assessment
PESTEL	Political, economic, social, technological, environmental, legal
SOC	Serious and organized crime
SOCTA	Serious and organized crime threat assessment

5. REFERENCES

1. 12983/1/11 REV 1 COSI 56 ENFOPOL 246 CRIMORG 110 ENFOCUSTOM 78.
2. 15358/10 COSI 69 ENFOPOL 298 CRIMORG 185 ENFOCUSTOM 94.
3. Andrews P. P., Peterson M. B. Criminal Intelligence Analysis, Loomis, CA: Palmer Press, USA, 1990.
4. Cornelis B., Federal Risk Inventory, Survey and Knowledge building, SPIRAL, Liège, 2004.
5. Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime, OJ L 300, 11.11.2008,
6. Maliszewski P. J., MODELING CRITICAL VACCINE SUPPLY LOCATION: PROTECTING CRITICAL INFRASTRUCTURE AND POPULATION IN CENTRAL FLORIDA, FLORIDA STATE UNIVERSITY COLLEGE OF SOCIAL SCIENCES (2008).
7. OJ L 121, 15.05.2009.
8. OJ L 300, 11.11.2008.
9. Ratcliffe Jh., Intelligence-Led Policing , Willan Publishing, Cullompton, Devon 2008
10. Smedts B., Studia Diplomatica Vol. LXIV : 2011, n°1 Critical infrastructure protection at the European level, EGMONT – The Royal Institute for International Relations,2011., http://www.egmontinstitute.be/FR/SD-2011-2012.html

UDC 726.9:75.041.5
ID 176374796

Saša Mijalković, Vladimir Cvetković
The Academy of Criminalistic and Police Studies, Belgrade
sasa.mijalkovic@kpa.edu.rs
vladimir.cvetkovic@kpa.edu.rs

VULNERABILITY OF CRITICAL INFRASTRUCTURE BY NATURAL DISASTERS

Abstract: Natural disasters increasingly threaten the safety of the mankind. Not only that, in past decades there has been an obvious increase in the number of natural disasters, but it is also present an increase in their destructiveness. This results in a higher loss of life, material and non-material damage. In addition, compromising critical infrastructure prevents or limits the implementation of vital state functions (governance, health, education, energy, economic, social, and general security functions), which is further reflected in the safety of states and citizens. Despite the technological development of mankind, societies are increasingly threatened. It is clear that the disasters and their impact on people and critical infrastructure cannot be prevented, but mechanisms for prediction and early warning of disasters can be improved that the resilience and capacity for faster and more efficient revitalization of endangered values and goods can be increased. Besides the degree of destruction, the response strategy in an emergency situation will depend on the type of disaster, but also on the kind of critical infrastructure and specific goods and values that are threatened. In this regard, the paper gives an overview of the scope and the content of (still undetermined) concept of critical infrastructure, the term and the phenomenology of natural disasters, the consequences of geophysical, hydrological and meteorological disasters on critical infrastructure and critical infrastructure protection capabilities against natural disasters.

Key words: *safety, critical infrastructure, natural disasters, the consequences of threats to critical infrastructure by natural disasters, protection of critical infrastructure from natural disasters*.

1. INTRODUCTION

Generally, a disaster is defined as a specific (current, real) threat to humans and their material goods. These are harmful (unfortunate) events with adverse effects on people, property, infrastructure and natural resources, which society cannot overcome without outside help or support resources (Bimal, 2011, p. 12). Therefore this is about "serious disruption of the functioning of society, causing severe financial, economic, social or environmental losses that exceed the ability of affected society to cope using its own resources" (Preet, 2006). Generally speaking, the disasters can be natural, technological, and with complex background (Mladjan, Cvetkovic, 2013, p. 105).

Natural disasters are consequences of mutual influence of natural events (geophysical processes and other processes in nature) and human systems (social-economic, cultural and physical). Consequently, they are different from natural hazards that generate natural disasters only when threaten people and their material goods (Wisner et al., 2004). All natural disasters cause serious damage to critical infrastructures. Natural disasters have,

in principle, *polymorphous character* (two instances of the same origin and intensity often produce different total effects), followed by *the phenomenon of parallelism* (affecting only certain geospatial areas where the conditions of life and environment significantly alter) and specific, usually, mass effect (social, health, financial and environmental) (Jakovljevic, Đarmati, 1998, pp. 55-58; Mijalković, 2011, p. 201). This makes it difficult to predict the impact and consequences of natural disasters, particularly to critical infrastructures.

Neither in national law, nor in the strategic documents of the Republic of Serbia, there is a definition of the concept of critical infrastructure. Generally, these are the resources and assets that are essential to the smooth functioning of the economy and society.

The documents of the National Strategy for Protection and Rescue in Emergency Situations, (*Official Gazette of the Republic of Serbia,* No. 86/2011), and the Law on Emergency Situations (*Official Gazette of the Republic of Serbia,* No. 111/2009), do not refer to critical infrastructure at all. However, we can say that the institutional frameworks for the definition of critical infrastructure exist and these are the Sector for Emergency Situations of the Ministry of Internal Affairs of the Republic of Serbia, the relevant ministries and the relevant regulatory bodies. In addition, the specific measures to protect parts of the infrastructure exist, but there is neither a strategy nor protection policy at the national level. The need to consider the safety of critical infrastructure has been identified within the project "Management of Critical Infrastructure for Sustainable Development in the postal, communication and railway sector in the Republic of Serbia" (Gospić, et. al, 2012, p. 3).

According to the Council Directive 2008/114/EC adopted on December 8, 2008, on identification and determination of the European Critical Infrastructures and the assessment of the need for improving their protection in the European Union, the critical infrastructure presents: asset, system or its part that is located in the territory of the Member State and which is necessary for the maintenance of key social functions, health, safety, economic and social well-being, and whose disruption or destruction would have a significant impact on a member state (Council Directive 2008/114/EC on 8 December, 2008).

According to the conclusion of the Euro-Atlantic Partnership Council, the Civil Protection Committee - EAPC CPC 2002, which was later adopted by the *Senior Civil Emergency Planning Committee* - SCEPC, critical infrastructure is consisted of adequate national capacities, services, and information systems that are so vital that their lack of action or damage could have a direct impact on national security, the national economy, public health and safety of people and the efficient operation of government. In addition, critical infrastructure includes (but not exclusively): food, water, agriculture, health care and emergency medical service, energy, transport, information and telecommunications, banking and finance, chemical plants, defense industries, post offices and distribution of goods, as well as national monuments and other cultural values (The Department of Homeland Security, 2002, p. 15; by: Gačić, Proda, 2012, p. 163).

According to the documents of the United Nations, critical infrastructure represents the infrastructure that consists of physical and information technology facilities, networks, services and property, which if collapsed or destroyed can have a serious impact on the health, safety and economic well-being and effective functioning of government (Gačić, Proda, 2012, p. 163).

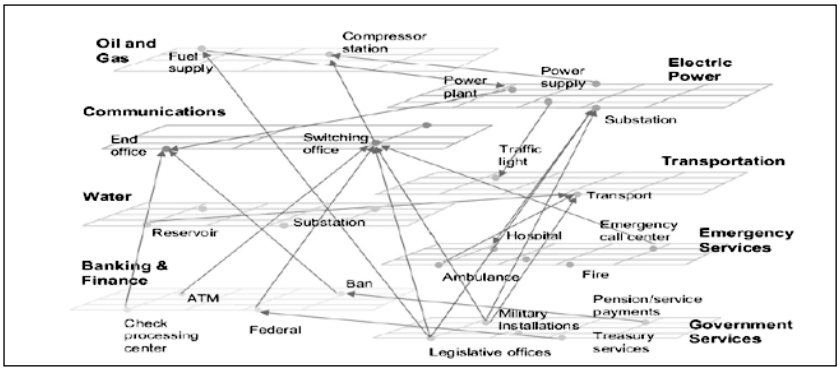


Figure 1: The interdependence of various infrastructures (Rajmohan, et al, 2012, p. 57)

Based on the comparative analysis performed in 16 countries in 2004, the researchers generalising came to the conclusion that critical infrastructure consists of: banking and finance, (tele)communications, information and telecommunication systems, and energy; transport, logistics and distribution; health services, water and water supply; central government/government services; first responders; petroleum products and gas supply; information services, the media (radio and television) and public administration; other areas - legislation strengthening, justice, public order and national security, waste management, police, RHB protection, army and military facilities, security system, social services, managing water, nuclear power plants (Gačić, Proda, 2012, p. 163). After all, it should be noted that the critical infrastructures are related at the various levels of dysfunction and an infrastructure can easily affect the functionality of other infrastructures, and vice versa (Rajmohan, et al, 2012, p. 57).

2. PHENOMENOLOGY OF NATURAL DISASTERS

Natural disasters as adverse events to people, their material goods (critical infrastructure) and the environment, occur in different areas of the Earth (lithosphere, hydrosphere, atmosphere and biosphere), such as e.g. earthquakes, floods, epidemics, hurricanes, etc. (Degg, 1992, p. 37, p. 199). Depending on the nature of the process of formation, natural disasters can be divided into:

geophysical (earthquakes, volcanoes, tsunamis, landslides, bog); meteorological (tropical cyclones/hurricanes, thunderstorms, tornadoes, lightning, hailstorm, snowstorm, ice storm, blizzard, cold and hot waves, landslides, snow, fog and frosts), hydrological (flood, inundation), biological (epidemics and insect pests) (Edward, 2005, p. 58; Tobin, Montz, 2007, p. 98); and, extraterrestrial (meteors) (Edward, 2005, p. 58). Given the place of origin, natural disasters may be: originally from the atmosphere and hydrosphere (e.g., tropical cyclones, tornadoes), originally from the lithosphere (earthquakes, volcanic eruptions, tsunamis) and originally of the biosphere (forest fires, bacteria). Also, with regard to the "source of origin", they can be divided into: endogenous (earthquakes, volcanic eruptions), exogenous (floods and drought) and with anthropogenic (human) origin (floods caused by dam failure) (Bimal, 2011, p. 43).

The consequences of natural disasters for the people and their material goods (critical infrastructure) and the environment can have primary or secondary characters. Thus, for example, the primary consequences of the earthquake caused by tremors, are various forms of demolition (critical infrastructure), while the effects of the secondary character are associated with causing landslides, tsunamis and various fires. Thus thunderstorms may be accompanied by copious amounts of rain, which can cause sludge (mud), inundation and flooding.[1]

Table 1: Primary and secondary threats of natural disasters (Source: Bimal, 2011, p. 145)

Primary threats	**Secondary threats**
Earthquake	Landslides, tsunamis, fires, floods
Surge	Coastal flooding
Volcanic eruptions	Earthquakes, wildfires, floods
Forest fires	Landslides
Severe storms	Tornado, stream
Landslides	Tsunami
Extremely hot weather	Forest fires
Floods	Fires
Hurricanes/cyclones	Surge

Natural disasters increasingly threaten people and their property (critical infrastructure) day by day. In addition, the number of disasters recorded in the first half of the last century is only 6% of the total number of disasters that have occurred over a period of 105 years, 62% disaster in the last 100 years happened in the last 15 years of this period, with 80% disaster recorded over the past 100 years occurred in the last 25 years of this period, in any month in the last 100 years, there is an average of 12 disasters; disasters threaten all parts of the world, especially in poor countries; redistribution disaster on different continents and more than 60 % of disasters happen in Asia and Africa, with almost 50% of disasters have meteorological character, 30% have technological character, 12% geological and 8% have biological nature; the worst cases of earthquakes, floods and famines in the last 100 years occurred in China; the worst cases of landslides, avalanches and volcanic eruptions have occurred in Latin America... (Kourosh, Richard, 2008, p. 78).

1 The volcanic eruption of Mount St. Helena in 1980 caused earthquake, landslides, floods and fires.

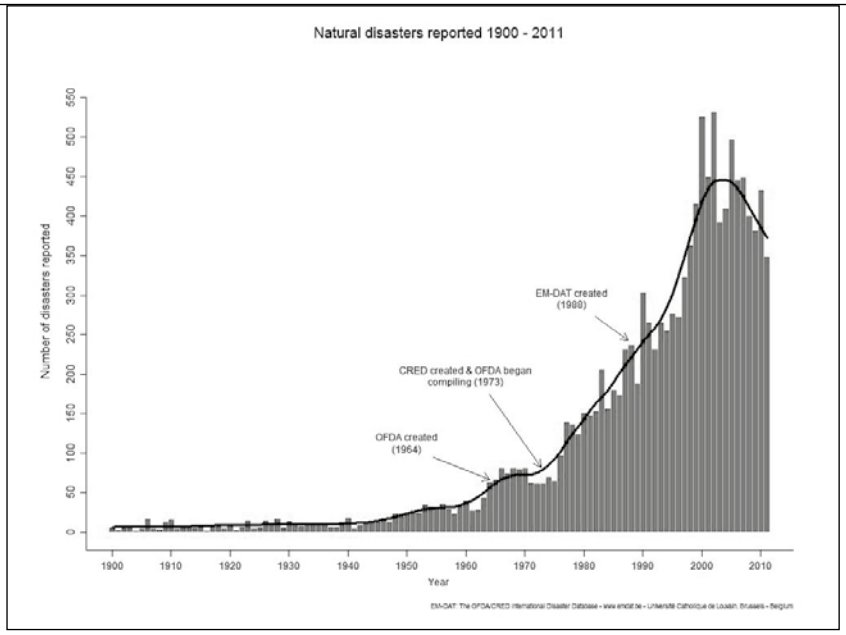


Chart 1: The trend of natural disasters from 1900 to 2011 (EM-DAT: The OFDA/CRED – International Disaster Database)

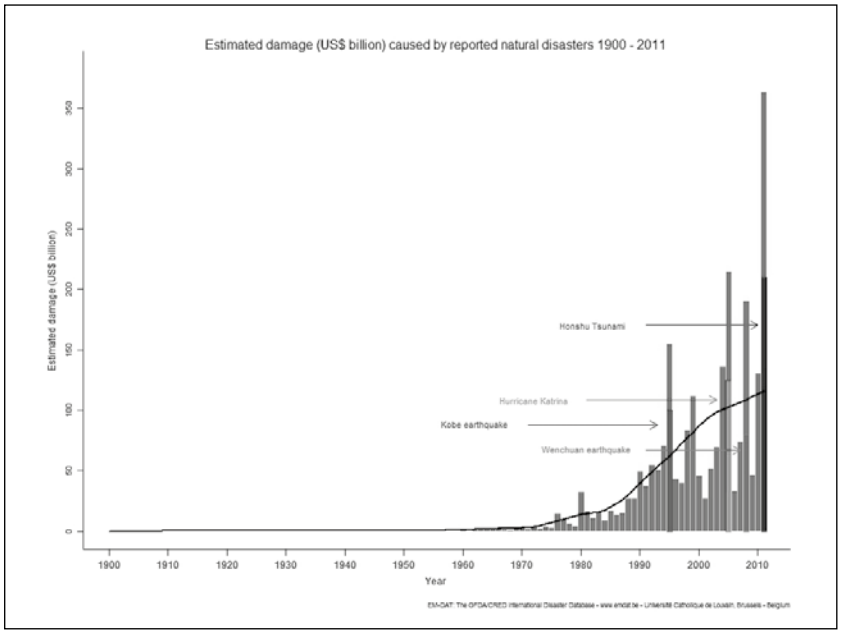


Chart 2: Estimated material damage caused by natural disasters, expressed in millions of U.S. dollars (EM-DAT: The OFDA/CRED – International Disaster Database)

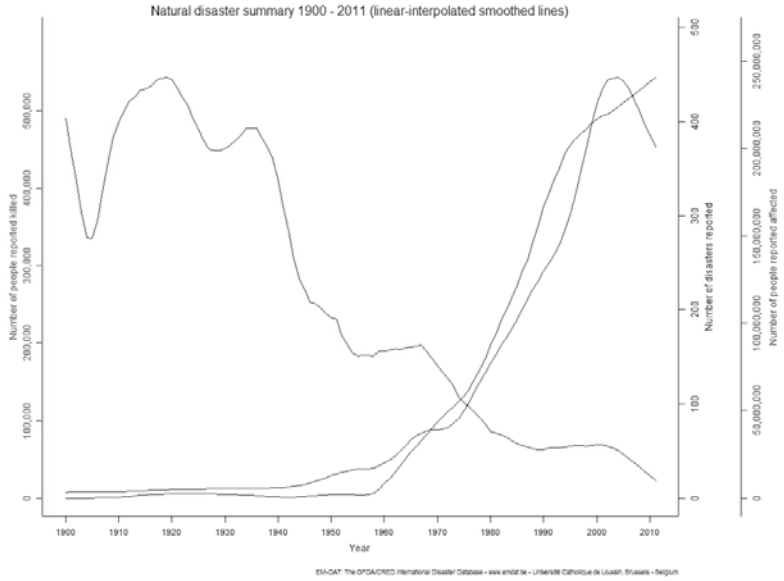


Chart 3 – The total number of natural disasters, casualties and material damage expressed in billions of U.S. dollars (EM-DAT: The OFDA/CRED – International Disaster Database)

3. CONSEQUENCES OF NATURAL DISASTERS ON CRITICAL INFRASTRUCTURE

The impacts of natural disasters on critical infrastructure can be seen through the understanding of the physical characteristics of natural disasters, that is, destructiveness that is determined by destructive force and possibility of propagation in the territory. The intensity of disasters is in strong correlation with the vulnerability of affected community (e.g., an earthquake of a certain severity will not cause the same damage to a rural village with crumbling earthen houses, and to a village with modern concrete multi-story buildings) (Cvetković, 2013). Consideration of the physical characteristics of natural disasters is important for mitigating the effects of various natural disasters (Tobin, Montz, 2007). There is a number of these characteristics:

1. *Intensity,* that is, power or force of events. In general, the risk of large intensity is an enormous potential for causing destructive effects on people and their material goods, which is the critical infrastructure. The possibility of measuring the intensity of natural disasters allows the comparison of natural disasters in space and time. However, direct and absolute comparison is often not possible (Edward, 2005, p. 34).
2. T*emporal distribution* is duration of natural disasters. It may take a few seconds (earthquake or landslide), hours or days (tornado or hurricane) or weeks or months (in case of flooding of the river), a few years (drought) (Hafiz, 2005). Accordingly, there will be a unequivocal correlation between the duration and the effects of natural disasters on critical infrastructure.

3. F*requency* describes how often an event with certain intensity affects the area within a certain period of time (Bimal, 2011, p. 34). This can be expressed using terms such as "common", and "rare" or "return time", which is the time elapsed between two events of the same intensity. The frequency of hazardous events is assessed during careful examination and the analysis of historical records and the use of such information for predictive models.
4. S*eason* - different studies have shown that certain natural disasters are not common in certain seasons (Preet, 2006). For example, the hot waves are not common during the month of December in Serbia, as it is unlikely that "blizzard" will infest Florida. Many types of natural disasters, especially hydro-atmospheric types are characterized by seasonal incidence (i.e., occur in certain seasons). Accordingly, certain types of critical infrastructure will suffer greater impacts due to natural disasters specific to different seasons;
5. *Spatial distribution*, that is, risk distribution in the area where a disaster can happen (Bimal, 2011, p. 23) is an important parameter of natural disasters because areas are not subject to the same types of natural disasters.
6. *Formation speed of a phenomenon* is the speed of a natural hazard turning into a natural disaster (Hafiz, 2005, p. 23). This can take place very quickly, as is the case with earthquakes, landslides, tornadoes and flash floods, or very slowly, as is the case with the drought. The first-mentioned type of disasters is called "creeping disaster", and the latter is called "sudden disaster". Sudden disasters typically cause bigger damage to critical infrastructure than creeping disasters, taking into account adaptation and coping mechanisms against natural disasters.

Considering all the facts presented so far, it can be safely concluded that natural disasters have great potential of direct/indirect threats to critical infrastructure. The vulnerability is the possibility of physical distortion and social disruption of societies and their larger subsystems by natural disasters (Bimal, 2011). There are two main types of vulnerability: physical vulnerability, as threats to physical structures and critical infrastructures, natural environment and is associated with economic losses (Committee on Disaster Research in the Social Sciences, 2006) and social vulnerability, as threats to well-being of the human population (e.g., death, injury, disruption of behaviour and functioning of the system) and is associated with non-economic losses.

3.1. Consequences of geophysical disasters on critical infrastructure

The earthquake is one of the most destructive geophysical disasters. It is a sudden shaking of the earth's crust (Bimal, 2011, p. 12). Earthquake's hit is sudden with almost no warning, making it impossible to predict. It damages the settlements, buildings, structures and infrastructure, particularly bridges, overpasses, railways, water towers, pipelines, the facilities for the production of electricity, and destabilizes the government, economy and social structure of the country (Edward, 2005). Subsequent earthquake's hits can cause heavy damage to already weakened structures. Secondary effects include fires, cracking dams and landslides that can block the land routes and waterways and cause flooding. It can cause damage to facilities with hazardous materials, resulting in leakage of chemicals. Also, there may be failure of communication facilities.

The consequences of earthquakes are diverse. There are a large number of casualties due to the poor design of buildings and critical infrastructure systems. Among the total num-

ber of persons who died in the earthquake, 95% of them lost their lives due to the demolition of buildings (Murray, 2012, p. 2). In addition, there is enormous damage in the public health system, transport, communications and water supply in the affected areas.

For example, the earthquake that hit Kobe in Japan in January, 1995, caused the following effects on critical infrastructure: 240,000 buildings were destroyed, 1.3 million people were left without water, 2.6 million people were left without electricity; 860,000 people were left without gas supply; 300,000 telephone devices were destroyed; highways and railways were destroyed; damage to the gas supply network was as follows: 26,459 medium-pressure cells were destroyed, it took 15 hours to stop the leak with a gas system and 85 days were spent on the reconstruction of gas pipeline network (Bimal, 2012, p. 119).

The earthquake that struck Kraljevo on 3 November 2010 seriously jeopardized the critical infrastructure. On that day the city was left with no heating and partially electricity, water was not recommended for drinking. Maternity hospital was flooded, in the "Studenica" Clinical Centre the operating rooms were not working, while shop shelves collapsed causing the supply of the population to be very difficult. Due to the earthquake, mobile telephony in Kraljevo was interrupted. In the village of Vitanovac, about 70% of 850 buildings collapsed. In Mataruska Spa several houses were damaged and cracked. In Kraljevo the streets were covered with pieces of glass, concrete and mortar, which disabled the normal flow of traffic. It is estimated that the total damage was around one million Euros (Valentine, 2011, p. 21).

3.2. Hydrological consequences of disasters on critical infrastructure

We are witnessing the catastrophic floods that cause huge damage, destroying villages, towns, farmland and critical infrastructures. Flood is one of the major threats to human community and has a significant impact on social and economic development. This deadly, harmful phenomenon kills thousands of people around the world annually thereby causing widespread damage. Even very small streams, gullies or small rivers are not harmless and can also cause flooding. Therefore, each country may be at risk of flooding (Blakie, et. al., 1994).

Flooding is uncontrolled flooding of land due to surface water outflow from natural and man-made waterways as a result of high water, punching or destruction of embankments, dams and other protection structures, as well as from flooding by inland waters in terms of abnormal weather conditions and rising groundwater and heavy rain, raising the levels of the lakes and the seas, due to the unusual strength of the waves and tides (Simon, George, 2000, p. 118).

Floods can occur gradually and can also take hours or even happen suddenly, without warning due to cracking of the embankment, spilling, heavy rain, etc. The flood greatly damages critical infrastructure. In addition, the structures such as houses, bridges and roads are damaged by incoming water. Landslides are triggered by incoming water, and boats and fishing nets may be damaged. Huge losses are in the form of human lives and livestock due to drowning. The lack of proper facilities for drinking water and the pollution of water (wells, groundwater, and drinking water) lead to the epidemics of diarrhoea, viral infection, malaria and many infectious diseases (COPO 2007). Flooding of large areas of agricultural land leads to the major losses of crops. This results in a lack of food, fodder and death of animals. Flooding may also affect the characteristics of the land, and it

becomes arid due to erosion of topsoil or may become salty if it is flooded by sea water (Bimal, 2011). Depending on the strength and extent, the flood has undoubted potential to destroy bridges, damage traffic infrastructure, destroy communications systems, power supply, etc.

3.3. Consequences of meteorological disasters on critical infrastructure

Drought rarely causes structural damage. When meteorological drought starts turning into a hydrological drought, damage begins to appear first in agriculture that depends on the moisture in the soil. The irrigated areas are less influenced by drought comparing to the areas irrigated only by rain. However, the regions near rivers tend to continue a regular life, even when drought conditions prevail. In addition, the impact of drought slowly spreads to the social structures, as the availability of drinking water decreases, reducing the production of energy, groundwater pressure and food supplies, undermining the health of people and animals, increasing poverty, which causes the reduced quality of life and leads to social unrest and migration.

Hurricanes can cause serious damage to critical infrastructure. For example, hurricane Katrina hit different areas of the United States causing multiple damages. In fact, in Mississippi, Hurricane Katrina, coming up 25 to 30 feet, was removing vehicles and objects from the road. Hotels and buildings were significantly damaged and sometimes literally the whole community disappeared. In New Orleans, there was a flood due to the formation of holes in dams, and 80% of the city was under water up to 6 weeks. However, some parts of the city, particularly those near rivers, as French Quarter, were slightly flooded. Wind and rain caused significant damage to homes and offices. More than 1.3 million people were evacuated before Katrina made landfall, and about 800,000 people were relocated for a long period of time (Haddow, et al., 2011). Critical infrastructure, such as water, electricity, communications, schools and hospitals, was significantly damaged and dysfunctional in all the affected areas. Both state and private sectors suffered huge losses. The homes were damaged in the amount of $ 67 billion; operating assets suffered a loss of $ 20 billion, and the state assets in the amount of $ 3 billion.

4. INSTEAD OF A CONCLUSION: THE PROTECTION OF CRITICAL INFRASTRUCTURE AGAINST NATURAL DISASTERS

The protecting of critical infrastructure is recognized as the foundation of maintaining the functionality of the community in emergency situations such as natural disasters. The main goal of protecting critical infrastructure from the impact of natural disasters is to maintain the continuity of its operation (Hromada, Lucas, 2012). Reducing the impact of natural disasters on people and critical infrastructure includes interventions to prevent or reduce the possibility of physical treats and social disruption (Zhou, et al., 2010). However, there are two dominant types of reducing the impact of natural disasters. Structural reduction involves the design, construction, maintenance and renovation of physical structures and infrastructures to resist the physical forces and impacts of natural disasters. Non-structural reduction includes the efforts to reduce the exposure of human population, physical structures and infrastructures to terms of danger. Non-structural reduction approaches include legally adopted town planning measures that take into account the possible impact of the disasters; regulating development in high risk areas such as the sloping fields that are prone to landslides and the coastal zones as storm waves targets, and even in some cases

the purchase and the relocation of communities or parts of the communities, which is a measure that is now used for areas that have experienced repeated flood losses (COPO, 2007, p. 123; Preet, 2006).

Examining the attributes and determinants of elasticity of facilities and critical infrastructure, researchers in Multidisciplinary Centre for Earthquake Engineering Research - MCEER, University at Buffalo, USA, have developed an R4 resistance frame: robustness, redundancy, resourcefulness and rapidity (Tierney and Bruneau, 2007). The first component of this framework refers to the *ability of the system*, system elements, as well as other units of analysis to withstand a given magnitude of the disaster without significant degradation or loss of function. Robustness reflects the inherent strength of the system. The lack of robustness may cause the system failure as happened with the breaking of the dike in New Orleans 2005 after Hurricane Katrina. The second R4 component - *redundancy* - refers to the extent to which elements of system are sustainable (i.e., able to meet the functional requirements if there is a significant impairment of functionality). Redundancy provides alternative options, choices and substitutions. The lack of these components prevents the proper response to natural disasters. A significant number of people in New Orleans were not able to get out in accordance with the mandatory evacuation before landslides during Hurricane Katrina, because public transport was unavailable (Harrington, et al., 2005). Component *resourcefulness* is associated with the capacity to diagnose the problem, the prioritization, and the adequate mobilization of resources for rapid recovery from the impact of natural disasters. Last R4 component is *rapidity*, and refers to the capacities to meet priorities and timely rehabilitate consequences and revitalize endangered values (Mileti, 1999).

In order to reduce the possibility of food shortages in the areas affected by the floods, it is necessary to plan the food storage on the high ground. Thus, the vulnerability of the system can be reduced by reducing dependence on one source of production or services; increasing the levels of portability in order to maximize the utilization of resources and the innovation of efficient and flexible systems that can withstand major disasters and reduce the need for reconstruction costs (COPO 2007). Warning against putting "all eggs in one basket" may be well applied here, because the system is less vulnerable when its resources of critical infrastructure are versatile and widely distributed (Bimal, 2011).

REFERENCES

1. Bimal, P. (2012). Environmental Hazards and Disasters Contexts, Perspectives and Management. Kansas: State University, Wiley – Blackwell.
2. Committee on Disaster Research in the Social Sciences: Future Challenges and Opportunities. (2006). Facing hazards and disasters – understanding human dimensions. Washington: The National Academies Press.
3. Copola, D. (2007). Introduction to International Disaster Management. New York: Oxford Press.
4. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union L, pp. 345-375, 23.12.2008.
5. Degg, M. (1992) Natural Disasters: Recent Trends and Future Prospects. Geography 77 (3), pp. 198-209.
6. Edward, B. (2005). Natural Hazards, Second Edition. Cambridge, University Press.
7. EM-DAT (2009). The OFDA/CRED International Disaster Database, Université Catholique de Louvain, Brussels, Belgium. http://www.emdat.be.
8. Gačić, J., Proda, Š. (2012). Resursi Republike Srbije u zaštiti kritične infrastrukture od terorističkih pretnji. Beograd: Bezbednost, broj 3.
9. Gospić, N., Murić, G., Bogojević, D. (2012). Definisanje kritične telekomunikacione infrastrukture u Srbiji. *Beograd: XXX* Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobracaju – PosTel.
10. Haddow, G., Bullock, J., Coppola, D. (2011). Introduction to Emergency Management. USA. Elsevier.
11. Harrington, L.S.B. (2005) Vulnerability and Sustainability Concerns for the US High Plains. In Rural Change and Sustainability: Agriculture, the Environment and Communities (eds S.J. Essex, A.W. Gilg, and R. Yarwood). Cambridge, MA: CABI Publishing, pp. 169–184.
12. Hromada, M., Lukas, L. (2012). Critical Infrastructure Protection and the Evaluation Process. International Journal of Disaster Recovery and Business Continuity Vol. 3, November.
13. Jakovljević, V., Đarmati, Š. (1998). *Civilna zaštita u Saveznoj Republici Jugoslaviji*, Beograd: Studentski trg.
14. Kourosh Eshghi, Richard C. Larson, (2008), Disasters: Lessons from the Past 105 years, Disaster Prevention and Management, Vol.17 Iss: 1 pp. 62 – 82,
15. Kramer, W. (2009). Disaster Planning and Control. New York: Oxford Press.
16. Mijalković, S. (2011). Nacionalna bezbednost. Beograd: Kriminalističko-policijska akademija.
17. Mlađan, D., Cvetković, V. (2013). Klasifikovanje vanrednih situacija. Beograd: Međunarodni naučni skup ,,Dani Arčibalda Rajsa", tematski zbornik radova međunarodnog značaja, Kriminalističko-policijska akademija.

18. Cvetković, V. (2013). Interventno-spasilačke službe u vanrednim situacijama. Beograd: Zadužbina Andrejević.
19. MunichRe (2010) NATCATSERVICE. Download centre for statistics on natural catastrophes. Münchener Rückversicherungs-Gesellschaft, Geo Risks Research, Munich, Germany.http://www.munichre.com/en/reinsurance/business/nonlife/georisks/natcatservice/default.aspx
20. Murray, T. (2012). Critical Infrastructure Protection: The Vulnerability Conundrum. Telematics and Informatics, vol. 29, no. 1.
21. National Infrastructure Protection Plan, Homeland Security, 2009.
22. Parker, D. et al. (1997) Reducing Vulnerability Following Flood Disasters: Issues and Practices. In Reconstruction after Disaster: Issues and Practices (ed. A. Awotona). Aldershot: Ashgate, pp. 23–44.
23. Predlog zakona o kritičnoj infrastrukturi sa konačnim predlozima 2013.
24. Preet, V. (2006).Natural hazards and disaster management. A supplementary Textbook in Geography Class IX on unit 11: Natural hazards and disaster.
25. Rajmohan, C., Subramanya, G., Sharma, N. (2012). Telecommunication Networks: Security Management, Tata Consultancy Services Limited.
26. Smith, K. (2001) Environmental Hazards: Assessing Risk and Reducing Disaster. London: Routledge.
27. Tierney, K., Bruneau, M. (2007) Conceptualizing and Measuring Resilience: a Key to Disaster Loss Reduction. TR News 250, May–June: 14–17.
28. Tobin, A. Montz, E. (2007). Natural hazards and technology: vulnerability, risk, and community response in hazardous environments. In Geography and Technology (ed. S. D. Brunn et al.). Dordrecht: Kluwer, pp. 547–570.
29. UNCHS (United Nations Centre for Human Settlements) (1994) Sustainable Human Settlements in an Urbanizing World, including Issues Related to land policies and mitigation of natural disasters. 15th Session of the Commission on Human Settlement. Unpublished Draft Theme Paper.
30. UN-ISDR United Nations – International Strategy for Disaster Risk Reduction, 2004.
31. Wisner, B. et al. (2004) At Risk: Natural Hazards, People's Vulnerability and Disasters. London: Routledge.
32. Zhou, H. et al. (2010) Resilience to Natural Hazards: a Geographic Perspective. Natural Hazards 53 (1), pp. 21–41.

SECTION II

REGIONAL AND NATIONAL PROTECTIVE POLICY AND OPTIONS

UDC 726.9:75.041.5
ID 176374796

Ernst-Peter Döbbeling
University of Applied Sciences, Furtwangen
epd@hs-furtwangen.de

PROGRAMS AND TRENDS IN CRITICAL INFRASTRUCTURE PROTECTION IN THE EU

Abstract: The Critical Infrastructure Protection (CIP) in the EU has a 10 year history until today with programs and multiple activities. Attacks and disasters that hit critical infrastructures have been identified as a serious security risk for the European countries and due to the high interdependencies as a risk for the EU as a whole. Therefore an EU CIP program was set on route in 2005 followed by a directive of the EU Council in 2008 for the energy and transport sectors. The EU countries took their responsibilities on CIP by implementing the EU Council directive into national legislation. In addition, they developed regulations and recommendations, intensified the CIP planning by national agencies and supported national research as for example risk analysis, cascade effects or interdependencies of different critical infrastructure sectors. Especially for the energy and IT sectors risk management and impact simulation models were developed. Several countries installed new agencies to give more attention to CIP and to support industry and administration in CIP-Planning.

In the EU's "Seventh Framework Program" (FP 7) from 2007 to 2013 which is a 50 Billion EU research program, a high number of CIP related projects were launched especially related to border security, CBRNE detection and interdependencies of CI-sectors as Electricity or transportation.

The EU has to be seen mainly as promoter, supporter and coordinator of measures for Critical Infrastructure Protection in the EU. But significant for CIP in EU is the primary responsibility of the Member States for national Critical Infrastructures and the complementary responsibility of EU for so called European Critical Infrastructures. Methods, procedures and responsibilities can differ in the member states according to federalism, centralism, national agencies and private-public partnership.

On EU level only a small number of European Critical Infrastructures have been identified.

From a viewpoint of an observer it seems that the EU initiative on Critical Infrastructure Protection has not enormously increased the level of CI protection of so called European Critical Infrastructures but nevertheless stimulated national activities in EU Member States and supported the exchange of information and best praxis by implementing platforms for communication and cooperation.

Key words: *Critical Infrastructure Protection (CIP), EU Council Directive 2008/14/EC, Critical Infrastructure Warning Information Network (CIWIN), Business Continuity Management, Subsidiarity in EU*

1. INTRODUCTION

The starting point in Europe of what is today known as Critical Infrastructure Protection (CIP) was the Millennium when industry, commerce, administration and emergency ser-

vices recognized the threat of extensive failure of important infrastructures being caused by failure of IT-systems, embedded systems or communication systems. An in deep analysis showed in some sectors or installations not only the high dependency of energy, water, communication from IT-systems but also very often interdependencies of these systems. The result of these studies was: To create resilient singular systems is not sufficient, but it is indispensable to make the system of interdependencies as resilient as possible.

After, in 2001, the worldwide terrorist threat and the attack on the world trade center reinforced in Europe the need of awareness and appropriate actions for CIP. The European countries and the European Council became strongly aware of the high dependency of European economy and citizens' security from infrastructure systems. Terrorist attacks against critical infrastructures were identified as a serious security risk for the European countries and due to the high interdependencies as a risk for the EU as a whole. Critical Infrastructure Protection (CIP) has become an important issue for the EU council and a set of activities followed as described in the introduction of the Directive (EU Directive, 2008):

In June 2004 the European Council asked for the preparation of an overall strategy to protect critical infrastructures. In October 2004, the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

In November 2005 the Commission adopted a Green Paper on a European program for critical infrastructure protection" (EPCIP) which provided policy options on the establishment of the program and the Critical Infrastructure Warning Information Network.

In April 2007 the Council adopted conclusions on the EPCIP in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders. The Commission started the development of a European procedure for the identification and designation of "European critical infrastructures" ('ECI').

Finally in December 2008 the council adopted the DIRECTIVE 2008/114/EC to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrated on the energy and transport sectors. Due to the strong subsidiarity principle also the primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures.

2. EU INSTITUTIONS

A description of the structure and the decision making of the three EU institutions can be found on the official EU Website "How does the EU work" (EU Institutions, 20013): The European Union is more than just a confederation of countries, but it is not a federal state. Based on the Treaties (known as 'primary' legislation), regulations, directives and recommendations adopted by the EU institutions are the outcome of legal work. These laws, along with EU policies in general, are the result of decisions taken by the institutional triangle made up of the Council (representing national governments), the European Parliament (representing the people) and the European Commission (a body independent of EU governments that upholds the collective European interest).

The Council of the European Union (also known as the Council of Ministers) is the EU's main decision-making body. The EU member states take it in turns to hold the Council

Presidency for a six-month period. Every Council meeting is attended by one minister from each EU country. The Council has legislative power, which it shares with the European Parliament. In addition to this, the Council and the Parliament share equal responsibility for adopting the EU budget. The Council also concludes international agreements that have been negotiated by the Commission.

(EU Institutions, 2013)

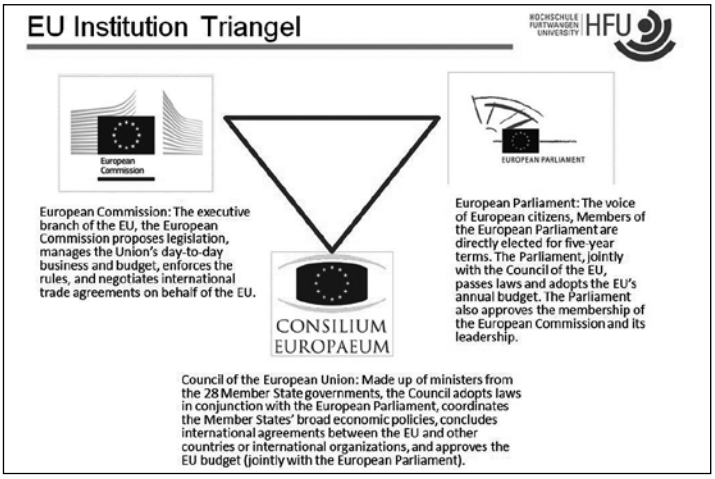


Figure 1: The Triangle of European Constitutions
Source: Author developed from (EU Institutions, 2013)

The European Parliament is the elected body that represents the EU's citizens. It exercises political supervision over the EU's activities and takes part in the legislative process. Since 1979, members of the European Parliament have been directly elected, by universal suffrage, every five years. The numbers of seats per country is according the population, from 5 seats for Malta until 99 seats for Germany. The total number of seats is 785 (EU Institutions, 2013).

The Commission is the third part of the institutional. Its members are appointed for a five-year term by agreement between the member states, subject to approval by the European Parliament. The Commission is answerable to the Parliament, and the entire Commission has to resign if the Parliament passes a motion of censure against it. Since 2004, the Commission has been made up of one Commissioner from each member state.

The Commission is the EU's executive arm. Its main task is to uphold the common interest, which means that it must not take instructions from any national EU government. It has to ensure that the regulations and directives adopted by the Council and Parliament are being implemented in the member states. If they are not, the Commission can take the offending party to the Court of Justice to oblige it to comply with EU law. The Commission is assisted by a civil service made up of 46 directorates-general (DGs) and services (EU Institutions, 2013).

On Directorates is the Directorate –General "Home Affairs" which comprises among other subjects (as police cooperation, Schengen affairs and immigration) the responsibility for crisis management and terrorism including Critical Infrastructure Protection matters (DG Home-Affairs, 2013).

3. THE SUBSIDIARITY PRINCIPLE OF EU

The principle of subsidiarity is defined in the Treaty on European Union. It ensures that decisions are taken as closely as possible to the citizen and that constant checks are made to verify that action at Union level is justified in light of the possibilities available at national, regional or local level. Following the Treaty of Lisbon on 1 December 2009, the protocol now requires the principle of subsidiarity to be respected in all draft legislative acts and allows national parliaments to object to a proposal on the grounds that it breaches this principle.

(EU legislation, 2013)

Under this subsidiarity principle national security laws, especially for incident response, disaster management and crisis management of which CIP is a part, are strictly under national responsibility. The EU influence on Emergency and disaster management is limited for example to coordination, planning support, research, and exchange of best praxis. When starting the discussion on CIP in EU under the experience of the 2001 terrorist attacks it became clear that there is a common interest of an EU centralized and coordinated part of border security, terrorism countermeasures and police coordination but also it was obvious that security in the sense of prevention and response against natural, industrial or human caused risks including CIP must remain under national responsibility. As consequence each member country had to develop and implement its own national CIP strategy. No general EU directive on CIP exists. Nevertheless, the EU has set up a program for CIP, implemented a Directive for so called "European Critical Infrastructures (ECI)" and published a not binding guideline for the implementation.

4. MECHANISM OF CRITICAL INFRASTRUCTURE PROTECTION IN THE EU

The Critical Infrastructure Protection in the EU has a history from 2004 until today with programs and multiple activities as shown in figure 2. Significant for CIP in EU are the primary responsibility of the Member States for national CIs and the complementary responsibility of EU DG Home Affairs for so called ECI. One can conclude that in EU exist in total 34 different activities: 6 pieces of the EU for the ECIs and 28 national pieces within the 28 member states for national CIs.

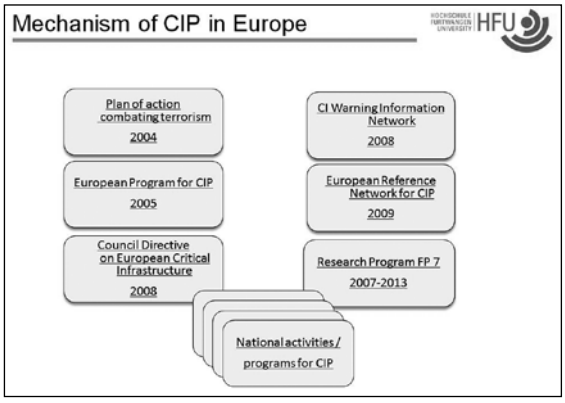


Figure 2: The mechanism of CIP in the EU –Overview
Source: Author, 2013

THE EU CIP PROGRAM

The EU has to be seen as promoter, supporter and coordinator of measures for CIP in EU while the member states act independently to ensure the protection of national CIs. As shown in figure 3 already the definition of CI can be different from country to country and on EU level. Also methods, procedures and responsibilities can be very different in the member states according to federalism, centralism, national agencies and private-public partnership.

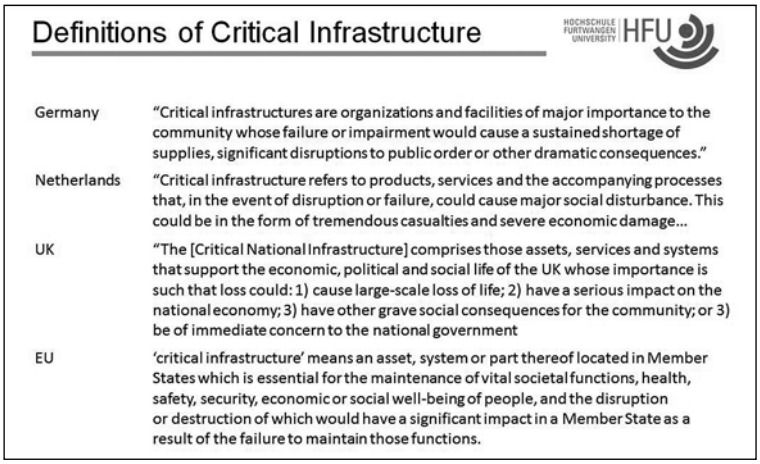


Figure 3: Examples for Definitions on Critical Infrastructure
Source: Protection of Critical Infrastructure and the role of investment policies relation to national security, OECD, 2008 and EU Directive, 2008

The differences of the EU member states are also mentioned in the task force report of the Centre for European Policy Studies, Brussels on "Protection of critical Infrastructure" (CEPS, 2012: It is stated: "....EU member states are still pursuing fragmented C(I)IP policies, and there is still a significant lack of cooperation between national governments and EU institutions in setting up a coordinated emergency response to potential threats. In other words, the higher degree of risk to which we expose our daily activities is not mirrored by an increased response potential of EU institutions. Yet member states are indeed interdependent: even if the internet backbone is not evenly spread over the EU27, several critical infrastructures are cross border infrastructures, and for those the weakest links – i.e. the countries with a weaker emergency response potential – affect the vulnerability of all countries. For example, if 26 out of 27 countries have sufficiently strong policies to protect the internet backbone or challenge the spread of malware, this is not enough to guarantee the resilience of the internet network in the EU. It takes no more than one country to disrupt the whole system and expose it to threats."

This statement postulates an appropriate balance between EU influence with centralized responsibilities and national independencies in CIP. Apparently the level of analysis, preparedness and resilience is different from state to state. If the weakest level determines the level of vulnerability this could create risks for other states.

4.1. The EU Critical Infrastructure Protection Program

The "Plan of action combating terrorism" was the starting point for CIP because CIP was explicitly mentioned as one consequence from the terrorist threats. The Council adopted a Solidarity program on the consequences of terrorist threats and attacks, that aims at improving the protection of critical infrastructures, the preparedness of consequence management resources and the management of crises with cross-border effects within the EU.(Plan of Action, 2004). In the following, the approach CIP against terrorism was modified to an all hazard approach in the "EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION (EPCIP)" which was the basis for the later Directive of 2008.

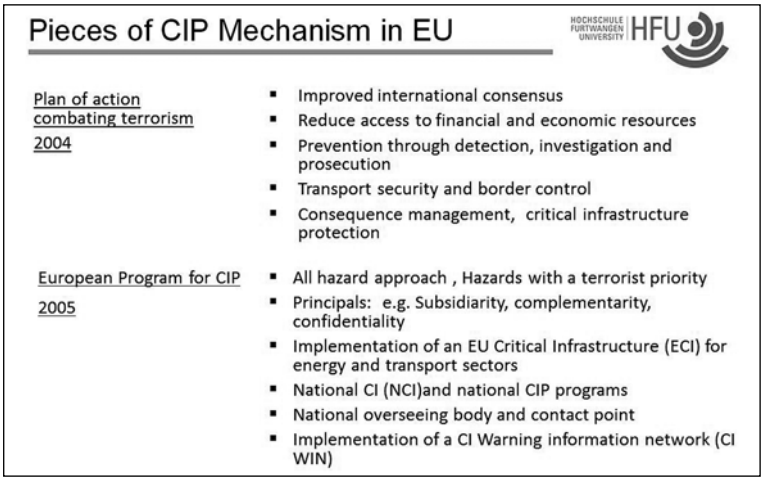


Figure 4: Pieces of CIP mechanism in EU (1) – Starting Documents
Source: Author developed from (plan of action, 2004) and (CI Program, 2005)

In the EPCIP as key principles were suggested Subsidiarity, Complementarity, Confidentiality, Stakeholder Cooperation and Proportionality in order to respect national interests of the member states, the interests of private stakeholders and the EU as a community. Figure 4 shows the main elements of EPCIP. Also the term "European Critical Infrastructure" was implemented as follows.

"European critical infrastructure' (ECI) means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure." (EU Directive, 2008)

4.2. The EU Council directive 2008

After long discussions with the member states the CIP program of 2005 concluded into the Council Directive 2008/114/EC "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection". Compared to the CIP program the Directive takes only reference to ECIs and its implementation was limited only to the transport and energy sectors. The directive did not implement any

regulations on national CIs or other sectors. With this limitation was acknowledged that for many industries which can be considered as CIs special regulations already existed as for example for drinking water or pharmaceutical industries ..An overview on the content off the Directive is shown in figure 5. (EU Directive, 2008)

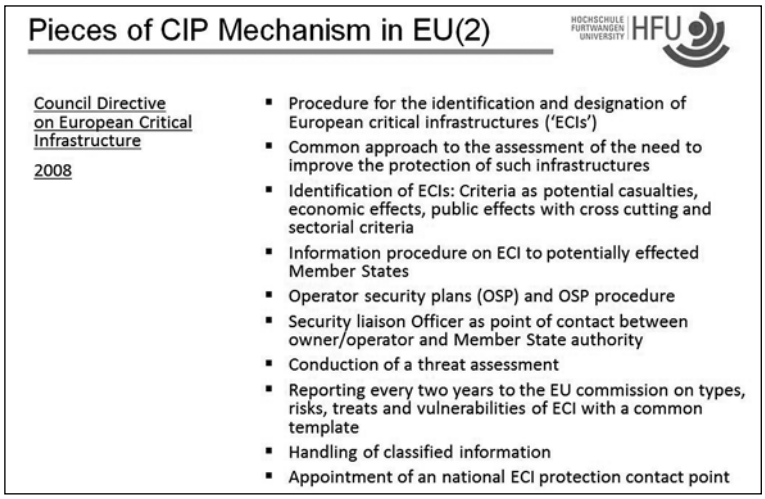


Figure 5: Pieces of CIP mechanism in EU (2)
Source: Author developed from (EU Directive, 2008).

Complementary to the directive a "Non-binding guideline for application on the directive" was published which gives advice to the member states how the identification and designation of ECI can be carried out in a common way and with consistent criteria. Figure 6 refers to this guideline. (CI Guideline, 2008)

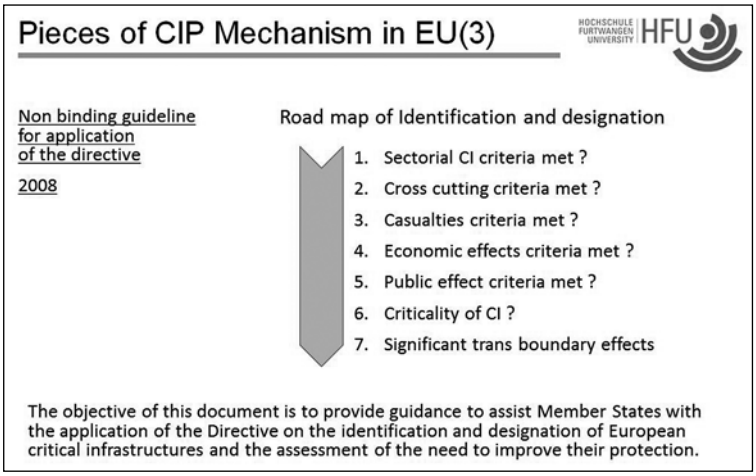


Figure 6: Pieces of CIP mechanism in EU (3)
Source: Author developed from (CI Guideline, 2008)

4.. Warning Information network

The EU Critical infrastructure Warning Information Network (CIWIN)is an EU activity to support national public and private CI activities. It is a protected public internet based information and communication system and offers recognized members of the EU's critical infrastructure protection community the opportunity to exchange and discuss CIP-related information, studies and good practices across multiple sectors. CIWIN is one of the measures foreseen to facilitate the implementation of the European Program for Critical Infrastructure Protection. (CIWIN, 2013).

The CIWIN portal, following its prototype and pilot phases, has been up and running since mid-January 2013. DG Home coordinates all activities. The CIP Point of Contact of the Member State nominates a CIWIN Executive and Support Officer who provide to the European Commission assistance in the context of the use and development of the CIWIN system (CIWIN Network, 2013)

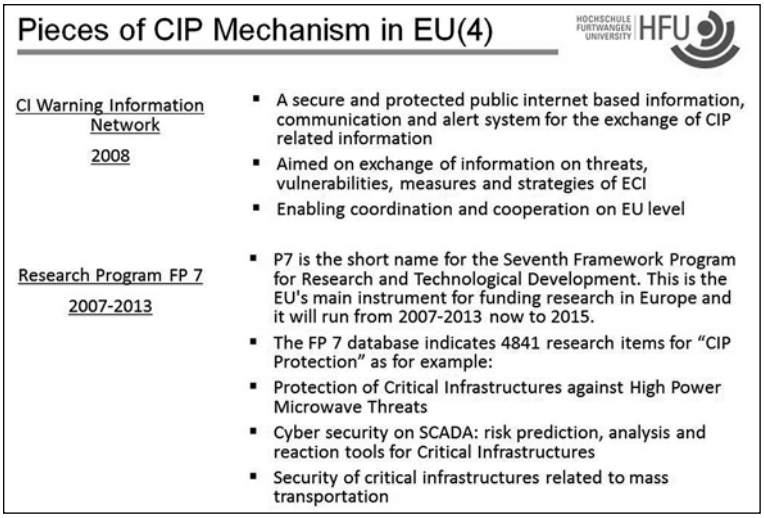


Figure7: Pieces of CIP mechanism in EU (4)
Source: Author developed from (CIWIN, 2013) and (FP7, 2006)

4.4. FP 7 Research Program- Security part

Since 1984 the EU has set up research programs for multi-disciplinary research and cooperative activities. From 2007 to 2013 the "Seventh Framework Program is on route with a budget of 53.2 billion euros. One objective of the FP programs is to bring together in one project researchers from different EU member states, private industries, public and private research institutes, universities and end-users in order to get results with practical use. The FP 7 program had security as one of the main research objectives and a great number of projects on Security were financed. Figure 8 gives some examples of CIP related subjects. In the work program, theme 10 "Security" the overall structure of the Security theme is separated in "Security mission areas" and Cross cutting areas:

Security mission areas

1. 1. Security of citizens
2. 2. Security of infrastructures and utilities
3. 3. Intelligent surveillance and border security
4. 4. Restoring security and safety in case of crisis

Cross-cutting areas:

5. 5. Security systems integration, interconnectivity and interoperability
6. 6. Security and society
7. 7. Security Research coordination and structuring

CIP can be seen as part of several areas, even if not explicitly addressed. In the FP 7 program especially research on CI sectors as electricity and fuel delivery were funded. (FP7, 2006)

3.5. European Reference Network for Critical Infrastructure Protection

Situated at the Joint Research center of the European Commission in Ispra the institute for Protection and Security of the Citizen has 2011 launched an EU wide Network for CIP (ERNCIP) in accordance with the EPCIP.

An overview on the main objectives is given in figure 9.

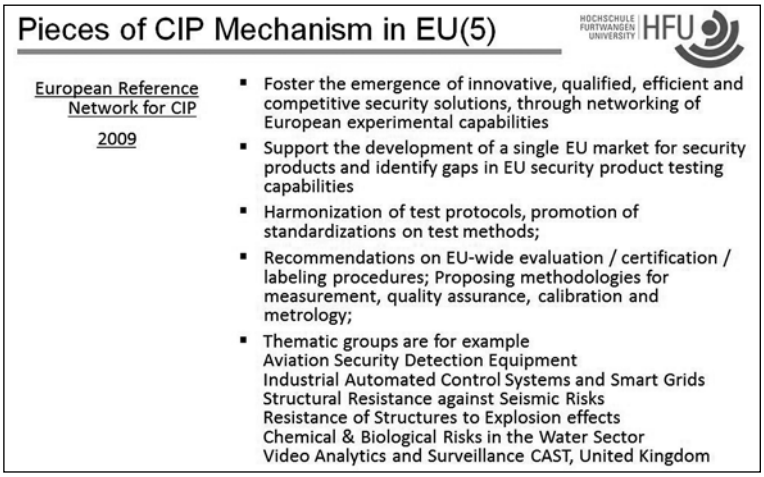


Figure 8: Pieces of CIP mechanism in EU (4)
Source: Author developed from (ERNCIP, 2012)

ERNCIP provides a framework for CIP-related experimental facilities and laboratories to share knowledge and expertise, and to harmonise test protocols throughout Europe, aiming at improved protection of critical infrastructure in the EU against all types of threats and hazards. The ERNCIP work program addresses several thematic areas (TA), as identified by the sponsors. The work is undertaken by specific thematic working groups, each led by a TA coordinator (see figure 9). (ERNCIP, 2012)

5. NATIONAL IMPLEMENTATIONS OF CRITICAL INFRASTRUCTURE PROTECTION

The EU member states assumed their responsibilities in CIP by implementing the EU Council directive into national legislation for ECI. In additions, they developed regulations and recommendations and intensified CIP planning by national agencies and supported national research as for example risk analysis, cascade effects or interdependencies of different critical infrastructures. Especially for the energy and IT sectors risk management and impact simulation models were developed. Several countries installed new agencies to give more attention to CIP and to support industry and administration in CIP-Planning. So Germany published the National Strategy for Critical Infrastructure Protection in 2009 and France a national regulation on vital services in 2006. In parallel to CIP activities, Business Continuity Management (BCM) and IT Security became an important subject. BCM is strongly linked to CIP because it can be considered as a complementary activity to create higher resilience for Critical Infrastructures when disruptive events occur. New ISO Standards as ISO 22301 on BCM will probably become European CEN standards.

The DG "Home-Affairs" has funded projects to facilitate the national implementation of CIP. One result is "RECIPE – Good practices manual for CIP Policies" which refers to possible CI in a country and gives practical advice how to identify CIs and to manage CIP (Recipe, 2011).

6. CONCLUSIONS

From the ECI perspective the EU Commission has launched in 2012 a review on the Directive of 2008. One result was, that in EU only a total of 14 ECI have been identified: 10 in the sector electricity, 3 in the sector gas and 1 in the sector rail. The review stated that, during implementation of the ECI Directive, the well-established network of national points of contact played a critical role in communication between Member States. This close cooperation and effective communication has also been facilitated by the various workshops on the implementation of the Directive.

It was also said that there is a strong perception that the implementation of the Directive has not resulted in sufficiently clear and tangible improvements to ECI security levels. A number of facts support this viewpoint, most importantly the fact that relatively few ECIs have been identified and consequently very few new Operator Security Plans have been produced.

In addition, there are concerns as to whether the set of identified ECIs is complete, since the assets of pan-European services do not appear to have been evaluated thoroughly as potential ECIs, while it is openly recognized that main energy transmission networks (gas, electricity) are of cross-border dimension. The current ECI designation process does not respond to this particular challenge, as protection measures cannot be the product of a single Member State or operator. (Directive review, 2012)

On the other hand the review gave the impression that in general CIP awareness and the level of cooperation in the EU have increased in the energy and transport sectors through the various activities and forums organized under the Directive. However, the credit for improved awareness and cooperation is not entirely due to the Directive and EPCIP, since other sectoral initiatives, for instance in the area of aviation security, have played an important role as well. (Directive review, 2012)

From national perspective, the importance of CIP has been well recognized in industries, multiple sectors of energy and transport, in IT services but also in public services during the period of 2004 to 2012. CI is today a known as major risk for society. Big companies but also more and more middle seize companies see the need to analyze CI risks and also Emergency services recognized that they belong to the Critical Infrastructures und started risk analysis.

From a viewpoint of an observer it seems that the EU initiative on CIP hit in the beginning strong national reservations because of the subsidiarity principle but apparently the initiative has nevertheless stimulated the national CI activities in the EU Member States and supported the exchange of information and best praxis

7. REFERENCES

1. CEPS, 2012
   CEPS TASK FORCE REPORT 2012
   Protection Critical Infrastructure in the EU
   ISBN: 978-94-6138-070-8
2. CI Guideline, 2008
   Non-Binding Guidelines for the application of the Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection
   General Secretariat of the Council, 15616/08
   Brussels, 13November 2008
3. CI Program, 2005
   GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION, COM(2005) 576 final
   Commission of the European Communities, Brussels, 17.11.2005
4. CIWIN, 2013
   COUNCIL DECISION on a Critical Infrastructure Warning Information Network (CIWIN)
   Commission of the European Communities, 2008/0200 (CNS)
5. CIWIN Network, 2013
   Official Website of EU DG "Home-Affairs"
   http://ec.europa.eu/dgs/home-affairs/what-we-do/
6. EU Directive, 2008
   OUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
   23.12.2008, Official Journal of the European Union L 345/75
7. Directive Review, 2012
   COMMISSION STAFF WORKING DOCUMENT ON THE REVIEW OF THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION
   Brussels, 22.6.2012, SWD(2012) 190 final
8. DG Home Affairs, 2013
   Official EU Website of Directorate –General "Home Affairs"
   http://ec.europa.eu/dgs/home-affairs
9. ERNCIP 2012
   European Network for Critical Infrastructure Protection (ERNCIP)
   Joint research Centre Ispra, Italy
   Institute for Protection and Security of the Citizen
   Website: http://ipsc.ec.europa.eu/?id=688
10. EU Institutions, 20131
    Official Website of the EU council
    http://europa.eu/abc/12lessons/lesson_4/

11. EU Legislation, 2013
Official Website of EU
"Summary of EU legislation"
http://europa.eu/legislation_summaries/glossary/subsidiarity_en.htm
12. Plan of Action, 2004
EU Plan of Action on Combating Terrorism - Update
Council of the European Union
Brussels, 29 November 2004, 14330/1/04 REV 1
13. FP 7, 2006
DECISION No 1982/2006/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2006
concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013)
Official Journal of the European Union L 412/1, 30.12.2006
14. RECIPE 2011
RECIPE – Good practices manual for CIP policies
TNO, Marieke Klaver, Eric Luiijf, Albert Nueuwenhuijs
http://www.tno.nl/recipereport

8. LIST OF FIGURES

1. Figure 1
The Triangle of European Constitutions
Source: Author developed from (EU Institutions, 2013)
2. Figure 2
The mechanism of CIP in the EU –Overview
Source: Author, 2013
3. Figure 3
Examples for Definitions on Critical Infrastructure
Source: Protection of Critical Infrastructure and the role of investment policies relation to national security, OECD, 2008 and EU Directive, 2008
4. Figure 4
Pieces of CIP mechanism in EU (1) – Starting Documents
Source: Author developed from (plan of action, 2004) and (CI Program, 2005)
5. Figure 5
Pieces of CIP mechanism in EU (2)
Source: Author developed from (EU Directive, 2008).
6. Figure 6
Pieces of CIP mechanism in EU (3)
Source: Author developed from (CI Guideline, 2008)
7. Figure 7
Pieces of CIP mechanism in EU (4)
Source: Author developed from (CIWIN, 2013) and (FP7, 2006)
8. Figure 8
Pieces of CIP mechanism in EU (4)
Source: Author developed from (ERNCIP, 2012)

UDC 726.9:75.041.5
ID 176374796

Momčilo Milinović
University of Belgrade – Faculty of Mechanical Engineering
mmilinovic@mas.bg.ac.rs

Zoran Jeftić
University of Belgrade – Faculty of Security Studies
jefticz@ymail.com

CHALLENGES OF NATIONAL DEFENCE IN INTERNATIONAL STATE AND PRIVATE CORPORATIVE MANAGEMENT OF INFRASTRUCTURE PROTECTION[1]

Abstract: Paper presents the general analyses of questions and requirements, which determine the global roles of military forces in protection and corporative security. Extended protection challenges in both the homeland and foreign territories come from the integrative roles with non-governmental and governmental non military forces. According to legal obligation, they have insufficient possibilities and capacities to protect huge infrastructures of international importance in the homeland areas, and military formations could appear as supplementary protecting forces. The protection of technology infrastructures required to be protected in corporative management could be extended over national defence system by technology and organization capabilities. The paper suggested the extended interoperable treatment as collective international, to the collective corporative international defence role, without obstacles and following political suspects. This paper also offers a modest frame for modular military package architecture as a solution joint with non-military actors, integrated at the smallest military units engaged in civilian and private corporative protection jobs.

Key words: *critical infrastructure security, military forces package, virtual and modular architecture, civil institutions participation, interoperable efficiency*

1. INTRODUCTION - BACKGROUND OF MILITARY FORCES IN THE NEW AGES

In general there are two types of military forces: expeditionary, and campaign forces. In line with the strategic defence documents, in most countries armed forces have three primary missions: protection of state independence, sovereignty and territorial integrity; preservation of the international peace and humanitarian assistance in case of disasters. However, this sets up a question of their aimed functions as homeland, territorial or foreign, exterritorial organization. Considerations of combat threats for campaign oriented forces usually designed for national defence of territorial, overall and particular protection roles as their first capability considers deterring task function as the main force quality element. These capabilities usually are not the first in defence philosophy considerations of expeditionary orientated forces, and especially are not applicable for the considerations aimed at the asymmetric war threats. The new age strongly distinguishes the joint international threats and joint defence efforts of all kinds emerge more often without political

1 This paper is the part of 2013 research on the project III 47029, MESTD of RS

obstacles. The new necessity of military design understands jointing of both campaign and expeditionary forces main capabilities in national forces particular elements.

Critical thinking in redesigned doctrinal task of military forces comes from two opposite balancing principal roles of military that have never before been so much underlined as nowadays. These are the role of combat and the role of peace keeping, combined with other no combat operations at the same time, and in the same battle field. Military services, as the continual national planed institutions, cannot fulfil these requirements by formation packages in the old fashioned manner which is based on traditional tactical units.

Combat role basically is determined to defeat enemy. New determined battle tasks (Valcourt, 2009), extend combinations of tactical activities, composed in D3&I principle (Dislocating, Destroying, Disintegrating and Isolating). But, joint required roles of stability and peace keeping operations, as the second military goal, include military tools (Valcourt, 2009) as the following:

Compel - Uses the threat of lethal force to establish control, and to deter enemy.
Control - The imposition of civil order. Actions to establish control include securing borders, routes, sensitive sites, population centres, infrastructure objects and individuals.

Influence - The shaping of opinions and attitudes of civilian population through information engagement, presence, and conduct.

Support - The establishment or strengthening of conditions necessary for other instruments of national power to function effectively.

Inside of this function it could be functions of Civil Emergency Help and Hazard Risk Helps in Emergency Situations (CEH). These functions will further be designated as CCIS tasks in the stability types of operation. This joint readiness of military, divided into three groups of mission tasks: D3& I tasks, CCIS tasks and CEH tasks within CCIS, is the key challenge to design national forces.

It is notable that shown general roles of military forces in the new ages as *defeating enemies, peace keeping on the territory of responsibilities and local and global hazard help operations*, are usually the opposite roles for military tactical capabilities design. That urges to defence planers, especially for land forces and joint troops, to put full stop on the twenty-century-long tactical military organizations, and to recognize a new approach in military employment.

Each of missions needs enough and right estimated capabilities but also the means to find out their unique expression for performance to be achieved as needed flexible quality of combat units. This paper deals with the outstanding question of these challenges which is virtual forces package design for the opposite requirements.

2. INTERNATIONAL AND INTEROPERABLE MILITARY CAPABILITIES

Recognition of international participation in the defence roles is also new, balancing requirement in doctrinal challenges for designing of national forces in new ages. International participation and joint defence is not new but is actual change in the 21st century. A new term of capability to be the part of international defence management is interoperability. Interoperability is signed by new doctrinal elements as the international cooperation abilities in joint operations.

In wider sense of meaning this is also the capability to make good interaction with civil instruments within national forces, between national forces, with civilian actors', etc.

(Major, Molling, 2011; EDA, 2006). This capability could be made as decentralized and tactically rapidly applicable. The cooperation with civilian actors, as the kind of interoperability, helps full efforts of unit's flexibility and adaptability to forces employing in different missions. These are the guaranties that military unit has relevancies as the defence power, obviously by organization and technology system capabilities, to defeat risk challenges of different kinds to the required reliability level. The operations of military units extend in the new missions' requirements as it civil hazard risks and population protections means help to international and homeland main infrastructure protection. But question is what is sufficient international care on the partnering level to protect joint critical infrastructure as it energy sources and supplies or other critical points and lines which violate all or the part of international consumers and commissioners using homeland responsibilities. Where are the military responsibilities beyond company or private security engaged in infrastructure protection and the control of points and lines exposed to huger asymmetric war risks or catastrophic challenges? The feature to offering help in these jobs leads into the new necessary capability for military tactical units, expressed as acceptability to the civilian private or company non military but professionally engaged actors in the security jobs.

3. EU SECURITY EFORTS AS CHALLENGES TO NATIONAL MILITARY FORCES CONCEPTS

Political and especially military strategy of the EU (Major, Molling, 2011; EDA, 2006; Solana, 2008; EDA, 2008) offers the comprehensive approach in military organization by the offer of Military EU Battle groups concept (Molling, Brune, 2011), as the attempt in organization of military joint multinational actors of the EU member states.

The EU Battle groups could be the interactive developing mechanisms for regulation and intensification military capabilities initiated by Pooling and sharing concept (EDA, 2008; Molling, Brune, 2011). EU Battle groups should be used as a starting point and as pooling initial practices, if considered as the extended new conceptual manner of forces employment. Expanded EU Battle groups concept (Major, Molling, 2011) could include more troops which would comprise a more comprehensive mix capabilities. The authors of the study (Major, Molling, 2011; Molling, Brune, 2011) suggested that the aim would be to transfer the high degree of readiness to a larger part of the EU armed forces. This requirement is not only the EU intention, but also local national principle including some east countries in their transformation processes of forces, which is more suggested by Milinovic et al. (2013).

4. CHALLENGES OF SMALL COUNTRIES FORCES AND DEFENCE PROGRAMS

Planning of EU distant operation capabilities, which makes forces ready to intervene around 6000 km (Molling, Brune, 2011) are typical expeditionary forces feature, and usually much more expensive and inappropriate for small countries. Defence planning of small countries is still comprehensive, circled in small national yards. But in reality, according to new political and economical circumstances, these countries are not able economically to maintain armed forces which cover the entire spectrum of conventional, comprehensive military forces, and refer political expectations for new defence umbrella of collective security. According to collective security obligations, they accepted military participation

in expeditionary EU capabilities, but focus it only on the small specialized tasks. Anyhow, small countries have small budgets to planed preventive and homeland territory defence operations on the appropriate levels, as the main constitutional state obligation. Comprehensive planning of defensive military missions becomes especially distinguishing nonsense when general state policy is faced with new sustainable developed strategy questions as planning of new wider infrastructure development, based on economically and politically participation in the world economy. Multinational sharing and exploitation of crucial resources and infrastructures, settled in the homeland area have also huger international risks, especially in the form of asymmetric or terrorist warfare actions. The question of implementation of military capacities in prevention, and potential asymmetric treats situations has to be considered as the national and international military forces defence tasks. At this moment the majority of small countries military forces do not have the appropriate level of capacities, technologies and organization flexibility, to be employed effectively in different missions, including civil emergency and infrastructure protection risks operations, joint with companies' private forces capacities engaged in security.

Small budget burdens of military, and other governmental agencies and institutions imposes on the national economies ultimately to develop joint, civil and military emergency capacities to share responsibilities in defence, peace protection and security risks variable tasks. This means the appropriate participation of military forces joining with other civilian armed and unarmed forces as it civilian protection, gendarmerie, police, special forces or private homeland or international security units. Universal forces for all security tasks are not possible to design. Preventive strategy as the element of forces capacity planning integrates the forces for different missions, including the EU interoperable capabilities and capacities.

The participation in the EU expeditionary forces as a part of interoperable Euro-missions requires flexible combat units designed for preventive risk operations and could give good exercise and training benefits. This helps rapid reaction training in the joint homeland missions, and makes experiences in integration with non military actors, with civilians and others, more or less organized and required groups and institutions from society and population.

Because of democratic development and free economies at the international level, military tactical units in the future will require much more civilian participation in the military joined actions and duties.

Preventive actions which have to be employed by the EU security requirements are also valid for the critical infrastructure protection, but miss actual private security and protection forces (PCSPF), as the elements of companies which take care of that. They have been rather modestly or never mentioned as possible national military forces constituents, or included in the strategy of preventive exterritorial or national interoperable actions. Finally, who is responsible for the high risk territorial technology in the situation when national military forces as modestly equipped and capacity constrained, face with catastrophic international disasters challenges on any territory, member or no member EU states? This needs to be answered, maybe after the announced treats, as late or timely sufficient only for improvised solutions.

5. OPEN STRUCTURE DESIGN OF SMALL FORCES PACKAGES

Including the capabilities of civil governmental and nongovernmental agencies and actors in joint military forces formations based on situational case are the benefit and the practice

that cannot be avoided in the homeland huger hazard disasters, but also the possible expectation in the international de-conflicting and peace keeping missions. Also, civil hazard help operations which require to be integrated in comprehensively-planned operations for the military forces have to be planed as modular constituents of battle teams packages. The example of civilians' participation in the military tactical forces is the CIMIC unit of NATO forces and UN units as well known in the former practice. The main aim of these forces are *to disharmonize and to de-conflict operational and tactical military efforts in order to stabilize a dysfunctional societies with those of civil entities doing likewise* (Valcourt, 2009; Molling, Brune, 2011).The executed core functions of these CIMIC sub-units is support to the force by leasing functions , support to the civilians by developing fast peace implementation projects, and continual liaison functions on the terrain to control the level of peace keeping reflections in the population. However, the classical role of CIMIC is not sufficient for the involvement of the army in the protection of the critical infrastructure. This type of exercise has its own component of the CCIS tasks, primarily in the area of control and support (Jeftic, Lalovic, 2011).

But this is a very small part of functions for the new challenges which could be expected in the further sustainable development of societies and their international links. Legacy and laws of defence items in small countries could be faced with problems of international forces, private, or state, which could not care too much about political dignity to protect property and to prevent the expenses of long term catastrophic risks and damage consequences.

Then state constitution and laws could be in the booby trap. The participation in CCIS capabilities tasks and homeland operability for the (CEH) tasks within CCIS capabilities missions have to accept also the capabilities of governmental non military forces and (PC-SPF), especially when they are trained and equipped for the special missions of infrastructure protection.

Table 1 shows items 1 to 7 as preventive operation engagement and military forces levels according to the capability which could be required and developed in the case of Serbian homeland constitutional obligations. Such a role of the military in its territory is acceptable given its available resources and peacetime capacity. This is a modest answer on the CCIS capability requirements preparation by tasks planning in international and homeland operability and participation frame to (CEH) tasks within trained capabilities for the part of forces. Preventive task No. 8 to help private and international companies' security capacities which control critical infrastructure is added as possible preventive task, but not regulated constitutionally. Does that mean that private property of foreign companies is not under the protection of homeland military forces, or it means that foreign private or governmental forces have all legal rights to protect their exterritorial infrastructure property? Regardless of the political fog which covers this question, the main defence regional treaties are inspired to bridge these risks.

From the considered point of view, the best design for military forces is to make flexible and mission adaptable force packages for the lowest structure as possible. This sets up challenges which have to answer to the following questions:

- Will the military organizations be able to adapt their lower tactical formations to the participation of civilian actors in the open architecture formation concepts and to face with the employment in the new types of civil threats challenges by disrupting principles of tactical roles about homogeneous minimum battle forces organization?

- Can the military tactical leaders take command and planed actions in the cases of both international and homeland interoperable units filled with virtual armed and disarmed organized non military and military participants and groups?
- Can the homeland tactical units take and share responsibilities and appropriate readiness for the international critical infrastructures protection roles, joint with private professional security units, which could be organized and appropriately equipped on the homeland or international levels?
- How to plan and accord organization structure of tactical military units to be adaptable in accepting professionals participants and civil actors formations which are trained for the civil hazard risks, civil protection, special civil missions or other security actors of civilian society, and to be at the same time effectively organized in the full combat engagements at the area of responsibilities? Also the question of training and appropriate equipping of joint units and modules is another distinguishing item, which has to be considered at the operational level of missions planning.

Table 1.

No.	Preventive Tasks	Readiness	Rapid Reaction Time	Forces	Basic Quality
1.	Civil humanitarian emergency	Readiness 5–10 days, for periodical or continual missions, depending on the situation	Immediate	Company BT or squad BT	interoperability rapid projection
2.	Peace keeping			Company BT or squad BT	sustainability
3.	Combat tasks in crises management and stabilization			Company BT or battalion BG	interoperability sustainability rapid projection
4.	Disarming operations			Company BT	sustainability
5.	Military consultation advising and military help			Command squad or platoon BT	interoperability
6.	Clashes stopping and prevention			Company BT or battalion BG	sustainability rapid projection
7.	Stabilization of peace keeping			Squad BT Company BT or battalion BG	interoperability sustainability rapid projection
8.	Homeland or international Missions with governmental or nongovernmental non-military forces(Private and/or company forces integration in the main infrastructure protection tasks)	*Readiness 5 – 10 days, for missions*	Immediate	*Squad BT*	*interoperability rapid projection joint* (PCSPF) *mission joint civil –military actions (interoperable or homeland operable)*

To answer to these questions seems simple and based on legal obligations. Practically the suggestion is to add private non military forces employment or governmental non military forces as the eighth hazard help task required by military forces, referred in Table 1 could be proved as additional military obligation. Also state could give exclusive rights to foreign forces to protect international or foreign company's infrastructure. But, everything which could be covered by law is not always understandable by itself, and could be missed for longer application because of the concern of political and strategic misuse, both on homeland or international level. This paper offers small functional contribution in the approach to new virtual structure of battle teams which provides modular concept of new functional formation, framed namely for smaller parts of military national units redesigning to fulfil different requirements, including the integration of private professional security forces in their structures. The level would be about 200 people of mixed participants, military and others, virtual by formation, with the aim to respond to different challenges from special battle operations, peace keeping operations to the civil emergency intervention. This frame could be taken only as the principle design, but ready to accept different and virtual tasks by rapid rearranging by high operational command, using both homeland and international modular components for homeland oriented risk missions. This could be partnership formation usable in two directions, applied in the homeland as joint international or internationally applied as homeland integrated defence and security military formation.

6. MODULAR UNITS AND ADAPTABLE FORCES IN THE FORM OF TASK TEAMS – GENERAL APPROACH

The elements of modular concept contain the principles which require the design of modules and appropriate force packages for new compromising opposing opportunities but which are rapid adapted for different operations. To be modular in structure at low levels, largely self-sustaining and capable of operating jointly with traditional formations as well as accept their disaggregating elements into the new reinforced virtual teams could be the key organizational capability of new concepts for small countries and armies. General approach for the land forces battle teams require some elements that should be taken from frame recommendations by Milinovic et al. (2013), but could vary from special required operations and missions to the conventional employments of force packages.

Modular packages of military units, especially as balancing designed by light military forces and civilian actors, security and other unit modules, could achieve a higher level of joint efficiency by adaptable integration, composed of land, air, and maritime precision task function elements, like intelligence and counter intelligence elements, civilian hazard help operations elements, risk teams, focused logistics elements, with a goal of delivering military help effects in a more flexible way. All these requirements are opposite but also possible to join with rigidly determined functional technology required for a mission. General example of modular forces seems to be the frame for modular changes of formation elements, and could consist of:

- FIXED COMMAND CORE composed of:

1. Commander with protection platoon supported by two squad teams virtually designed
2. First squad team as composed of special officers or joint civilian command authorities depending on the mission. This team is composed for the CCIS tasks in the stability

types of operation, civil emergency and help operations CEH or, in full military operations, D3&I, (Dislocating, Destroying, Disintegrating &Isolating) tasks and actions.

3. Second squad team is Information command squad. In principle, this team is information and intelligence/counterintelligence and security source and links CIMIC and other civilian actors and groups to help their tasks and operations. It could consist of information intelligence and civil links on the squad level, as intelligence platoon, security platoon or CIMIC platoon.

- MAIN TERRITORIAL CONTROL MISSION ELEMENTS could be composed of the forces for rapid projection or for specialized operations, as possible open links for the variable actors.
- INDIRECT ACTION ELEMENTS could be support modular squad groups as replaceable elements composed of the forces which provide special support depending on the mission or tasks. This module is under the control of staff vice commander and commander deputes.
- SUSTAIN COMBINED LOGISTICS ELEMENTS are focused logistics teams mixed of replaceable and fixed elements composed of group members.

All could be designed as the variable member groups depending on the mission as D3& I, CCIS, or CEH, military operations. Private control and patrol groups as security part could find the place in the territorial mission elements .Variable logistic groups for modular indirect and direct support contributing with the modular squad group are also the elements which could be directly linked to the variable mission elements of the designed teams. An example of composition based on exposed general frame of this virtual formation is given within Figure 1. as mixed (green and yellow participants) aimed for one of CCIS military, or for the CEH emergency tasks, where the private security company elements could take part.

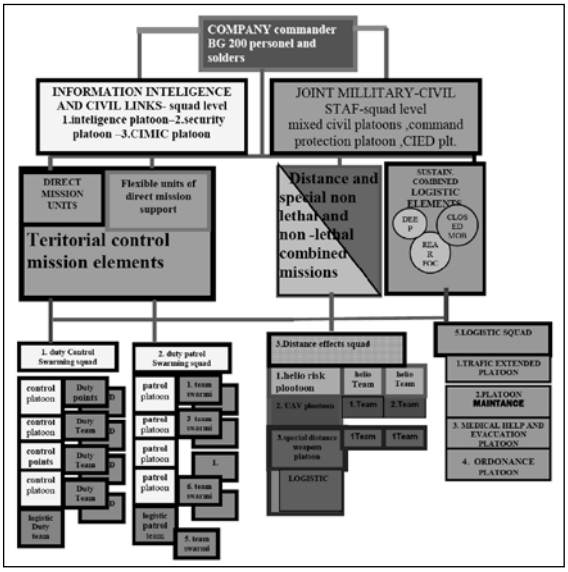


Figure 1 - Composition Principles of Millitary Modular flexibile Company Battle Group for CCIS Tactical Operations with total No of 200+

Unit structure may have a form of evolved when used in the territory of their own country. In that case their autonomy of action is not dominant and it will be able to recline significantly by the existing rescue and protection systems. The second question that must be answered is the chain of command and the responsibility, but it is primarily a matter of legislation and internal organization of the security system.

7. INSTEAD OF A CONCLUSION

Task mechanisms of forces are the question of how and what to develop at the appropriate level of efficiency to measure the quality of forces employed in the operations.

These tasks could be grouped in the main three military efficiency measures such as command and control efficiency in decentralized environment, the efficiency probability of basic fire power and manoeuvre function, the efficiency probability of protection and sustainment of over all types. But military tasks measured by efficiency are hard to be explicit representatives of multifunctional forces engagements. Each function contains technology performances as one of the most important fact capabilities influence factors. Also, each of the selected functions exposes different efficiency requirements for different tasks in mission's characteristic for the new roles of forces designed as the multipurpose and modular. Figure 2 represents some of the variable efficiency elements important for flexible mission requirements of modular combat units. The same battle team could take tasks with distinguishing one function as relevant (blue signed performances) and some other missions could require red signed performances evaluated in situation of mission.

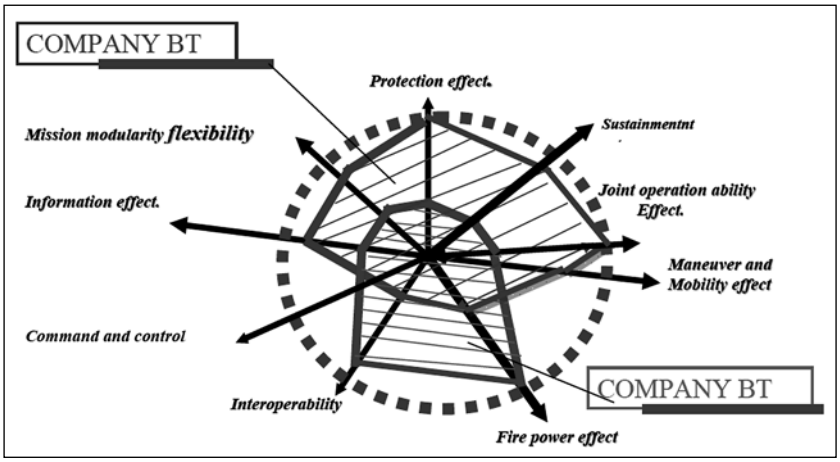


Figure 2 - Modular units analysis in relative estimated performances for two different tasks

In each of the efficiency task functions some performances could be more or less important.

This principle could be recognized as the intensive and extensive in particular efficiency performances selection and could mean the orientation on the best capabilities selection for the particular mission. What is more or less important for some combat performance can be expressed by independent mathematical variables if efficiency of some welcome or not welcome capability depends of their relevance in the mission. Mathematical model

as possible estimator could be designed as summarized expert estimations and helps it to get orientation in the expected efficiency for the adaptable forces design according to Przemieniecky (2000). That could mean the evaluation of technology training education special skills mobility or any other military quality constituent could get efficiency function distribution of relevancies arguments. Functions are namely probability rooted, but their distribution could be determined by random variable as the argument of relevance. This variable has to express expert opinion and to limit this opinion by real estimations especially when this final decision leads into big expenses. Relevance is the argument to design more real expectations of efficiency laws and to exclude unreliable experts estimated weight coefficients. Relevancies argument as variable values taken from mission to mission can be linked with the observed dynamics or time available requirements in planning functions which determines efficiency probabilities in particular or overall military units' estimations. This variable has to be named as the measure of adaptability or functional task relevancies coefficients which require special considerations beyond this paper contents.

REFERENCES

1. D. P. Valcourt, Lieutenant General, U.S. Army, Deputy Commanding General (2009), The army capstone concept, Tradoc pam. 525-3-0, Department of the Army Headquarters, United States Army Training and Doctrine Command Fort Monroe, VA 23651-1047 21 December 2009, http://www.tradoc.army.mil/tpubs/pams/tp525-3-0.pdf
2. C .Major ,C. Molling , (2011), EU Battle groups, what contribution to the European defence – progress and prospects of European rapid response FORCES, SWP Research Paper, Berlin Institute for International and Security Affairs, June 2011, Berlin, Germany, http://www.swp-berlin.org/en/publications/swp-research-papers/archive/2011.htm1
3. European Defence Agency, (2006), EU governments launch new plan to build defence capabilities for future ESDP operations, Brussels, 14 December 2006 http://www.eda.europa.eu/News/2006
4. Javier Solana, (2008), Future trends from the capability development, European Defence Agency, Brussels, 8 July 2008, www.eda.europa.eu/Libraries/Documents/CDP_brochure.sflb.ashx
5. European Defence Agency (2008), European armaments co-operation strategy, Brussels, 15 October 2008, http://www.eda.europa.eu/Strategies/Armaments
6. C.Molling, S, C. Brune, (2011). The impact of the financial crisis on European defence, policy , Directorate general for the external policy, Study, European Parliament, Brussels, 2011, http://www.europarl.europa.eu/activities/committees/studies.do?language=EN
7. C. Major, (December 2010). Civil military headquarters for the EU. SWP comments, Berlin Institute for International and Security Affairs, Germany, http://www.swp-berlin.org/en/publications/swp-comments-en/archive/2010.html
8. J.S. Przemieniecky, (2000). Mathematical methods in defence analyses, Third edition, AIAA, Education Series, Reston, Virginia, USA,
9. Milinovic M., Jeftic Z., Forca B., Miscevic T., Jeremic O. (2013). Contribution of European initiatives for battle teams integrations based on initial technology capabilities, Technics Technologies Education Management (TTEM-Journal), March 2013, ISSN: 1840-1503.
10. Jeftic Z, Lalovic M. (2011), Civilno vojna saradnja, Medija Centar Odbrana, 2011, Beograd, ISBN 978-86-335-0310-5

UDC 726.9:75.041.5
ID 176374796

Želimir Kešetović, Nenad Putnik
University of Belgrade, Faculty of Security Studies
zelimir.kesetovic@gmail.com
nputnik@fb.bg.ac.rs

Marko Rakić
Ministry of Foreign Affairs of the Republic of Sebia
m.rakic01@gmail.com

POSSIBILITIES OF IMPROVING CRITICAL INFRASTRUCTURE PROTECTION IN COUNTRIES IN TRANSITION

Abstract: Large infrastructure systems such as transportation, water supply networks, energetic, chemical and nuclear industries, and information and communication technologies enable normal functioning of the contemporary society. That is the reason why the question of their adequate protection is one of the principal and the most important security challenges of the "modern age". Countries in transition are in a specific situation, facing deep transformations in all spheres (democratization of the society, overcoming authoritarian legacy, transformation of social property, deteriorating infrastructure, outdated technologies, etc.). They heavily fall behind the developed countries which have by now developed the effective systems of critical infrastructure protection. They also face other problems that make it difficult to establish the appropriate protection system (insufficiently developed democratic institutions, the absence of appropriate economic policies, the lack of clearly identified sources and forms of endangering critical infrastructures, the lack of clear classification of critical sectors and a coherent legal framework which regulates this area). While identifying the said problems with which the majority of countries in transition is faced, it is important to bear in mind that each of these countries has certain specificities which make it difficult to give universal conclusions and recommendations. In this paper, we used the comparative method to try to identify critical sectors and elements which can contribute to the improvement of critical infrastructure protection in countries in transition, through an overall analysis of different critical infrastructure protection systems in technologically advanced countries.

Keywords: *critical infrastructure, countries in transition, critical infrastructure protection*

1. INTRODUCTION

The introduction of the concept of critical infrastructure protection on the public agenda of the Western countries can be explained by the changes which at first originated in the perception of threats and growing interdependence of various infrastructure elements, which made social system extremely vulnerable, while risks and threats increased. In the past few years the approach to the concept itself, as well as the perspective on the critical infrastructure vulnerability changed. Vulnerability of critical infrastructure and the society as a whole used to be related to the problems referring to the functioning of "high-risk" technologies, while nowadays critical infrastructure and its protection are considered to be the question of vital importance for national, regional and even global security.

The mentioned phenomena and problems, regarding efficient protection of critical infrastructure, were pointed out by Charles Perrow in 1984, by introducing the concept

of "normal accidents" which referred to system vulnerability of high-risk technological systems such as, for example, nuclear power plants and genetic engineering. Perrow states and gives arguments in support of the assumption that managing complex technological systems can be improved by taking into consideration man and technology induced security risks in a decision-making process, as well as that in spite all the efforts accidents and disasters can hardly be avoided, as a result of the great complexity of the tasks assigned to the management system. In his opinion, "high-risk technologies represent the creation of social and state systems and they are not individual acts or a product of an ideology" (Perrow, 1999, p. 351). Perrow disputes nuclear power production, DNK engineering and air traffic control systems, because according to his words "these systems come into being and survive thanks to concatenations of political bargains, privatizations and careless attitude towards the expenses that the society has to defray" (Perrow, 1999, p. 351).

In 1986, a German sociologist Ulrich Beck conducted research regarding the implications of high-risk technologies on social and political dynamics. In this research study, he discusses everyday risks which a society faces, as well as paradigmatic characteristics of future risks. Beck tries to establish an early disaster identification system, and draws attention to the existing practices and techniques in use while forecasting global risks. Sometime later, the mentioned risk assessment practices and techniques have become structural parts of the national security system (Beck, 2009; Rothstein, 2006).

After more than thirty years, Perrow's interpretations of critical infrastructure system vulnerability and Beck's research of risk society are still contemporary. In his book from 1999, Perrow states that accidents such as the Chernobyl, Bhopal and Challenger disasters, which had a direct and indirect impact on the whole world, are just a confirmation of the fact that not many things have changed in the industrial world since 1984. He also asserts that no significant improvement in preventing accidents has been made, but that a great improvement has been made in interpreting accidents (Perrow, 1999). Perrow concludes that new perceptions of threats to critical infrastructure are largely related to the traditional ones, but that in the process of interpreting them, security risks of the "modern age" must be taken into consideration.

2. CONTEMPORARY APPROACH TO THE CONCEPT OF CRITICAL INFRASTRUCTURE PROTECTION

A contemporary concept of critical infrastructure notion refers to the assets, including physical and computer systems which are of vital importance to securing economic and political stability of a country (Radvanovsky, McDougall, 2010). These are, in fact, a framework of interdependent networks and systems encompassing certain industries, institutions (including people and procedures) and capacities for distribution which offer a reliable flow of goods and services necessary for defensive and economic security of a country, undisturbed functioning of the government on all levels, as well as of the society as a whole. Critical infrastructure encompasses energy systems, telecommunications, transportation, water, food, banking systems and finances, civil administration, including both public and private sector, but it is not limited only to those (Radvanovsky, McDougall, 2010). None of critical infrastructure classifications can be regarded as absolute, and they are mainly based on expert and/or political decision-making estimates.

Today, we can talk about increasing number of infrastructure sectors that are becoming transnational – information and communication overcame national state borders a long time ago, and the same goes for transportation sector (road, railway, air, and water transportation), telecommunication sector, chemical industry, as well as nuclear industry. Financial sector is especially significant as it has become largely transnational, and that was shown by the world economic crisis which started at the end of 2007 in the USA and it went from national to international level very quickly thus leading to a global recession, shaking the foundations of national market economies and questioning free market efficiency which was indisputable up to that moment (Global Economic Crisis, August 5, 2013).

All this heavily complicates establishing efficient critical national infrastructure protection[1] and develops new approaches in order to prevent possible threats and risks. Accordingly, the efficient protection of critical infrastructure must involve social activities and objects necessary for normal functioning of a system. This includes people, physical property and information and communication systems essential to the national and supranational security, economic stability and legal order and security. The methods and means of protecting critical infrastructure deter or mitigate attacks on critical infrastructure caused by people (terrorists, criminals, hackers, etc.), natural disasters (earthquakes, storms, floods, etc.), fires and explosions in nuclear and chemical plants. Basically, protecting critical infrastructure means protecting the assets considered invaluable to society (Radvanovsky, McDougall, 2010).

3. CRITICAL INFRASTRUCTURE PROTECTION POLICIES IN TECHNOLOGICALLY DEVELOPED COUNTRIES (USA, RUSSIA, JAPAN)

In the United States of America critical infrastructure, according to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act)[2] of 2001 "refers to systems, services and plants, physical and virtual, that are so vital to the USA that their incapacity or destruction can have a debilitating impact on security, national economy, public health, or any combination of those matters" (Macaulay, 2008, p. 8).

According to this definition, 17 critical infrastructures and key resources have been identified, and roles and responsibilities for their protection have been established (*Homeland Security Presidential Directive 7 - HSPD-7*, *December 2003*) (Macaulay, 2008). The Department of Homeland Security identified another critical sector in 2008 – Critical Manufacturing Sector. Therefore, the current list of critical sectors contains: information technologies, telecommunication, chemical plants, industrial capacities, dams, commercial nuclear reactors, materials and waste, government facilities, transportation system, emergency services, postal and shipping, food and agriculture, healthcare and public health, water and wastewater systems, energy – including production, refining, storage, and distribu-

1 The term critical infrastructure protection (CIP) was first used by President Clinton in 1996, after the terrorist act on the Alfred P. Murrah Federal Building in Oklahoma in 1995 (Executive Order, July 1996). This Order emphasized certain national infrastructures, that were of vital importance to the USA, and whose incapacity or destruction would have a great impact on the defence, economic security and well-being of the citizens.

2 USA PATRIOT Act came into being as a response to the September 11 attacks that befell the USA on September 11, 2001. It was passed by Congress, and signed into law by President George W. Bush on October 26, 2001.

tion of petroleum and gas, electric power, banking and finance, national monuments and icons, defence industrial base and critical manufacturing (Macaulay, 2008).

While the idea of critical infrastructure protection was still in its beginnings, the system was organized so that two agencies shared the largest part of responsibility – Critical Infrastructure Assurance Office – CIAO, which used to be housed in the Department of Commerce and National Infrastructure Protection Centre which was an organization within Federal Bureau of Investigation-FBI. However, after issuing the already mentioned executive orders, their functions were transferred to the Department of Homeland Security. 9/11 attack that befell the USA on September 11, 2001 prompted restructuring of the whole organizational framework of national security protection, including organizational framework of critical infrastructure protection. In March 2003, 23 federal agencies and numerous offices were integrated into one organ – the Department of Homeland Security – DHS (Who Became Part of the Department, August 6, 2013). The Department of Homeland Security currently coordinates the activities of several federal, state and local administrations and encompasses a great number of agencies which perform various tasks regarding state security (Who Became Part of the Department, August 7, 2013). Within the Department of Homeland Security there are agencies dealing with critical infrastructure protection and they are connected with National Protection and Programs Directorate, whose task is to reduce both physical and virtual threats to state security (National Protection and Programs Directorate, accessed August 7, 2013). Two offices, components of the Department of Homeland Security, deal with critical infrastructure protection: the Office of Infrastructure Protection – OIP and the Office for Cybersecurity and Communications – SC&C.

The Office of Infrastructure Protection (The Office of Infrastructure Protection, August 7, 2013) coordinates the activities in various sectors regarding critical infrastructure protection and key resources. Its missions include: management of a robust organization which deals with critical infrastructure and key resources identification, coordination and protection; development, implementation and updating National Infrastructure Protection Plan; coordination and assistance during 18 USA critical infrastructure sectors and key resources vulnerability assessment and informing owners and operators about the infrastructure safety standards that have to be fulfilled; monitoring administrations responsible for managing critical infrastructure as well as information sharing; information collection, risk and threat to critical infrastructure analysis and providing information to government and private sector on how to prioritize during the process of resources allocation.

The Office of Cybersecurity and Communications (The Office of Cybersecurity and Communications, August 7, 2013) coordinates, together with private sector, the activities regarding threat identification, risk management and raising awareness on potential crisis situation. In order for a whole country to be prepared for catastrophic accidents which could damage or even destroy the network of information and communication technologies, the Office for Cybersecurity and Telecommunications implemented three programs – the National Communication System (About the Office of Emergency Communications, August 7, 2013), the National Cyber Security Division (National Cyber Security Division, August 7, 2013), the Office of Emergency Communications (About the Office of Emergency Communications, August 10, 2013).

One of the most important preconditions for the efficient protection of critical infrastructure in the USA is the active cooperation between public and private sector. The Presi-

dent's Commission on Critical Infrastructure Protection – PCCIP concluded that "the need for infrastructure protection further causes the need for cooperation and shared responsibilities between private and public sector" (President's Commission on Critical Infrastructure Protection, *Critical Foundations*. October 1997, p. 35, August 10, 2013). Ever since then, public-private partnerships and quality information sharing between private and public sector represent one of the most important tasks in the process of critical infrastructure protection in the USA.

When it comes to the Russian Federation, during the past few years a significant improvement regarding critical infrastructure protection was made. National security and economic well-being of this country depend on the actual degree of critical infrastructure protection, and this is going to be even more important, especially when it comes to the information infrastructure. We can conclude how much Russia cares about the information infrastructure security based on the efforts it puts in the field of human rights protection in the information sector, as well as based on information and telecommunication systems protection in various spheres of public life.

This is a list of infrastructure sectors considered critical in Russia:

- - Economy;
- - Domestic and foreign policy;
- - Science and technology;
- - State information and communication systems;
- - Defence;
- - Judiciary;
- - Emergency services.[3]

Earlier research studies regarding the Russian critical infrastructure policy were mainly related to military reform, modernization of military-industrial complexes, economy, and foreign policy and similar. On the other hand, Russia was frequently mentioned in Western discussions about cyber threats. In this context, Russia is considered to be "the home of the most dangerous cyber crime systems in the world" and the place where intelligence agency uses "an intimidating surveillance system, named COPM-2 (SORM-2)" (Glenny, 2011, p. 18).[4] The First Chechen War (1994-1996) and "the first world cyber war" between Russia and Estonia in 2007 (Kaiser, 2012) represent the examples of Russian ability and readiness to engage in the battle against cyber crime. Simultaneously, there is a public debate in Russia on state industry and other critical assets vulnerability, and there is the idea that it can be fixed by improving information security (Mikhailov, 2010), which contradicts a previously stated fact that Russia has a considerable capability in the field of information infrastructure.

The first set of documents used to redefine state interests and goals in the field of critical infrastructure protection (the documents referring to defining critical buildings and critical infrastructure) was issued in December 2003. The state policy of improving chemi-

3 What presents the biggest problem for Russia, when it comes to critical infrastructure protection is a great number of buildings considered to be critical (about 45,000) and the number of people who live in so-called high risk zones (over 90 million).

4 SORM-2 is a system managed by the Federal Security Service in order to collect all the data that appear on the Internet in Russia. Similar measures of communication surveillance are undertaken by the National Security Agency (NSA), which is confirmed by the recent disclosure of the details about the secret program "Prism".

cal, biological and nuclear security set a foundation for the reform of the whole critical infrastructure policy, as well as for the shift from strictly security component towards the policy of protecting critical assets from terrorist attacks and other threats to national security and socio-economic development (the President of Russia V. Putin, 2003). In August 2005 *a concept of federal system monitoring* of critically important assets was presented, whose interruption of functioning could lead to negative consequences on the economy and administrative unity of the country, as well as on the security and well-being of citizens (Распоряжением Правительства РФ, 2005).

A new document named "Conceptual foundations of state policy in the field of protecting citizens and cricitally important and potentially dangerous assets from crisis situations caused by natural and technological disasters and terrorist acts", was issued in September 2006 (the President of Russia, V. Putin, 2006). The said document defined a state strategy and identified possible threats to critical infrastructure.[5] In May 2009, a Concept of national security (later Strategy) was presented and it gave a completely new tone to the critical infrastructure protection policy. The first sentence of the Strategy states the following: "Russia has overcome the consequences of the systemic political and socio-economic crisis from the end of the 20th century...the state now has the potential to strengthen its capacities and to defend its interests, as a key player within multipolar international affairs" (Russia's National Security Strategy, 2009). This statement shows that there is a general opinion of the Russian government that despite world economic crisis, which has started in 2008, a modernization within certain economy sectors will be continued in the future.

When it comes to cooperation between private and public sector in Russia, there used to be a long-time practice of applying measures of infrastructure protection only in case of infrastructures closely related to the military, government systems and institutions and other state institutions and services. Nowadays, the situation is different and a lot of effort is put into attending to the issues of protecting infrastructure owned by the private sector, which is mostly noticed in the sector of information infrastructure protection – the development of commercial security products in the field of IT sector on the market in Russia is increasing, but still there are problems such as financial restrictions and the lack of IT experts.

The cooperation between private and public sector in the field of information security is still limited in comparison to other developed countries. This is the result of the fact that for many small and medium enterprises in Russia the information infrastructure protection and security are not the biggest issue. However, both sides – public and private sector, are currently changing their attitudes and they are constantly improving their mutual cooperation.

Critical infrastructure protection policy in Japan was defined in 2005 by The Action Plan on Information Security Measures for Critical Infrastructures, issued by the Information Security Policy Council. It states that "critical infrastructure consists of agencies which provide services absolutely necessary for functioning of Japan's society and economy. In

5 Identified threats: an increasing danger from technological and natural disasters, as well as increase in the number of such disasters; increase in the number of potentially risk buildings, many of which are located in big cities and densely populated areas; physical dilapidation and technological outdatedness of systems and complexes created to improve security of risk objects; a low level of education and staff training, the lack of technological discipline, a low level of security culture; insufficient financial means for critical infrastructure improvement; increased danger from international and domestic terrorism and crime rate increase.

case a critical infrastructure interruption occurs or if the functioning of a certain infrastructure is at risk, the functioning of the whole society and economy of Japan will be severely impacted" (Information Security Policy Council, p. 2, August 25, 2013). The Action Plan formulates ten critical infrastructure sectors: telecommunication; government and administrative services; civil aviation; railways; logistics; electricity; gas; medical services; and, water supply.

According to that Plan, the Ministry of Internal Affairs and Communications (Ministry of Internal Affairs and Communications, August 25, 2013) is responsible for creating critical infrastructure protection strategy in Japan. As its name suggests, the Ministry deals with issues related to the safety of all types of communications. During the past few years, the measures regarding critical information infrastructure safety, communication safety, information technologies and Internet safety were issued. In the field of protecting other segments of critical infrastructure, Japan works on coordinating its norms with the international critical infrastructure protection laws. Furthermore, the Ministry works on developing cooperation with other countries in the field of critical infrastructure protection. Policies regarding information safety are divided into three groups: network security, terminal and equipment security and individual (user) security. The Ministry issues a Report on the State of Information and Communication Technologies in Japan annually. The Report always has separate chapters regarding privacy protection and information security. The aim of these Reports is strengthening the cooperation between private and public sector regarding information security issues. The Ministry, also, conducts research concerning efficacy of protection measures against cyber attacks and various other issues regarding information and communication technology security and data security.

The Report on information and communication technologies in Japan, deals with problems regarding information society problems in this country year after year. The Ministry stresses that all the policies regarding information society creating (officially came into being in 2010) are based on four principles: ubiquitousness, universality, being oriented to users and uniqueness. The point of information society development (named u-Japan) lies in creating the possibilities for users to connect to any network, any time and any place, with maximally safe information exchange. The partnership of private and public sector is an important segment of critical infrastructure protection in Japan. Thus, for example the comprehensive strategy on information security from 2003 already contains in its part the suggestions about the cooperation between public and private sector (Comprehensive Strategy on Information Security: Executive Summary, August 25, 2013). The first national strategy on information security and the Action plan on security measures for critical information protection, also, highlighted the need for establishing special organizations whose task would be formulating the measures of protection, technical operations, and analysis and taking actions when it comes to critical infrastructure protection within each sector. These organizations would be in charge of secure data exchange between state organizations and private sector. The organizations would obtain information from Cabinet Secretariat for infrastructure protection and they would forward them to private sector – critical infrastructure owners and operators.

4. THE ISSUE OF CRITICAL INFRASTRUCTURE PROTECTION IN COUNTRIES IN TRASITION

Countries in transition are in a specific position, facing a deep transformation in all spheres. These countries have to put a lot of effort in order to establish democratic institutions and overcome the burden of communist legacy, because building democratic structures is one of prerequisites for efficient dealing with conflict situations through adopting various resolutions. The elements of resolutions regarding conflicts and establishing peace and stability, such as negotiation, dialogue and trust building are the key to a successful transition to democratic system (Engelbrekt & Fröberg, 2005). During transition from one socio-political system into another, these countries face numerous problems that do not exist in stable democratic countries. Joining the free market, mainly without adequate economic state policy, leads to spreading poverty and disappointment among wider social classes thus putting key decision makers into a very complicated situation. A bad economic situation can frequently lead to crisis.

One of the problems which countries in transition face, and which is connected with economic growth rate, is outdated technology in comparison with the developed countries of the Western Europe and world. A sudden and increasingly fast development of information-telecommunication infrastructure, satellite communications and the Internet, requires a continual technological development as well as constant employee training which requires significant financial resources. Countries in transitions are not often in a position to allocate resources for improving technology and conducting new employee training programs, which directly affects the efficiency of crisis management and vital infrastructure protection system (Vuletić, 2011).

Moreover, the majority of countries in transition do not have clearly identified sources and forms of critical infrastructure jeopardizing, as well as a precise critical sector classification (Vuletić, 2011). One of the main reasons for such a state in this field is worn out infrastructure that cannot respond to requests and standards laid down by the EU and NATO. Outdated critical infrastructure protection programs, dating back to the age of socialism and based on the Cold War postulates (according to which the military sources and forms of security jeopardizing are the most dominant ones), cannot put an end to contemporary security risks and enable the efficient functioning of infrastructures of vital importance. In order to establish an efficient critical infrastructure protection in countries in transition, it is necessary to modernize the outdated infrastructure assets which require large investments into reconstruction of the whole sectors (Christian von Hirschhausenand Berit Meinhart, 2001).

Also, one of the more important problems countries in transition face, when it comes to crisis management and critical infrastructure protection, is security sector transformation. Private security is closely related to critical infrastructure protection, because a great number of these infrastructure buildings are under the protection of private security companies. A successful functioning of the private security sector in the majority of the Western Balkan countries is not possible due to the lack of legal basis and theoretical support (Талијан, August 26, 2013). The absence of a coherent legal framework in this sphere complicates the cooperation between private and public sector, and that cooperation is actually the key to a successful critical infrastructure protection and efficient crisis situation management (Nickolov, 2005).

This problem is additionally hindered by inefficient private-public partnership. In most countries in transition, a significant part of infrastructure is privately owned or in the process of privatization and cooperation between infrastructure owners and public institutions is very bad. One of the main reasons for such a situation is the absence of legal framework which would force the owners and operators to undertake necessary steps for establishing the efficient cooperation with public institutions (Tagarev & Pavlov, 2007).

While identifying the mentioned problems that most countries in transition face, it is very important to bear in mind that each of these countries has certain specificities (territory size, economic development, political and historical circumstances, international status, culture, tradition, etc.), and because of that it is really difficult to draw universal conclusions and make generalizations. It is a fact that these countries have different experiences regarding the transition process, and the most successful countries should be the ones to set an example. The experiences of successful countries in transition and the developed countries could be very useful to the countries in the phase of developing a crisis management systems and policies for protecting infrastructure of vital national interest.

5. CONCLUSION

According to the overview of critical infrastructure protection policies in the highly developed countries, it is possible to establish a mode of critical infrastructure protection which could be applied to the countries in transition. By identifying key sectors included in strategies of almost all countries with clearly defined critical infrastructure policy, we can establish the following classification of critical sectors:

- Energy (production, distribution and storage of energy generating products – gas, petroleum and electricity);
- Information and telecommunication technologies (electronic communication, data transfer, information systems, providing audio and multimedia services);
- Transport (road, railroad, air, water);
- Health (hospitals, pharmaceutical industry);
- Water (drinking water supply, dams, waste waters, protecting water);
- Food (production, food supply, food safety, intervention stocks);
- Finances (banking, stock exchanges, investments, security and payment systems);
- Public services (law enforcement, emergency services).

In addition to adopting a strategy and precise critical sector classification, it is necessary to improve information exchange system which is important for creating an efficient early warning system. One of the key steps in creating an efficient early warning system implies forming a team for emergency situations in the field of information communication technologies.[6] In many developed countries there are similar teams which closely cooperate on a daily basis and build a mutual database which possesses all the relevant information regarding potential and actual threats to critical infrastructure. Also, the mentioned database contains the data on positive and negative experiences of certain countries in solving problems related to critical infrastructure protection. The mentioned teams should work

6 One if the first and most famous is certainly CERT (Computer Emergency Response Team) from Carnegie Mellon University in the USA, while in European and Asian countries the most frequently used acronym is CSIRT (Computer Security Incident Response Team).

both on prevention and overcoming the existing crises and protecting country's internet environment from potential cyber attacks.

It is necessary to establish or authorize a state organ or institution whose job would be to coordinate shared activities within the early warning system model. That role would primarily refer to surveillance, risk assessment, timely warning and forming proper reaction mechanisms in case endangering of a certain critical infrastructure occurs. Also, an efficient early warning system should have analysis and data exchange centres, like the countries with the developed critical infrastructure protection systems do. The main role of these centres would be providing information about threats, vulnerabilities and incidents which could endanger critical infrastructure.

Making and adopting the Law for critical infrastructure protection and regulating the cooperation between public and private sector should be the basis for the stated proposals. If there is no coherent legal framework which regulates public-private partnership functioning (which is the case in most of transition countries), it is not possible to establish an efficient critical infrastructure system.

REFERENCES

1. About the Office of Emergency Communications. http://www.ncs.gov/about.html (accessed August 7, 2013)
2. About the Office of Emergency Communications. http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm (accessed August 10, 2013)
3. Beck, U. (2009). *World at Risk*. Cambridge: Polity Press.
4. Christian von Hirschhausenand Berit Meinhart. (2001). *Infrastructure Policies and Liberalization in the East European Transition Countries:Would Less Have been More?*, Proposal for the Annual Congress of the European Economic Association Université de Lausanne, Switzerland.
5. Comprehensive Strategy on Information Security: Executive Summary. http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf (accessed August 25, 2013)
6. Glenny, M. (2011, October 31). The Cyber Arms Race Has Begun, *The Nation*.
7. Global Economic Crisis. http://yaleglobal.yale.edu/content/global-economic-crisis (accessed August 5, 2013)
8. Information Security Policy Council. *Action Plan on Information Security Measures for Critical Infrastructures*. http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf (accessed August 25, 2013)
9. Engelbrekt, K., & Fröberg, M. (2005). *Managing Political Crises in Bulgaria: Pragmatism and Procrastination*. Stockholm: Elanders Gotab.
10. Kaiser, R. (2012, October 4). *Estonia and the Birth of Cyberwar*. Presentation at Aleksanteri Institute.
11. Macaulay, T. (2008). *Critical Infrastructure - Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies*. London: CRC Press.
12. Михаилов, А. (2010, November 17). Критичесская инфраструктура оказалась в кибероп асности. *BusinessFM*.
13. Ministry of Internal Affairs and Communications. http://www.soumu.go.jp/english/index.html (accessed August 25, 2013)
14. National Cyber Security Division. http://www.dhs.gov/xabout/structure/editorial_0839.shtm (accessed August 7, 2013)
15. National Protection and Programs Directorate. http://www.dhs.gov/xabout/structure/editorial_0794.shtm (accessed August 7, 2013)
16. Nickolov, E. (2005). Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations. *Information and Security Journal*, 17, 105-119.
17. Office of Infrastructure Protection. http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm (accessed August 7, 2013)
18. Office of Cybersecurity and Communications. http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm (accessed August 7, 2013)
19. Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies*. Princeton: Princeton University Press.

20. President's Commission on Critical Infrastructure Protection, *Critical Foundations*. October 1997. http://www.fas.org/sgp/library/pccip.pdf (accessed August 10, 2013)
21. Президент РФ В. Путин. (2003, Декабр 4). Указ Пр-2194: Основы государственной политики в области обеспечения химической и биологической безопасности РФ на период до 2010. года и дальнейшую перспективу.
22. Распоряжением Правительства РФ. (2005, Август 27). Концепция федеральной системи мониторинг критически важных объектов и/или потенциально опасных объектов инфраструктури РФ и опасных грузов, Но. 1314.
23. Президент РФ В. Путин. (2006, Сентябрь 28). Основы государственной политики в области обеспечениябезопасности населения РФ и защищености критически важных объектов и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов.
24. Radvanovsky, R. & McDougall, A. (2010). *Critical Infrastructure, Homeland Security and Emergency Preparedness*. Second edition. New York: CRC Press, Taylor & Francis Group.
25. Rothstein, H. (2006). The Institutional Origins of Risk: A New Agenda for Risk Research. *Health, Risk & Society*, 8(3), 215-221.
26. Russia's National Security Strategy. (2009, May 12). Approved by Presidential decree no. 537.
27. Tagarev, T., & Pavlov, N. (2007). Planning Measures and Capabilities for Protection of Critical Infrastructures. *Information and Security Journal*, Vol. 22, 38-48.
28. Талијан, М. Менаџмент и безбедност: Прве установе приватне безбедности у Србији. http://www.gmbusiness.biz/index.php/arhiva/31-40/gm_32/prve_ustanove_privatne_bezbednosti_u_srbiji.html (accessed August 26, 2013)
29. Вулетић, Д. (2011). Заштита критичних информационих инфраструктура, Зборник радова са Конференције о безбедности информација, Београд: Универзитет Метрополитан.
30. Who Became Part of the Department. http://www.dhs.gov/xabout/history/editorial_0133.shtm (accessed August 6, 2013)
31. Who Became Part of the Department. http://www.dhs.gov/xabout/structure/index.shtm (accessed August 7, 2013)

UDC 726.9:75.041.5
ID 176374796

Predrag Marić
Sector for Emergency Management,
Ministry of Interior of the Republic of Serbia
predrag.maric@mup.gov.rs

Zoran Jeftić
University of Belgrade, Faculty of Security Studies
jefticz@ymail.com

Sanja Žugić
Sector for Emergency Management,
Ministry of Interior of the Republic of Serbia

EXPERIENCES IN THE OPERATION OF NEW PROTECTION AND RESCUE SYSTEM IN SERBIA

Abstract: Within this paper the experience of the functioning of the system of protection and rescue in emergency situations in the Republic of Serbia, with special emphasis on critical weaknesses after its founding in 2010, will be discussed. We will present the results of the studies that confirmed the need for necessary measures to be taken in order to improve the system as a whole and make it more efficient.

Keywords: *emergencies, protection and rescue, natural disasters, civil protection.*

1. INTRODUCTION

Since the introduction of the System for protection and rescue in emergency situations in the Republic of Serbia (December 2009 - July 2010) and in the years that preceded it, the increase of the number of natural and other disasters that threaten people's lives and their property was noticed. The increased number of fires, floods, extremely high and low temperatures, and even earthquakes, resulted in growing number of casualties and material damage from year to year.

By the adoption and coming into power of the new Law on Emergency Situations in 2010, as well as the adoption of the National strategy for protection and rescue in emergency situations in 2011, Serbia has established new organizational framework for the activities in emergency situations after many years. A unified emergency service (Sector for Emergency Management of the Ministry for Interior of the Republic of Serbia) was established, whose operational activities are based on the close conjunction with the activities of local self-governments. In this way, the country's need for protection and rescue of people was fulfilled, but at the same time the recommendations of the United Nations that the focus of protection and rescue must be on the activities of local self-governments, were implemented.

By establishing the Headquarters for emergency management on different levels (municipal, city, county, as well as to the level of province and the Republic), the Sector for Emer-

gency Management is fully empowered to serve protection and rescue of people at the level where they are mostly affected - the municipalities and cities in which they live. At the same time Mayors became the most responsible officials for organizing the protection and rescue activities of their citizens.

According to the Law on Emergency Situations, the term of "emergency situation" stands for an emergency and state of disorder caused by a large-scale event, that can paralyze the functioning of the society, due to the occurrence of a natural and technological disaster threatening the life and property of the population.[1] With the introduction of the system for protection and rescue in emergency situations, the concept of civil protection that existed in the former Yugoslavia in the twentieth century, was completely abandoned.

The Sector for Emergency Management consists of approximately 4,000 employees; of that number 3,000 are firefighters-rescuers, while the remaining number includes the employees engaged in the prevention of fire and explosions, risk management and organization of civil protection. The funding of the Sector is precisely defined through the budgetary fund for emergencies. A suitable legal framework that defines the role and the place of each protection and rescue entity and stakeholder (public administration, local self-governments, and commercial entities) and their responsibilities was created. The National Assembly of the Republic of Serbia adopted the National Strategy for Protection and Emergency Rescue in 2011. It is written in the spirit of "Hyogo Framework for Action" for disaster risk reduction of the UN. With this, the formal legal framework for the protection and rescue in emergency situations was created with fully implementing the recommendation of all the relevant factors in this field in the UN – the UN ISDR, UNDP, etc.

These activities were followed by the increased number of emergencies and natural disasters - mainly floods, earthquakes, droughts, extreme low temperatures with heavy snowfall, etc. Almost immediately after its establishment, this system had a number of big challenges (earthquake in Kraljevo 2010, floods in 2010, wild fires in 2010 and 2012). After more than two years, it is obvious that most of these challenges were successfully overcome although problems were evident on this path. These problems were caused mainly by the fact that it was necessary to adapt to the new system after a twenty-year delay since the system created in the time of Yugoslavia collapsed (Jakovljevic, 2004). It was primarily concerned not only to define responsibilities of all stakeholders in protection and rescue operations to take necessary measures for response in case of emergency, but also to apply preventive measures in order to mitigate the effect of disasters.

It is in this area of prevention that the most noticeable flaws of the system are experienced, and therefore research was conducted with the aim to highlight all necessary steps for the improvement and creation of true European system of protection and rescue in Serbia.

2. REALITY AND CURRENT SITUATION

One possible view of the current situation, which will be elaborated in this paper, refers to the insight in investing in the system for protection and rescue of people in emergency situations and its importance and potential impact on reducing the number of victims and the amount of damages. Undoubtedly, it raises some fundamental questions that are primarily related to the following: the lowest point in the prevention of emergency situa-

1 Law on Emergency Situations, Official Gazette of the Republic of Serbia, 111/2009 and 92/2011

tions; steps to be taken to strengthen all the weak points and to what extent this would affect the protection of human life and decrease of the amount of material damages caused by the disaster.

The starting point for any assessment of the state of preparedness for emergencies in Serbia is that the emphasis is still on the emergency response and compensation for the damages caused by disasters, than it is on the investment in prevention of emergencies.

The period from 2007 to 2010 was taken into account in this research, with recording the most common risks to life and health of the citizens of the Republic of Serbia and the protection of their material goods, as well as a comparative analysis of the number of victims and the amount of damage before the adoption of Law on Emergency Situation, as well as the period between 2010 to 2012. The data was collected by the Sector for Emergency Management of the Ministry of Interior of the Republic of Serbia. It is a comparative statistical research that clearly shows the weaknesses of the system; the increasing number of casualties and material damages caused by emergency situations in correlation with the funds that the State invests in the improvement of the system and capabilities.

Here are the data of the Sector for Emergency Management stating the number of interventions, the dead, the injured and the rescued, followed by the data on the amounts of investment in the equipment, vehicles, and maintenance of equipment and vehicles, and the facilities. Research shows the correlation between the number of extraordinary events and resources invested in their prevention, before and after the introduction of a new system of protection and rescue.

Data on number of interventions from 2007 to 2009

Year	Total No of events	Events									
		Fires	Explosions	Technical intervention	Traffic accidents intervention	CBRN intervention	Earthquakes	Floods	Water pumping	Fire Investigations	Rest
2007	35278	28698	31	1489	799	59	0	0	343	583	2722
2008	31584	24498	44	1525	752	82	0	3	213	611	2464
2009	28473	21656	41	1738	780	86	0	4	568	804	2473

Data on number of killed, injured and rescued from 2007 to 2009

Year	Casualties			Injured			Rescued
	Casualties	Firefighters	Citizens	Injured	Firefighters	Citizens	Rescued
2007	314	0	314	1057	55	1003	347
2008	370	0	370	1055	64	991	518
2009	380	0	380	1071	43	1038	1019

Investments in the period from 2007 to 2009 are shown in the following table:

	Budget			NIP		Budgetary Fund	
	Goods	Services	Work	Goods	Works	Goods	
2007	25.770.402,91		19.635.599,55	1.022.887.572,40			**1.068.293.574,86**
2008	45.367.818 ,22	2.361.180,00	10.989.729,40		43.737.009,37		**102.455.736,99**
2009	84.966.143,38		7.334.015,41	172.913.247,00			**265.213.405,79**
2007 - 2009	**156.104.364,51**	**2.361.180,00**	**37.959.344,36**	**1.195.800.819,40**	**43.737.009,37**	**0,00**	
????	**196.424.888,87**			**1.239.537.828,77**		**0,00**	**1.435.962.717,6 4**

Investment realization in period from 2007 to 2009, displayed in dinars with VAT

Year	Equipment	Vehicles	Equipment and Vehicles Maintenance	Facilities	Total
2007	25.770.402,91	1.059.101.772,40	0	19.635.599,55	1.104.507.774,86
2008	44.468.721,65	0	1.593.000,00	54.726.738,77	100.788.460,42
2009	84.842.666,92	172.913.247,00	3.923.233,32	7.334.015,41	269.013.162,65
2007-2009	155.081.791,48	1.232.015.019,40	5.516.233,32	81.696.353,73	1.474.309.397,93

It is evident from the above-given data that there is a substantial increase of the number of emergencies (fire, flood, etc.) and casualties in the period from 2007 to 2009.

In the period from 2007 to 2012, the investment in the Sector for Emergency Management, was as follows: total of 2,374,628,313.51 dinars through funding from the budget of the Republic of Serbia (532,527,236.65), investment through the National Investment Plan (NIP) (1,284,324,762.36), Budgetary Fund for Emergencies (557,776,314.50), and this into the goods, services and work, as can be seen from the attached tables.

Investments in the goods and assets during this period were as follows: from the National budget 343,698,635.51 dinars, through the NIP 1,195,800,819.40 dinars, and from the Budgetary fund 557,776,314.50 dinars. Investments in the work aspects during this period have been as follows: through the National Budget of the Republic of Serbia 138,405,805.95 dinars, while through the NIP 88,523,942.96 dinars was invested.

Data on the number of interventions for the period 2010 – 2012

Year	Total number of events	Events									
		Fires	Explosions	Technical intervention	Technical intervention in traffic accidents	CBRN Interventions	Earthquakes	Floods	Water pumping	Fire Investigation	Rest
2010	25335	17250	54	1883	700	89	0	1	1956	584	744
2011	38333	31889	51	1932	745	89	2	4	372	123	1072
2012	44578	35705	52	3619	641	89	0	1	403	3	1850

Number of casualties, injured and rescued for period from 2010 to 2012

Year	Casualties			Injured			Rescued
	Casualties	Firefighters	Citizens	Injured	Firefighters	Citizens	Rescued
2010	403	0	403	1049	24	1025	1388
2011	447	0	447	1368	60	1308	1181
2012	453	0	453	1205	69	1136	3451

Investments in the period from 2007 to 2009 are shown in the following table:

	Budget			NIP		Budgetary Fund	
	Goods	Services	Work	Goods	Work	Goods	
2010	101.314.559,00	12.238.051,00	62.003.361,71				**175.555.971,71**
2011	59.028.202,00	20.182.431,08	21.106.737,84				**100.317.370,92**
2012	27.251.510,00	15.641.133,11	17.336.362,04		44.786.933,59	557.776.314,50	**662.792.253,24**
2010 - 2012	**187.594.271,00**	**48.061.615,19**	**100.446.461,59**	**0,00**	**44.786.933,59**	**557.776.314,50**	
????	**336.102.347,78**			**44.786.933,59**		**557.776.314,50**	**938.665.595,87**

Investment realization in period from 2010 to 2012, displayed in dinars with VAT

Year	Equipment	Vehicles	Equipment and Vehicles Maintenance	Facilities	Total
2010	91.364.077,00	13.145.200,00	20.946.767,00	62.003.361,71	187.459.405,71
2011	81.993.395,04	0	10.888.043,08	21.106.737,84	113.988.175,96
2012	498.540.495,24	88.382.982,14	8.327.385,85	62.123.295,63	657.374.158,86
2010 -2012	671.897.967,28	101.528.182,14	40.162.195,93	145.233.395,18	958.821.740,53

From the above mentioned data it is not difficult to notice the inconsistency of the investment in the equipment of the Sector for Emergency Management. Furthermore, after every major investment a decline in investing was obvious, and thereby the slowing of the process of increasing the level of readiness and capacities for more effective response in case of emergency situations.

3. HOW TO IMPROVE THE SYSTEM

In order to improve the whole protection and rescue system in the Republic of Serbia and simultaneously identifying its main weaknesses and shortcomings, it is necessary to point out the activities that would surely lead to much more efficient emergency response, as well as taking into account the issue of preventive measures whose lack thereof formulates the weakest point in this protection and rescue system in Serbia.

3.1. 112 System

The European Emergency number 112 was introduced in the EU countries several years ago. It represents an operational-technical system that allows the EU citizens to receive timely and necessary assistance very quickly regardless of whether they are affected by natural disasters, crime or health issues. The Republic of Serbia is the only country in the region that still has not implemented this system, even though it is a "technical requirement" for every country applying for the membership to the European Union.

The implementation of this system connects the activities of all emergency services, fire-rescue units, police and the Ministry of Health. Despite the efforts over a nearly four-year period to obtain the initial funding and financial resources through the Ministry of Finance (amount of EUR 30 million), there was not sufficient political will to make an important step towards improving the safety of all citizens of the Republic of Serbia.

All major natural disasters, from earthquakes, floods, fires, chemical accidents, through extremely low temperatures followed by heavy snowfalls, to health problems and, finally, the effects of major terrorist acts, can be more effectively and efficiently addressed if a country has a functional and operational 112 System. Most importantly, it can affect the efficiency and speed of provided assistance, even in rural and remote areas. It goes without saying that in such circumstances and situations, the efficiency in providing assistance is a key factor for effective saving of people's lives and protection of property. So far, the possibility to obtain the necessary funds in the near future is frail, in spite of all the above-mentioned arguments.

3.2. Changing the education system

Since the 1980s, a very important segment in creating a culture of safety of all citizens is missing in the educational system of the Republic of Serbia – how to react in case of emergency situation in a way to successfully protect human lives. It should be noted that this

problem has led to the fact that one cannot speak of a "low awareness", but of its complete absence in terms of protection and rescue in emergency situations.

None of the media campaigns that aim to change this situation can be as effective as actual education of citizens, primarily the youngest, in this important field. This does not mean introducing the new subjects such as the previously existing school subject called "National and self defense". Instead of this, there is a need for somewhat broadening the existing school curriculum. In this manner, the children would learn that a river can pose a threat and danger in the form of flooding, and therefore, they would learn the ways how to react and protect themselves in case of floods. Of course, they would learn of the protective measures in the case of fires, earthquakes, low and high temperatures and so on.

The campaign that was jointly launched by the Sector for Emergency Management and the OSCE Mission to Serbia, through publishing the Family Guide for Emergency Preparedness and Response, can only partially moderate the consequences of these deficiencies in the education system, but it cannot in any way be a recompense for its gaps.

3.3. HR Capacity building

The number of members of the Sector for Emergency Management, particularly the members of fire-fighter and rescue units is approximately three thousand (3,000). The EU norms state that every country should have one fire-fighter on 1,000 inhabitants (according to the data of the European Commission, Directorate General for Civil Protection and Humanitarian Assistance). According to this, at this moment Serbia lacks three to 4 thousand fire-fighters. Furthermore, Serbia has the least number of professional fire-fighter-rescuers after Albania.

It is necessary to stress that the system of voluntary fire fighting units is underdeveloped, and that due to the lack of a viable legal solutions and financing, it cannot be considered an adequate support to emergency responders. Therefore, every emergency situation required the engagement of all available forces of the Sector for Emergency Management from all parts of the country. Because of this, all technical as well as human resources were exhausted to the extreme. Therefore, it was unavoidable to have the involvement of the Serbian Army, Gendarmerie of Ministry of Interior and other services, even though they were not trained and equipped for emergency response. The first step forward in this field has been made with the adoption of the National Budget for the year 2013 in which funding was planned for the employment of 500 additional fire-fighters – rescuers during this year.

It is necessary to provide necessary funding for the additional employment in order to raise the operational capacity of all units of the Sector for Emergency Management. Also, it is necessary to establish the solid method of funding voluntary fire fighting organizations and units and by doing so activate the engagement of the citizens.

3.4. Civil protection

All over the world civil protection is referred to as an organized response of a whole society in case of a dangerous threat to the population, material goods and environment. It represents the broadest form of organization, preparation and participation of population in protection and rescue in the event of natural disasters, technical-technological accidents, the consequences of war and other hazards in peace time. Civil protection is categorical

concept with clear priorities, modes of operation in the protection of the public interest - human lives, material goods and the environment.

This humanitarian activity is regulated by the international law, the Geneva Convention of 1949 and by the Additional Protocol of 1977 to the Geneva Conventions. Both documents were ratified by the Assembly of the Socialistic Federal Republic of Yugoslavia in 1950 and 1977. According to the international humanitarian law, the concept of civil protection refers to humanitarian activities in order to protect civilians from all types of risk (disasters) and secure all necessary conditions for survival.[2]

Therefore, the preparation for the successful functioning of civil protection is a task of primary importance, so that the human and material losses could be reduced to the fullest extent possible as well as to quickly and successfully overcome the consequences of natural disasters, technical, technological and other disasters as well as of the war consequences. Therefore, civil protection needs to become a subject of interest of all stakeholders in a society - from citizens to government institutions.

The system of civil protection in the Republic of Serbia collapsed with the breakup of Yugoslavia. Besides the occasional activation during the war in 1990s, with the establishing of the Sector for Emergency Management, civil protection is now in a position to be created according to the new normative, organizational, personnel and functional organization base. Furthermore, it can be organized according to different social and cultural circumstances currently present in the country. Although imperceptible, this reconstruction has already been initiated and implemented.

In the next four years, it is reasonable to expect to have 8 to 9,000 members of Civil Protection Units. These civil protection units will consist of young people, trained for protection and rescue in emergency situations, which will be activated when a disaster occurs to provide necessary assistance to professional fire and rescue units. It is necessary to bring this process successfully to the end. We can agree that it is very easy to shatter the efficient system; however, it is very difficult to rebuild it.

3.5. Continuity of funding

Since the adoption of the Law on Emergency Situations (December 2009) and to the end of 2012, the funds provided by the budgetary fund for emergency situations were less than 5.000.000 Euros annually. Although insufficient, these funds were enough to purchase the new protective and work uniforms for all fire-fighters and rescuers in Serbia after 7 years.

This amount was doubled after the adoption of the 2013 National budget. This would enable the purchase of new fire fighting vehicles, which are 25 years old on average. Fire fighting vehicles were last purchased in 2007. There is a need to invest in equipping helicopters for aerial fire fighting. It can be said that Serbia has a sufficient number of aircraft of this type, however only 3 helicopters are equipped for aerial fire fighting. With 3 agricultural aircraft of JAT this is insufficient for efficient aerial fire fighting in a case of major forest and wild fire in Serbia.

The purchase of flash flood protection systems, special vehicles for extinguishing forest fires, uniforms for the members of the Civil Protection units are some of the items in the

2 Zoran Jeftic, Civil Defence as Important Segment of Defence System Reform, in Armed Forces Reform Experiences and Challenges, CCMR Belgrade 2003.

Procurement Plan of Sector for Emergency Management for the 2013. On the other hand, it is certain that if there is no continuity in funding through the national budget in forthcoming years, it will directly affect and reduce the efficiency of the emergency response. The EU member states do not have a dilemma concerning the need to invest in this area (Council of Europe, 2011).

Climate changes have caused the increase of number of natural disasters that cause major damages and every country is trying to reduce the risks to disaster by increasing funds for these purposes. Therefore, it is necessary to establish permanent funds in the field of protection and rescue in emergency situations in Serbia. This is the only possible way to fill the gap that appeared during the last twenty years when nothing or very little was invested in this area.

CONCLUSION

Since the beginning of creation of the system for protection and rescue in emergency situations in the Republic of Serbia (December 2009 - July 2010) much has been accomplished. Although Serbia is one of the last Balkan countries that started the reform of the system for the protection of citizens in emergency situations, some of the evident mistakes were avoided; the mistakes such as premature decentralization, weak coordination within the service, undefined way of funding, bad relations between the members of the fire services and civil protection, etc. The system that existed in Serbia previously was appropriate for that period and for the circumstances in which the country was at that time. Financially, however, the situation was never good, as is not today.

The unified service for emergency management was established (the Sector for Emergency Management of the Ministry of Interior of the Republic of Serbia) by merging all human and technical resources that were divided between three ministries (Ministry of Interior, Ministry of Defence and Ministry of Environment). In Serbia from 2002 to 2008 there was no political consensus on the question how to organize this emergency management service. There were two approaches at the moment.

The first approach was to establish Emergency Management Agency that would be composed of the members of the Civil Protection of the Ministry of Defence, and they would have seniority over the fire fighting units that were part of the Ministry of Interior of the Republic of Serbia. The second approach was aiming to establish a unified emergency service within the Ministry of Interior of the Republic of Serbia following the model present in 27 countries of the European Union. According to this model all protection and rescue subjects that operated within these 3 ministries would be brought together.

In 2008 the decision was made to establish a service within the Ministry of Interior of the Republic of Serbia - merging the Department for the protection and rescue of Ministry of Interior (fire fighters), the members of the Civil Protection of the Ministry of Defence and the Department in the Ministry of Environment. The Sector for Emergency Management within the Ministry of Interior of the Republic of Serbia was created and became operational on 1 July 2010.

It is necessary to note that this was a good decision and suited to the moment in which the country was and where it still is. This primarily refers to the gross domestic product, which is inevitably reflected in the budgets of local self-governments. In other words, the politically encouraged decentralization of placing the fire fighting units under the author-

ity of local self-governments would put us in a situation that the fire-rescue units would get reduced to even lower number due to the inability of local self-governments to finance their operations. It is of no coincidence that usually the Scandinavian countries have established agencies for emergency management, knowing that local municipalities and cities there have substantial resources to fund the fire brigades, as well as to improve their capacities.

When it comes to the types of organization of the system of protection and rescue, there are different opinions which road to take in the forthcoming years - is it the establishment of a Ministry, an Agency or a Directorate for emergency management?

Although the current administrative position of the Sector for emergency management within the Ministry of Interior is well known and accepted in international practice, its expressed multi-sectored activities provides the basis for further reflection on the future organizational matters.

The idea that is imposed is that we should work on the creation of the Directorate of Emergency Management, as an independent state authority directly under the Prime Minister's Office. The arguments in this favour lay in the fact that mainly large countries (in terms of territory and population) resort to the establishment of the Ministry for this purpose. These are the countries such as Russia, Belarus, and Ukraine. On the other hand, service for emergency management needs to be separated from the politics and from appointing management by political preferences; and this would be inevitable with the establishing of the Ministry of Emergency Management.

The creation of an Emergency Management Agency is a solution that has been abandoned since 2008. The reasons for this are still present - according to the Law on State Administration, fire fighting-rescue units cannot be a part of an Agency; the local self-governments do not have sufficient financial resources to fund the operation of fire brigades; finally, the ever-present issue of coordination in these conditions would be a problem. The practice in the past two years has shown that the Sector for Emergency Management of the Ministry of Interior of the Republic of Serbia already functions, in many ways, as an autonomous state body separated from politics.

Therefore, it is necessary to establish a Directorate for Emergency Management as an independent state body. Furthermore, it is necessary to strengthen the professional status of the service and enable it to get more room that it now lacks because of the dominance of the Police within the Ministry of Interior. On the other hand, the Directorate is a form of organization which allows all subjects of protection and rescue to be under it: Fire-Rescue units, Civil Protection units, and fire and explosion prevention. In other words, a Directorate may arise through the separation of the Sector for Emergency Management from the Ministry of Interior of the Republic of Serbia. It is impossible to estimate when this would happen. In any case, it will be possible when we obtain political will for necessary changes. The financial factor in this case is not dominant because these changes require minimal financial costs. Otherwise, this is the path that will be taken in the years ahead and that will assure more efficient emergency response.

If there comes to the will and determination to take these steps for the change in the following years, it is certain that Serbia will get a modern European Emergency Management Service and have a developed system that will provide better protection of human lives and their property. The outcome will depend on the persistence of the members of the

Sector for Emergency Management and understanding and appreciation of their efforts by the highest political officials in the state. Old Japanese proverb says: "Fifty steps are the same as 100 steps." You should not start the business if you do not have the strength to do it right or end it successfully. It remains to be seen whether this endeavour will be successfully completed.

REFERENCES

1. Јаковљевић, В. (2004). *Систем цивилне одбране*, Факултет безбедности, Београд
2. Марић П., Томић Д. (2010). *Управљање ванредним ситуацијама*, Балкански институт за управљање и процену ризика
3. Zoran Jeftic, Civil Defence as Important segment of Defence System Reform, Armed Forces Reform Experiences and Challenges, CCMR Belgrade 2003
4. Taylor P. (1993). *International Organization in the Modern World,* The Regional and the Global Process. London
5. United Nations (1995). *The United Nations in Second Half-Century. A Report of the Independent Working Group on the Future of the UN*, Yale, CT
6. Council of Europe (2011) 12th Ministerial Session on European and Mediterranean Major Hazards Agreement (EUR-OPA), Saint Petersburg 28.09.2010.
7. OECD (2010) *International CEP Handbook 2009*, Swedish Civil Contingencies Agency (MSB) 2009.
8. Review of the Italian National Civil Protection System, Reviews of the Risk Management Policies, Italy, 2010, OECD
9. Emercom of Russia (2009) *Modern Aspects of Humanitarian Operations in Emergency Situations and Military Conflicts*, Moscow.
10. Российская академия наук, МЧС (2003). *Стратегические риски чрезвычайных ситуаций: оценка и прогноз, Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийныбедствий, России*, Москва.

UDC 726.9:75.041.5
ID 176374796

Branko Mihaljević, Ivan Toth, Alen Stranjik
University of Applied Sciences, Velika Gorica
branko.mihaljevic@vvg.hr
ivan.toth@vvg.hr
alen.stranjik@vvg.hr

IMPACT OF CRITICAL INFRASTRUCTURE OWNERSHIP ON THE NATIONAL SECURITY OF THE REPUBLIC OF CROATIA

Abstract: Based on the property law, the owner has the right and the power to exercise and protect his interests over the property at his disposal. It is likewise one of the fundamental principles of lawful action and procedures of the legal state. The above premise is also important for the national security and critical infrastructure which are increasingly interrelated. Critical infrastructure is a relatively new concept in Croatia and conceptual levels are in the process of official definition. Public debate and the adoption of the Critical Infrastructure Act are under way, which shall systematically define the issues stated above in the context of national security. Legal rulings and definitions to date have in general partially considered these issues and have been insufficient considering the importance of critical infrastructure and its impact on the national security. In this paper the authors will analyze critical infrastructure in the context of national security and the importance of ownership and their role in the context of national security, and above all the connections between these three concepts, that is, these three categories. Hereafter, the authors will examine different theories of privatization and then present critical infrastructure concepts in selected countries, as well as the examples of privatization of selected elements of critical infrastructure in Croatia with regard to the ownership structure in various sectors. Depending on the properties of individual sub-sectors, the consequences of privatization and its impact on the national security of the Republic of Croatia also vary.

Keywords: *critical infrastructure, national security, ownership, Republic of Croatia*

1. INTRODUCTION

The right of ownership is an actual right over a specific thing that authorizes its holder to do as he pleases with that thing and benefits from it, as well as excluding everyone else from this if it is not contrary to other people's rights or legal restrictions. The owner has the right to own, use, utilize and dispose of his property. The owner must not exercise his right of ownership over the limitations imposed on all owners of such things according to the law in order to protect the interests and security of the state, nature, environment and human health. Ownership binds and the ownership holders and their beneficiaries are required to contribute to the common good. Ownership provides exclusive right and control over the property being disposed of.[1]

State ownership implies the right of management over the organization, leadership, management and use of public property in the interest of citizens, and all this gives a certain

1 Zakon o vlasništvu i drugim stvarnim pravima, Narodne novine, 92/13.

power to the state. Of all economic and security entities for the national security of a country, critical infrastructure (CI) is especially important, since normal functioning of the society increasingly depends on it, especially in this age of rapid changes, unforeseen events, crises and other security challenges. At the same time, we must not overlook the threats to national security in other ways, which are now in a time of global economic crisis reflected primarily in the economic area, where ownership plays a great role.

The motive to cover this topic arises from the attempt to understand which role is played by CI within the framework of national security and how the ownership over CI affects national security of the Republic of Croatia.

The aim of this paper is to define the basic concepts of CI, national security and ownership, present and analyze the impact of CI ownership on national security, describe CI in selected countries and describe the CI ownership structure in the Republic of Croatia. Based on theoretical postulates and examples of privatization, we will try to determine whether CI ownership affects the national security of the Republic of Croatia.

The problem in the treatment of the aforementioned topic is the lack of current knowledge on CI in the Republic of Croatia. Based on the identified problems and the aim of the research, the following research hypotheses are set:

H1: Ownership over CI affects national security. Ownership provides management rights and thus indirectly decides in the field of national security.

H2: In the Republic of Croatia, the majority of CI in the public sector is in the ownership of the Republic of Croatia, but the Republic of Croatia has partially enabled the transfer of the CI ownership in the private hands, so the assurance of national security in this area has become questionable.

Many Western countries have the majority share of CI in private ownership, and the state – in order to ensure undisturbed operation and functioning of CI - invests great effort in the cooperation of state structures and private entities. In the Republic of Croatia, CI has just been defined at the conceptual level, and this is the reason why lines of responsibility between various actors – private and public – in the field of CI have still not been defined.

In the writing of this paper the authors have used the following methods: (a) method of analysis and interpretation of the contents of primary, secondary and real sources on the Internet, books, scientific articles and journals; (b) descriptive method has been used in the definition of basic concepts, analysis of CI and examples of privatization; (c) case studies have been used in the analysis of privatization cases, and (d) comparative method has been used in the examination of the impact of CI ownership on the national security.

2. THEORETICAL DETERMINATION OF BASIC CONCEPTS

2.1. National security

The essential requirement and the aim of every national policy is the survival of the state and society, and the requirement of the survival of the state and society is its security. Therefore, this is inter alia the purpose of all activities of state institutions. This likewise represents the framework of security policy which has the task of creating the organization which achieves internal and external security of the state and society, that is, national security.

National security it first appeared in the United States and is in use from the beginning of the 1940s. It was then that the concept of national security took a central place in the international relations and security studies.[2]

The concept of national security in its initial phase had no clear content. In the early years of the Cold War, politicians often used it as a slogan to support their policies. But over time the content of the concept of national security became clearer. It implied the totality of political, military and economic efforts which the governments needed to take to achieve their internal and external security. National security usually implied the absence of any kind of fear of attacks, compromising the interests or threats from another state or country.

The concept of national security as the concept which is a framework for the security of state and society in current research is not unambiguously and completely defined.[3] Some theorists define national security as the absence of any kind of fear of attacks, compromising the interests or threats from another state or country. International Encyclopaedia of Social Sciences defines national security as the ability of state/nation to protect its internal values from external dangers.[4] Certain authors interpret national security as a function of the nation-state with which they protect their own identity, survival and interests, in accordance with their capabilities now and in the future, while respecting global changes and development in the world.[5] Some authors understand national security as the security of the political nation, which includes: security of national territory, protection of human life and property, protection and preservation of national sovereignty and the operation of fundamental social activities – economic, political, social, cultural and ecological.[6] Regardless of the differing definitions of national security, the majority of theorists agree regarding the values included in the category of national security and the goal of the strategy of national security, understood as the art of effective application of national resources in order to achieve national interests.[7]

2.2. Critical infrastructure

Critical infrastructure has become an important segment of the national security of individual countries in the early 1990s. At the same time, the systems of protecting critical infrastructure started to develop and it today represents one of the protection priorities of almost any state.

Critical infrastructure represents physical or virtual systems and resources that are vital for the normal functioning of a state.[8]

European critical infrastructure denotes critical infrastructure of interest for at least two member states or one member state, while being located on the territory of another member state.[9] National critical infrastructures are systems, networks and facilities of national

2 Lippman, W., US Foreign Policy, Hamish Hamilton, London, 1943., p.32.

3 Tatalović, S., i Bilandžić, M., Osnove nacionalne sigurnosti, MUP, Zagreb, 2005., str. 30.

4 International Encyclopedia of the Social Sciences, sv. XI, The Macmillan Company, London, 1968., str.40.

5 Huwaydi, A., Militarization and Security in the Middle East, Printer Publishers, London, 1989., str.16.

6 Grizold, A., Međunarodna sigurnost – Teorijsko – institucionalni okvir, FPZ, Zagreb, 1997., str. 29-30.

7 Encyclopedia Britanica, sv. 21., 1985., str.454.

8 Grupa autora, Pojmovnik sigurnosne kulture, Centar za CVO, Beograd, 2009., str.61.

9 Zakon o kritičnim infrastrukturama Republike Hrvatske, Zagreb, Narodne novine, broj 56/13.,članak 2.

importance whose cessation of operation or the interruption in the delivery of goods or services can have serious consequences for the national security, health and lives of people, property and environment, security and economic stability and the uninterrupted functioning of government.[10]

During 2004, a group of scientists has developed a comparative analysis of critical infrastructure in sixteen countries of the world which looks like this:[11]

a. banking and finance, communications, information and telecommunications systems and energy – important in 14 countries;
b. transport, logistics and distribution – important in 13 countries;
c. healthcare services, water and supply – important in 12 countries;
d. central government/government services – important in 11 countries;
e. emergency rescue services – important in 10 countries;
f. supply of petroleum products and gas – important in 9 countries;
g. information services, media, public administration – important in 8 countries;
h. other areas – strengthening of legislation, judiciary, public order and national security, waste management, police, radiological, chemical and biological protection, army and military facilities, security system, social services, water resource management, nuclear power plants – important in 1 to 6 countries.

Through the analysis of the above-mentioned eight groups of priorities within the context of critical infrastructure, we can conclude that determination and definition of critical infrastructure, as well as its content cannot be identical in every state and every part of the world. Therefore, it is natural and logical that the definition and content of critical infrastructure have to be determined and defined individually on the national level, or the level of every state.

2.3. Ownership

Regarding the ownership, it is necessary to define the difference between the economic and legal concept of ownership. Ownership in the economic sense denotes a social relationship expressed in the fact that a certain item belongs to a specific subject. In the legal sense, ownership over an item gives the owner the right over it, as well as the right to appropriate its usability properties. What constitutes a basic difference between the economic and legal concept is the fact that economic ownership gives the holder of the item all properties of the item, as well as the economic result of the realization of those properties. In other words, economic ownership can survive even without appropriate legal regulations.[12]

There are numerous categories of the division of ownership, but for our purposes in this paper we retain the classic division of ownership to private and state ownership. But apart from this, the need for substantial investment in public infrastructure in order to increase efficiency of public sector is ever more obvious in the EU states, as well as in the Republic

10 Isto, članak 3.

11 Čemerin, D., Kritična infrastruktura – objekt i sredstvo, u Zbornik radova - Kako se štitimo od katastrofa, DUZS; HCK i VVG, Zagreb, 2007., str.81.

12 Vedriš, M., Klarić,P., Građansko pravo, Narodne novina, Zagreb, 1996., str.182.

of Croatia. Lately, public-private partnership is frequently mentioned as the new model of the procurement of public infrastructure, although public-private partnership dates back to the 18th century as a concept for the privatization of public infrastructure. Public-private partnership actually represents project relationship of a long-term nature which includes various forms of cooperation between public and private partners and is significant for our issues.

3. IMPACT OF CRITICAL INFRASTRUCTURE OWNERSHIP ON THE NATIONAL SECURITY

Ownership gives its holders an exclusive right to dispose of and control a specific property. State ownership represents the right of the state over the regulation, management, leading and use of public property in the interest of all citizens, while private ownership belongs autonomously to its owners and serves their interests.

National security is a public good consumed by all citizens. Once secured, it is extremely difficult to exclude individuals from the enjoyment of national security, since they participated in its creation. Today, contemporary threats and hazards are aimed not only at the nation-state, they also appear inter alia in the form of information warfare, cyber crime, economic espionage and similar. Actors of threats are numerous and can be terrorist groups, hackers, international criminal organizations, companies and corporations.

Due to an ever greater intertwining of private and public sector, the question what should be protected increasingly arises. In the past national security entailed primarily the protection of national state and its institutions, but now it is important to include in the protection those private actors whose activities are important for national economy and national security. The ability of private sector to ensure optimal protection of critical infrastructure is questionable, primarily because of the high costs associated with protection. Since the market is not able to take care of the specific protection of critical infrastructure, the state has to intervene in those areas where it is necessary.

Ownership of critical infrastructure is related to national security, both in the economic-financial sense and in the sense of protecting critical infrastructure from various threats, depending on the individual economic sectors or subsectors. Protection of critical infrastructure is necessary for the maintaining of national security and the boundaries between individual forms of threats are small due to the relationship and intertwinement of individual sectors. Banking sector, for example, is more exposed to economic threats, in the sense of financial collapse, and not physical threats, while the sector of drinking water supply is more exposed to the threats of physical destruction of infrastructure or water pollution. Critical infrastructure itself can be used as a weapon for criminal activities. Cyber crime, terrorism, industrial espionage and other threats can use critical information infrastructure to achieve some of their goals.

Critical infrastructure is practically a part of all those structures, so individual sectors or individual elements of critical infrastructure are actually a means of others' power.

Protection of critical infrastructure is in itself a very complex and demanding activity. Considering the abundance of critical infrastructure, significant challenges or difficulties in the realization of protection of critical infrastructure appear, some of them being:[13]

13 Prezelj, I., *Konceptualna opredelitev kritične infrastrukture,* FDV, Ljubljana, 2008. str. 13.

- Complexity of critical infrastructure sectors, so it is almost impossible to protect the entire critical infrastructure and related components, for example, in the transportation sector it is almost impossible to protect numerous kilometres-long communication lines, a large number of airports, sea ports, numerous bridges and similar structures.
- Lack of supervision and responsibility in the sector where several public and private institutions are engaged.
- Insufficient exchange of information between institutions engaged, which leads to new vulnerability and impacts the efficiency of responses in the protection of critical infrastructure.
- Complexity of knowledge considering the large quantity of special skills which have to be known before policies and strategies in the field of protection of critical infrastructure.
- Interdependence of individual sectors of critical infrastructure and between sectors. This problem additionally influences the complexity of protection of critical infrastructure.
- Imperfection of tools for the analysis of critical infrastructure and its vulnerability. Science usually centres on the general approaches, tools and solutions.
- Asymmetric conflicts are an especially efficient form of critical infrastructure vulnerability.

States are responsible for the protection of the public and the provision of a certain level of social functionality and security, but the fact is that a part of social infrastructure is state-owned, while a part is in private ownership – domestic or foreign, and that there are critical infrastructure owners who do not possess the same values and views of the securing of the critical infrastructure system. The essence of the problem between public and private responsibility for the protection of critical infrastructure is the relationship between the perception of vulnerability and efficiency, since the main aim of private capital is efficiency, conditioned by market activity, and vulnerability is considered only if the actual situation compels them to do it. Likewise, the problem exists in the cooperation of private and public institutions due to the different goals arising from different motives. Quite often, the governments want to improve security when it is required by the private companies in the fields of telecommunications, energy and banking. However, private companies almost always offer resistance when costs for security need to be increased, since they consider those costs unnecessary. In addition, in numerous private companies preparedness for disruptions is low since the administrations do not realize the importance of preparations for critical situations as something especially important. All this is expressed in different ways – the lack of protection plans, assessments, scenarios, exercises, the lack of information exchange with other sectors and similar.

4. CRITICAL INFRASTRUCTURE AND ITS OWNERSHIP: EXAMPLES OF THE EU, USA, GERMANY AND GREAT BRITAIN

Critical infrastructure is defined differently in various states, so in this part of the paper we will briefly present the definitions of critical infrastructure in selected countries and show the examples of privatization of critical infrastructure, in order to more easily understand the above-mentioned concept on the example of the Republic of Croatia. In the brief analysis, we have selected the following states: the USA, Germany, Great Britain and the EU.

The United States have first begun with the identification, determination and protection of critical infrastructure and are still a leader in this field. Germany and Great Britain are powerful European states; both countries have developed efficient systems for the protection of critical infrastructure. The European Union is interesting since the Republic of Croatia became a member of this community, and all decisions related to the protection of critical infrastructure in the EU likewise concern Croatia.

4.1. Critical infrastructure in the EU

In summer of 2004, at the request of the European Council, the European Commission prepared a comprehensive strategy of critical infrastructure protection and formed a definition. The European Union defines critical infrastructure as material and information resources, devices, networks, services and property which, in the event of disruption or destruction, have a significant negative impact on the health, security, protection and economic welfare of the citizens, as well as efficient functioning of the governments of the EU member states. The European Council has slightly reshaped the above-mentioned definition in 2008, and it reads as follows: European critical infrastructure includes property, systems and their components located in the EU member states, and are essential for the maintenance of vital social functions, healthcare, safety, protection, economic and social security – for example, the production, transport and distribution of electricity, gas and oil, telecommunications, agriculture, finances and security services, whose destruction or damage has serious consequences for at least two members of the EU.[14]

4.2. Critical infrastructure in the USA

The United States have defined critical infrastructure in 1996 as infrastructure of vital interest for the USA, whose destruction or damage would have a negative impact on the defence and national security. The last definition accepted determines critical infrastructure as the resources, systems and networks, physical and virtual, which are of such importance for the US that their destruction or damage would have significant and great negative impact on the security, national economy, public health or the protection or combination of all of the above. In addition, the definition of key resources in critical infrastructure has been introduced into the entire matter. Those are the resources in public and private management important for the minimal functioning of the economy and the government. Supervision over the majority of critical infrastructure is carried out by the Department of Homeland Security. At the moment, key resources of critical infrastructure are divided into 18 sectors, and about 85% of critical infrastructure is privately owned.

Ever since the Industrial Revolution in the 19th century, the United States rely on foreign investment, although several cases have been recorded when the Congress banned the sale of certain institutions to foreigners due to the endangerment of national security, for example, the sale of some radio stations in 1927 and the sale of a well-known energy company to a Chinese owner in 2005.[15] Some other examples of the privatization of significant facilities show the views of the USA on the critical infrastructure ownership.

---

14 Zakon o kritičnim infrastrukturama, Narodne novine, 56/13., Zagreb,2013.

15 Kaplan, E., Lee, H.T., Foreigen owership of U.S. Infrastructure,2007.

4.3. Critical infrastructure in Germany

In Germany, the definition of critical infrastructure reads as follows: critical infrastructure are organizations and institutions of special significance for the society, whose deterioration or weakening leads to continuous lack of resources, significant disruption of public order or other dramatic consequences. In Germany, critical infrastructure has been divided into 8 main sectors.[16] According to the data of the Federal Office for Information Technology, the share of privately owned critical infrastructure ranges from 80% to 85%, with variations in certain sectors. In the past decade, a multitude of initiatives and projects contributing directly or indirectly to better understanding and improvement of the critical infrastructure protection emerged in Germany. The central institution responsible for the security and protection of critical infrastructure is the Ministry of the Interior. Privatization in Germany did not lead to major social problems. Relevant examples are the reshaping of German national railways, the post, telecom and postal bank.

4.4. Critical infrastructure in Great Britain

Critical national infrastructure in Great Britain is represented by the resources, physical and electronic, important for the integrity and continuous access to the services relied upon by the UK, whose loss or damage can lead to serious economic and social consequences or the loss of human life. In Great Britain, critical infrastructure is divided into 10 sectors. In 1989, the water supply companies have been privatized in Great Britain whose privatization is controversial to this day. The privatization of railways likewise presents many dilemmas. Privatization in other sectors did not lead to significant social problems, and the security has not been disturbed after privatization.[17]

As we can see, the definitions of critical infrastructure in selected countries differ, but they all have something in common, that is, the damage or destruction of critical infrastructure leads to various crisis situations. The United States have the widest classification of critical infrastructure since they include even shopping malls. In all countries selected, critical infrastructure is for the most part privately owned, about 80%. Considering this fact, in all countries selected there is a central national body responsible for the coordination when it comes to the protection of critical infrastructure, and for the cooperation between state and private sector. Privatization in selected countries led to significant changes, both good and bad, but is has also shown there was no place for excessive fear and panic regarding the change of the critical infrastructure ownership and the impact on the national security.

5. CRITICAL INFRASTRUCTURE AND ITS OWNERSHIP IN THE REPUBLIC OF CROATIA

The Law on critical infrastructure has been adopted in mid 2013 in Croatia. The Law regulates national and European critical infrastructure, sectors of national critical infrastructure, critical infrastructure management, risk analysis development, the security plan of the owner, or the manager, the security coordinator for critical infrastructure, handling sensitive and classified data, as well as the supervision over the implementation of the Law. Through the Law on critical infrastructure, the EU acquis communautaire contained

16 Definition Kritische Infrastrukturen. http://www.bsi.bund.de/fochthem/kritis/definition.htm (07.08.2013).

17 Water privatizion in Englad. http://en.wikipedia.org/wili/Water_privatizion_in_England (07.08.2013).

in the Council Directive 20087114/ec from the December 8, 2008 is taken over into the legislation of the Republic of Croatia, concerning the identification and determination of European critical infrastructure and the assessment of the need for the improvement of its protection.

National critical infrastructure are the systems, networks and facilities of national importance whose cessation of operation or the interruption in the delivery of goods or services can have serious consequences for the national security, health and lives of people, property and environment, security and economic stability and the uninterrupted functioning of government.

Critical national infrastructure has been divided into ten sectors, these being: (1) energy, (2) communication and information technology, (3) transportation, (4) healthcare, (5) water management, (6) food, (7) finances, (8) production, storage and transportation of hazardous substances, (9) public services and (10) national monuments and values. Beside the afore-mentioned sectors, the Government of the Republic of Croatia may by its decision designate critical infrastructure from other sectors.[18]

The owners or managers of critical infrastructures identified are directly responsible for the management and protection of critical infrastructure in all conditions. The criteria for the determination of individual network, system and facility as a national critical infrastructure are classified data and are classified with the appropriate level of confidentiality in accordance with the special provisions on confidentiality.

Critical infrastructure owners are required to prepare a Security plan of the owner/manager which includes the measures for the protection and the securing of the continuity of operations of critical infrastructure and the delivery of goods or services. The deadline for the preparation of security plans is six months from the receipt of the act of the responsible central body within whose jurisdiction the critical infrastructure belongs. Security plan is valid when the owner or the manager obtains prior approval of the central state administration body. Security plan of the critical infrastructure owners is a part of the business plan of a legal entity and is not publicly available. Plans are reviewed within one year of the designation of critical infrastructure, and regularly once a year.

Central state administration bodies nominate a security coordinator[19] for critical infrastructure and his deputy for every sector of critical infrastructure within his jurisdiction. The owners or managers of critical infrastructure are required to do the same. In the implementation of critical infrastructure protection, security coordinator for critical infrastructure is responsible for the communication in security issues between the owner or manager and the responsible central state administration body within whose jurisdiction the critical infrastructure belongs, in order to ensure protection and continuity of operations of critical infrastructure.

European critical infrastructures in the territory of the Republic of Croatia are protected in the same way as national critical infrastructures, unless the EU regulations regulate that issue differently. The Government of the Republic of Croatia submits every two years a summary of general information on the types of danger, threats and weaknesses determined in every sector in which European critical infrastructure has been determined in

18 Zakon o kritičnim infrastrukturama, Narodne novine, 56/13, članak 4.

19 Ibid, article 14.

the Republic of Croatia to the European Commission. The reports are classified data and are labelled with the appropriate level of confidentiality.

The inspection of the implementation of the Law on critical infrastructure with the owners or managers of critical infrastructures is conducted by the central state administration bodies within whose jurisdiction individual critical infrastructures belong, as well as competent regulatory agencies.

The national security of the Republic of Croatia may be defined as the state of protection of basic social values and institutions based upon them.[20] The security concept is based upon the strategic assumption that national security is the field of activity which ensures the survival and requirements for survival and development of society in relation to other international factors.

In the Strategy of national security, one of its points is dedicated to the privatization and it emphasizes that it is of strategic importance to take into account the areas of the economy important for national security of the Republic of Croatia when privatizing the economy.

By the declaration of independence, the Republic of Croatia entered the process of transition, and thus the process of the transformation of ownership. Privatization in Croatia was carried out in four phases – the first one, from 1991 to 1994, has initiated the key problem of the relationship between banking and the economy. Second phase, from 1994 to 1998, prevented the recovery and the rise of the economy and the third phase, from 1998 to 2000, was characterized by PIFs and the privatization of banks. The fourth phase in 2000 was dominated by bankruptcies, with a tendency to sell of the remaining portfolio and potential revision of privatization.[21]

Critical infrastructures are mostly state-owned, namely: production and transmission of electricity, roads, railways, air, sea and river ports, post, water, medical institutions and stock reserves. Beside the public television service, several private televisions operate, while the sector of banking and telecommunications is mostly in private, foreign ownership. The sector of fuel supply is likewise privatized, as well as gas supply. In some other sectors privatization has been announced, for example, railways and airports.

6. CONCLUSION

The main issue of this paper is whether the ownership of critical infrastructure impacts the national security of the Republic of Croatia? In the available literature this problem has not been particularly elaborated, except for individual cases. The majority of topics relate to the protection of critical infrastructure and ownership is mentioned only within the context of cooperation of state institutions and private owners. From the above, it can be concluded that the question of who is the owner of critical infrastructure is not being asked right now, but it is important that the owner ensures uninterrupted functioning of critical infrastructure. The overview of various cases of privatization has shown that in some cases there is a connection between the critical infrastructure ownership and management. Privatization has led to various results depending on the sector, country and the manner of ownership change. Some privatizations are always controversial, but the fact remains that not only state can be responsible for national security. Therefore, private own-

20 Strategija nacionalne sigurnosti Republike Hrvatske, Narodne novine, 51/02.

21 Barbarić, K., Privatizacija u Republici Hrvatskoj, Inženjerski biro, Zagreb, 1996.

ers must show more responsibility in critical infrastructure management. The hypothesis that possession, that is, ownership over critical infrastructure can impact national security can be partially confirmed.

In the Republic of Croatia, critical infrastructure is mainly state-owned, except for certain sectors where critical infrastructure has been privatized. However, privatization is about to follow in other sectors. Since the privatization of critical infrastructure has not been implemented to a greater extent, and where privatization has been implemented, the state has retained certain shares in its ownership, so the privatization of critical infrastructure could not significantly impact the state of national security.

The hypothesis that the privatization of critical infrastructure in certain sectors in Croatia influenced national security could be neither confirmed nor dismissed.

The countries where critical infrastructure is privately owned must have a quality normative regulation of this field and the control over the management and protection measures concerning critical infrastructure in order to maintain their power. It is important that the decision-making power does not remain in the hands of the state apparatus.

REFERENCES

1. Barbarić, K., Privatizacija u Republici Hrvatskoj, Inženjerski biro, Zagreb, 1996.
2. Čemerin, D., Kritična infrastruktura – objekt i sredstvo, u Zbornik radova - Kako se štitimo od katastrofa, DUZS; HCK i VVG, Zagreb, 2007.
3. Encyclopedia Britanica, sv. 21., 1985.
4. Grizold, A., Međunarodna sigurnost – Teorijsko – institucionalni okvir, FPZ, Zagreb, 1997.
5. Grupa autora, Pojmovnik sigurnosne kulture, Centar za CVO, Beograd, 2009.
6. Huwaydi, A., Militarization and Security int he Middle East, Printer Publishers, London, 1989.
7. International Encyclopedia oft he Social Sciences, sv. XI, The Macmillan Company, London, 1968.
8. Kaplan, E., Lee, H.T., Foreigen owership of U.S. Infrastructure.
9. Lippman, W., US Fopreigen Policy, Hamish Hamilton, London, 1943.
10. Prezelj, I., *Konceptualna opredelitev kritične infrastrukture,*FDV, Ljubljana, 2008.
11. Strategija nacionalne sigurnosti Republike Hrvatske, Narodne novine, 51/02.
12. Tatalović, S., i Bilandžić, M., Osnove nacionalne sigurnosti, MUP, Zagreb, 2005.
13. The Department of Homeland Security, June 2002., White House.
14. Vedriš, M., Klarić,P., Građansko pravo, Narodne novina, Zagreb, 1996.
15. Zakon o kritičnim infrastrukturama, Narodne novine, 56/13., Zagreb,2013.
16. Zakon o vlasništvu i drugim stvarnim pravima, Narodne novine, 92/13.,Zagreb, 2013.

UDC 726.9:75.041.5
ID 176374796

Dragiša Jurišić
Armed Forces of Bosnia and Herzegovina
jurisicvrs@yahoo.com

CRITICAL INFRASTRUCTURE PROTECTION IN BOSNIA AND HERZEGOVINA AND ROLE OF THE MILITARY

Abstract: Taking into consideration the fact that Bosnia and Herzegovina (BiH) has a problem with terrorism, as do many states in the world, and that the search and rescue system is still in the development phase, the question of critical infrastructure and its protection must be seriously discussed. The protection of everything all the time cannot be achieved, meaning that priorities must be decided and subsequently focused upon. This paper issues a number of concerns that are manifested in critical infrastructure management in general and in BiH in particular. Of particular importance to this paper are the problems of legal definition of critical infrastructure and the absence of the critical infrastructure list in BiH, which will all be examined. BiH does not have 'Critical Infrastructure Law' or the list of critical infrastructure, which is a key problem when it comes to critical infrastructure protection, a part of modern national security and an unavoidable element of contemporary national protection and rescue system. There are many different Laws on the Entity and State level which contains the term 'critical infrastructure', but there is no one which implicitly lists or specifically defines critical infrastructure. Underlined in this paper will be the problem in relation to a deficiency of 'Critical Infrastructure Law' in BiH and the absence of the list of critical infrastructure, in order to remind authority in BiH at all levels of the importance of this issue. On the other hand, there is also problem of protection for critical infrastructure on all levels, starting at the municipality level, through Entity level and ultimately at the state level. On the Entity level, security forces and private agencies are the base for protection, but when it comes to the protection of critical infrastructure on the state level, there are a few agencies, such as the Border police and State Investigation and Protection Agency, which are tasked with protecting the critical infrastructure of BiH. However, in the event that disasters or civil emergencies occur and endanger critical infrastructure, only the Armed Forces of BiH have the duty, from the state level, to assist civilians. They are trained and equipped for this kind of task, but should be the last resort for the state and should be seen as a temporary measure. Herein will be noted in which conditions the Armed Forces of BiH could be used in order to protect civil authorities in conditions when critical infrastructure is endangered.

Keywords: *Critical Infrastructure, protection, Armed Forces, Bosnia and Herzegovina*

1. INTRODUCTION

There are many papers which discuss critical infrastructure (CI) topic. In the last ten years, it became very important part of human security. People became aware that they could not protect everything and always, and they must decide, which of infrastructures is crucial for them and why. Critical infrastructure protection (CIP) is at the crossroads between politics, business, technology and risks. Everybody is aware of importance of

CI, but still there is no unique list or definition of CI and it leads to different approaches when it comes to CIP.

Bosnia and Herzegovina (BiH) also has a similar problem. The organization of state and civil protection makes it even more complex. The most important thing would be defining state CI and making the list of CI. On the entity level, each entity and Brčko District are responsible for their list of CI, but the definition should be common. Also, there is need for a clear understanding, whoever will protect which CI. There are some solutions on the state level, and it was defined by some laws, but nothing was done by entities and Brčko District. Also, on the state level there is no definition of CI or its list and there is no strategy for CIP. It is just the protection of VIP (list is in the law) and the protection of some objects that should be listed by the Council of Ministries and infrastructure which is protected by international laws (embassies, international agencies, etc.). Some agencies on the state level have a task to protect those VIPs and the objects, but they are not listed or defined as CI.

One of the organizations on the state level which has an important role in both external and internal security of state is the Armed Forces of BiH (AFBiH). AFBiH has some tasks defined by the Law of Defence. Two of the five mentioned tasks are in the field of non-traditional tasks but according to some other documents the AFBiH could be engaged in some activities connected with CIP, but there is not a task which explicitly mentions CIP.

2. CRITICAL INFRASTRUCTURE AND ITS PROTECTION

In the last ten to twenty years, the question of CI was highlighted. Modern stile of living and dependence of people and economy from electricity, fuel, internet (communication in general) is increasing every. Security of CI is the key question of modern national security,[1] because CI is the base for community live,[2] and asymmetric threats became a common thing. The terrorist attacks in the USA of 11 September 2001 gave a new meaning and a new dimension to the concept of CIP. The terrorist attacks in Madrid, London, Moscow, Mumbai and Islamabad have just confirmed the need for a new approach in CIP. Additionally, the hurricane Katrina in the United States, the tsunami in South-East Asia and the tsunami in Japan have also demonstrated that natural disasters could have devastating consequences on infrastructure.[3] Even political decisions can have similar effects.[4] Because of that, CIP has become one of the key priorities of European Union (EU) security area. Also, in 2007 National Strategy for Homeland Security of USA crisis management in natural disasters is put on the top of the list in front of terrorist attacks.[5] The same situation is all over the world.

---

1 Herga M. (2010). Nacionalna kritična infrastruktura, Menadžment i sigurnost – M&S 2010: "Planiranje i sigurnost", str. 311

2 Čemerin D. (2011). Upravljanje kritičnim infrastrukturama. Zbornik radova, IV međunarodna konferencija, „Dani kriznog upravljanja", Veleučilište Velika Gorica, str. 442

3 Jopling L., The protection of critical infrastructure, http://www.nato-pa.int/ default. asp? SHORTCUT=1165, assessed July 31, 2013.

4 Disruptions of gas supply from Russia to East-Europe during the winter of 2008-2009; Smedts B. (2010), Critical Infrastructure Protection Policy in the EU: state of the art and evaluation in the (near) future, Royal High Institute for Defense, Center for Security and Defense Studies, Focus paper 15, p.11

5 Zuter B. (2011). Strateški krizni menadžment Švajcarske - poređenje švajcarskog modela sa devet stranih referentnih država. Vojno delo, jesen/2011, Beograd, p.37

Depending on criteria and in order to define CI, there is a possibility for a closer view on different types of CI. In general, CI could be of the interest for: state, region or world, and it means that we can talk about national, regional (European, African, Euro-Asian) and world CI. On other hand, in some states it is possible to talk about CI on local, regional (the economical or cultural region in the state), state (national) and international level. In BiH it is possible to talk about CI on an entity level, too, and from the moment when Croatia became a member of the EU, it is possible to talk about European's CI (ECI) in BiH.[6] There is also a possibility to talk about national, bilateral or multilaterals CI.

Moreover, depending on the duration of importance of CI and the need for protection, CI could be permanent, temporary or potential. A permanent CI is key infrastructure for some state, prescribed by Law, and the one which must be in focus all the time. In a category of temporary CI, it is possible to include some political or sport events (participants, facilities, etc.) that are short, but which are very important for the state or internationally. For these infrastructures it is known that they would be important in some time of a year or during some events. Potential CI is infrastructure which is not in focus but in some situations could be very important. For that infrastructure it is known that it can become CI in some occasions, but these situations are not planed in advance.

According to some authors, CI in relation to ownership, on a national level, can be in possession of: the state, municipality, private persons, property management person in state ownership, owned by legal persons who are the founders of the local government.[7] On other hand, it means that CI can be in public, private or public-private hands. Public-private partnership is essential since it is estimated that over 85% of what can be classified as CI in the United States is owned by the private sector,[8] also in Germany it is estimated that over 90% of CI in the hands of private sector.[9]

So, it means that the types of CI are very different and depend on different views of those who decide what CI is, and of structural level of government, but in the area of CIP there is a need for a comprehensive approach. It means that all levels of the authority in the state need to recognize their CI and undertake the measures to protect them. If just one of the levels fails to recognize and protect its CI, it would lead to a disaster, because the various CI are connected mutually and dependent on each other.[10]

All kinds of CI must be considered when CIP is planned. Large number of CI types means that all levels of government in the state or in some organizations and even on the world level, should take their part of the job on CIP. That is the way how to use the resources

6 ECI means CI located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure", Official Journal of the European Union L 345, 23.12.2008, http://eurlex.europa.eu/LexUriServ/ LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF, Assessed July 09, 2013

7 Herga M. (2010). Nacionalna kritična infrastruktura, Menadžment i sigurnost – M&S 2010: "Planiranje i sigurnost", str. 314

8 Jopling L., The protection of critical infrastructure, http://www.nato-pa.int/ default. asp? SHORTCUT=1165, assessed July 31, 2013.

9 Jopling L., The protection of critical infrastructure, http://www.nato-pa.int/ default. asp? SHORTCUT=1165, assessed July 31, 2013.

10 Čemerin D. i D. Trut (2010). Kriterije za utvrđivanje hrvatske kritične infrastrukture. Zbornik radova „Hrvatska platforma za smanjenje rizika od katastrofa", Državna uprava za zaštitu i spašavanje, Zagreb, str. 33

in the best way. The protection of ECI must lie on coordination of member states and on national and sub-national level, too. Some kind of system for CIP must be established, depending on the level of government and state structure. CIP is defined as the strategies, policies, and preparedness to protect, prevent, and when necessary, respond to attacks on these infrastructure and key assets.[11]

There is no general solution for all states in relation to CIP. CIP involves several stakeholders such as public authorities - at the national and local levels, including public agencies; the operators of CI, which are often from private sector firms; and the population at large. CIP has also increasingly gained an international dimension, which raises the question of international co-operation on CIP.[12] There are different institutions responsible for CIP in different states. The responsibility for national CIP in the USA is at the Department of Homeland Security and in UK it is a similar agency, The Home Office, in Germany, the Centre for the Protection of Critical Infrastructure is within the Federal Office for Civil Protection and Disaster Response (Federal Ministry of Interior). The process of globalization has led to a growing interdependence and interconnection of markets and networks in a number of essential sectors such as energy, information and communications, food, transport, which increases the vulnerability of infrastructure in each of these sectors. Additionally, the wave of privatization and liberalization in many of these sectors has eroded the dominant role previously played by public authorities. Most CI are today owned and operated by private sector, which therefore bear the primary responsibility for protecting their infrastructure.[13]

3. CRITICAL INFRASTRUCTURE IN BOSNIA AND HERZEGOVINA

Protection and rescue system in BiH is very complex and still in the developing phase. It has more levels, and should be base for CI management. Before we say something about CI in BiH, it is needed to understand some basic things about the protection and rescue system of BiH. The first remark is that BiH is very complex state with two Entities (Republic of Srpska and the Federation of Bosnia and Herzegovina), Brcko District and three constitutive nations (the Serbs, the Croats and the Bosniaks).

At the state level, since 2008, the system of protection and rescue has been vested to the Ministry of Security, the Department of Protection and Rescue. The framework law on protection and rescue of people and property from natural and other disasters in Bosnia and Herzegovina was issued in 2008 by the Ministry of Security of BiH and it regulates the protection and rescue system at the state level in accordance with the Law on Ministries and other authorities of BiH. According to that Law, the Ministry of Security of BiH has just a coordinating role when it comes to protection and rescue system in BiH, and the operational responsibility is in the hands of the entities and Brčko District. According to that, there is only one operational force on the state level, which has the protection and rescue task and that is AFBiH.

---

11 Lewis G.T. (2006). Critical Infrastructure Protection in Homeland Security – Defending and Networking Nation. Wiley-Interscience, New Jersey, p.8

12 Jopling L., The protection of critical infrastructure, http://www.nato-pa.int/ default. asp? SHORTCUT=1165, assessed July 31, 2013.

13 Jopling L., The protection of critical infrastructure, http://www.nato-pa.int/ default. asp? SHORTCUT=1165, assessed July 31, 2013.

The protection and rescue system is in the hands of entities and basic CIP should be also in the same hands. On the other hand, BiH has some infrastructure which belongs to the BiH state or BiH institutions are using it. Some of those infrastructures are: international airports, border crossings, military barracks, some state institutions and state officials. On the state level there exist several organizations whose job is to protect these infrastructures. Those are Border Police, Security Investigation and Protection Agency (SIPA), the Directorate for Coordination of Police Bodies of BiH and the Armed Forces. Those institutions did not recognise these infrastructures as critical, and it is not defined as CI, but according to the Law on SIPA, and its changes in 2009, the Council of Ministers of BiH is going to decide which objects should be protected, and in the same Law there is a list of persons who should be protected. The protection of embassies and international institutions is predicted in accordance with international laws which were signed by BiH. Also, according to the Law of Defense of BiH, The Presidency of BiH is going to decide which of the objects are important for defence, but on the Ministry of Defence's proposal. In contrast to some other states and militaries in the world, all military infrastructures in BiH are guarded and protected by military forces.

According to the Strategy of BiH for prevention and counterterrorism (2006-2009), this CI had to be defined, but it did not hapen, and in the new Strategy (2010/2013) there is the same task but again it was not done. Also, in the Strategy for establishing of CERT (Computer Emergency Response/Readiness Team) in BiH, as a short-term task there was the identification of CI which should be protected. In middle-term tasks list, it is written that BiH has to assess security of CI and improve work on risk reduction and also to educate the CI administrators. Moreover, nothing happened yet. Until the end of this year, the Ministry of Security of BiH would for the first time make the Plan for protection and rescue of institutions and government elements of BiH regarding natural or other disasters, focusing on the Risk Assessment of BiH regarding natural or other disasters.

It is obvious that list of CI in BiH does not exist. Just in some laws, on state or entities level, is possible to find a list of assets which belong to some of infrastructures. In the Law of Forests in the Republic of Srpska there is a list of forest infrastructure (facilities, forest roads, transportation assets, etc.) and the same is in the Federation of BiH. The same is with railway infrastructure in the Law of Railway of the FBiH or with the mainline infrastructure in the Law on Spatial Planning and Land Use of the FBiH.

In a document The Risk Assessment of BiH Regarding Natural or Other Disasters,[14] it is not possible to find a definition or a list of CI in BiH, but according to the list of infrastructure which was discussed in the document, and according to Methodology for Risk Assessment of BiH Regarding Natural or Other Disasters, it is possible to conclude that CI in BiH could be:

- Territorial political structure;
- Natural resources (forests, water);
- Population;
- Governmental buildings;
- Health capacities;

14 Procjena ugroženosti Bosne i Hercegovine od prirodnih ili drugih nesreća (2011). Vijeće ministara BiH, Sarajevo, p.4-5

- Historical monuments and cultural infrastructure;
- Environment;
- Transportation;
- Water supply;
- Energy-generating plants with transformer sub-stations and supply lines;
- Oil and gas pipelines, factories, gas stations;
- Chemical industry;
- Post offices and information system;
- Objects of pharmacy industry;
- Objects of food-processing industry;
- Geological resources and mining facilities.

Almost similar list can be extracted from the Risk Assessment of the FBiH Regarding Natural or Other Disasters. But in Risk Assessment in the Republic of Srpska it is very hard to make conclusions about CI, because they use the humanitarian tasks of Civil Protection[15] as a base for assessment. A new Risk Assessment will be done very soon and it will be done similarly to state level. In that way it will be possible to extract from that document some list of CI. But, in the Republic of Srpska, in the Plan for Making Methodology for Civil Protection, infrastructure was listed that should be risk-assessed, and the infrastructure is:

- Traffic–air, road, railway and water; telecommunication; transportation in private and public sectors; accommodation capacity in private and public sectors;
- Health and veterinary capacities in public and private sectors;
- Capacities for production and distribution of electricity;
- Basic industrial branches;
- Chemical and petrochemical industry;
- Capacities of food industry.[16]

It can be used as a base for CI list in the Republic of Srpska. Those lists that we mentioned above can be a starting point on the way to make the official lists of CI in BiH on all levels. There is a need for better coordination on all levels in the state.

4. ARMED FORCES OF BIH IN PROTECTION OF CRITICAL INFRASTRUCTURE

Today it is quite common for militaries around the world to be involved in the following five functions:

1. Protection of the independence of the state, its sovereignty and territorial integrity, and in the broader context of its citizens;
2. The preservation of peace in the international field or peace enforcement;
3. Humanitarian assistance in case of disasters;
4. Tasks of Homeland Security, and
5. Participation in nation building.[17]

Generally, those are internal and external tasks, or in some researches they are called non-traditional and traditional tasks. Geneva Centre for the Democratic Control of Armed

15 Article 61, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

16 Metodologija za izradu Plana civilne zaštite. Vlada Republike Srpske, član 9.

17Žugić B.R. (2007), Civilna kontrola vojske, VIZ, Beograd, p.21

Forces (DCAF), a research was conducted in 2012 in 15 Western consolidate democracies[18] about internal roles of the Armed Forces. The result was that there were 20 categories of roles identified, and ten fell under the broader category of law-enforcement-related tasks. Among those tasks is building and personnel security task. Only, Luxemburg, Spain and Germany do not have this task for their AF. Among those tasks there is a support for major public events and only the USA do not recognize that task for their AF. Moreover, every country is involved in the provision of aid with the help of AF in cases of natural or humanitarian disasters. It is important to add that any of the 15 countries does not have CIP as an exclusive task for its AF. Also, the conclusion was driven that calling on the assistance of the AF is considered a measure of the last resort, following the request of civilian authorities.[19]

CIP is not something new in the military tasks, even if the military does not qualify it that way. In the last ten years, big military operation near Somalia coast against the pirates has been in progress. It is classical example of world CIP. Army took the role in security measures during the Olympic Games in the USA, Greece, Canada, England and China. In England during the Olympic Games 18,000 troops were engaged and significant amount of military equipment and weapons (air-defence missiles), too.[20]. During the 2010 Vancouver Olympics, the 4,500 military personnel were engaged at land, air and sea tasks, including the use of special operations forces. In France during the African-France Summit in 2010, approximately 1,200 soldiers and 16 aircraft were deployed. In Italy the AF have been used regularly to provide security at identified key sites. In 2008, around 1,000 soldiers were sent to guard high-profile public places such as train stations and St Peter's Cathedral in Rome, and more than 3,000 Italian military personnel were deployed in support of police patrols to combat crime in 2008.[21]

Analyzing tasks in the armies of neighbouring countries, it is evident that all the armies in their assignments include the task to help civilian authorities in the event of natural or other type of disasters. In those cases, the military performs tasks such as maintaining order, providing food, medical and other resources, facilitating communication and maintenance of various types of transportation.[22]

The AFBiH in accordance with Article 4 of the Law on Defence of Bosnia and Herzegovina has five basic tasks such as:

- Participation in collective security, peacekeeping, and self-defence, including the fight against terrorism;
- Providing military defence of Bosnia and Herzegovina and its citizens in case of attack;
- To assist civil authorities in responding to natural and other disasters and accidents;

18 Austria, Belgium, Denmark, Finland, France, Germany, Italy, Luxemburg, the Nederland, Norway, Spain, Sweden and the United Kingdom, along with the United State and Canada

19 More in Schnabel A. and M. Krupanski (2012). Mapping Evolving Internal Roles of the Armed Forces. DCAF, SSR Paper 7

20 Army warns Olympic Games recovery will take two years, http://www.guardian.co.uk/uk/2012/ aug/13/army-olympic-games-recovery-two-years, Assessed June 13, 2013

21 Schnabel A. and M. Krupanski (2012). Mapping Evolving Internal Roles of the Armed Forces. DCAF, SSR Paper 7, p. 25-27

22 Centre for the Democratic Control of Armed Forces (2003). Parliamentary oversight of the security sector: principles, mechanisms and practices. Interparlemantarna Union, Sarajevo, p.72

- Mine Action in Bosnia and Herzegovina;
- To fulfil the international obligations of Bosnia and Herzegovina.[23]

In line with that the Ministry of Defence developed "The Policy of Military Assistance to Civil Authorities". The military roles according to that Policy include:

a) Help to civil authorities in the areas of:

- responding to natural and other disasters and accidents,
- fight against terrorism,
- assistance to law enforcement agencies, implementation of the protocol and representative activities;

b) To assist civil authorities in the implementation of humanitarian activities:

- countermine action and disposal of unexploded ordnance,
- medical evacuation,
- the search and rescue operations delivering humanitarian aid and other humanitarian operations and activities to help the people;

c) Other types of assistance to civil authorities, such as:

- integrated forms of assistance through the practical training of the Armed Forces (help in restoring, maintaining and building infrastructure, controlled delivery of services and the transfer of military resources to civilian use),
- conducting of cultural, sports and other activities,
- assistance in other activities that contribute to the reputation and prove the usefulness of social structures of BiH Defence.[24]

The engagement of the AFBiH in the activities of military assistance to civil authorities is carried out in accordance with legislation and in accordance with authorization of the federal authorities. The manner of engagement of the AFBiH in this case is prescribed by "The Standard Operating Procedures of Engagement of the AF BiH to Assist Civil Authorities in Responding to Natural and Other Disasters", issued by the Ministry of Defence. In accordance with the procedures in Article 11 of that document, the Minister of Security delivers to the Minister of Defence a request for AFBiH assistance, and then the Minister of Defence requests authorization from the BiH Presidency to engage the AFBiH in assisting civil authorities in responding to natural and other disasters. After obtaining the authorization, the AFBiH can be engaged in help to civil authorities. In a order to speed up military respond on civilian's request, and according to the Defence Law of BiH, the Presidency of BiH can authorize the Ministry of Defence to engage AFBiH in military assistance to civil authorities without the approval of the Presidency of BiH. In that case the Presidency of BiH makes the list of events when the Ministry of Defence can engage AF BiH without the authorization from the Presidency. The obligation of the Minister of Defence is to report to the Parliamentary Assembly of BiH and to the Presidency of BiH, about the AFBiH engagement in assistance to civil authorities in responding to natural or other disasters. It is important to emphasize that it is specified in Article 6 of the same document that the AFBiH can be engaged to assist civil authorities in responding to natural and other disasters when civil authorities exhaust the available resources or when the

23 "Official Gazette" No. 88/05

24 BiH Ministry of Defense (2010). The Policy of Military Assistance to Civil Authorities. Sarajevo, p. 6

civil authorities do not have the necessary or sufficient resources to respond to natural or other disasters.

It is obvious that AFBiH does not have direct mission of CIP if we exclude the protection of the military infrastructures. Moreover, AFBiH can be engaged in fight against terrorism where CIP has big importance, or in assistance to law enforcement agencies. Those activities, together with the protection of cultural, sports and other activities, and these are indirect but basic roles of AFBiH on CIP. Nonexistence of CI definition and the CI list in BiH is additional challenge for AFBiH on the way where to put focus and which infrastructure is the most important in the area of responsibility for the units of AFBiH so that they can make some plans, conduct some trainings and develop cooperation with other agencies and civil structures which are responsible for CIP in that area.

5. CONCLUSION

There is no broadly accepted definition of CI and it is still a question of a single state. Also, there are different selection criteria for CI depending on the country of origin and the practical interpretation of a list of CI, and it depends on a unique methodology. Each state or organization must define and classify its infrastructure and underline which infrastructure is critical. According to the EU documents CI must be defined and listed in all member countries and in all countries which want to become the members of the EU. As for BiH, there is not any state strategy or central institution which deals with CIP. The same situation is on entities level. Also, there is no definition of CI in official documents and there is no any official list of CI. According to that, there is not any plan or other document, on a state or entities level, that discuss CIP. There is a need for a common definition of CI on the state level, which should be accepted by entities and lists of CI on state, entity and municipality levels. It will be a starting point to CI risk management. It is needed to establish temporary working group for CIP to define CI and make a list of CI in BiH, and to issue the law about CIP on state and on entities level. Moreover, information between private sector and government, between state and entities and between entities themselves must be shared, and the flow of information must be better and constant.

The military in general plays only a supportive role in CIP, focusing mainly on consequence management, which is in the aftermath of an emergency.[25] In the immediate aftermath of a conflict, catastrophic incident or natural disaster when appropriate civil agencies are unable to act quickly or operate with sufficient safety, the reconstitution of CI and the restoration of essential services may fall to the military, within the means available.[26] The AF are not the primary domestic security providers within a country's security sector. They are secondary security providers that are called upon under exceptional circumstances, when police or other internal security organization (gendarmerie, carabineers) are not in a position to respond adequately to a particular security challenge.[27]

Armed Forces of BiH in the area of CIP generally play an indirect and supportive role in CIP, focusing mainly on consequence management. AFBiH must stay secondary security

25 Jopling L., The protection of critical infrastructure, http://www.nato-pa.int/ default. asp? SHORTCUT=1165, assessed July 31, 2013.

26 AJP-1 (D) – Allied Joint Doctrine – STANAG 2437, p.2/17

27 Schnabel A. and M. Krupanski (2012). Mapping Evolving Internal Roles of the Armed Forces. DCAF, SSR Paper 7, p. 52

provider and a resource of the last resort, when efforts are required to respond to exceptional situation and CIP. The protection of military installation must stay primary protection task of AF, but modern militaries are more and more included in non-traditional tasks, so AFBiH must reconsider their internal role, too.

REFERENCES:

1. AJP-1 (D) – Allied Joint Doctrine – STANAG 2437
2. BiH Ministry of Defense (2010). The Policy of military assistance to civil authorities. Sarajevo
3. Centre for the Democratic Control of Armed Forces (2003). Parliamentary oversight of the security sector: principles, mechanisms and practices. Interparlemantarna Union, Sarajevo
4. Čemerin D. (2011). Upravljanje kritičnim infrastrukturama. Zbornik radova, IV međunarodna konferencija, „Dani kriznog upravljanja", Veleučilište Velika Gorica
5. Čemerin D. i D. Trut (2010). Kriterije za utvrđivanje hrvatske kritične infrastructure. Zbornik radova „Hrvatska platforma za smanjenje rizika od katastrofa", Državna uprava za zaštitu i spašavanje, Zagreb
6. Herga M. (2010). Nacionalna kritična infrastruktura. Menadžment i sigurnost – M&S 2010: "Planiranje i sigurnost"
7. Jopling L., The protection of critical infrastructure, http://www.nato-pa.int/ default.asp? SHORTCUT=1165, assessed July 31, 2013.
8. Lewis G.T. (2006). Critical Infrastructure Protection in Homeland Security – Defending and Networking Nation. Wiley-Interscience, New Jersey
9. Metodologija za izradu Plana civilne zaštite, Vlada Republike Srpske
10. More in Schnabel A. and M. Krupanski (2012). Mapping Evolving Internal Roles of the Armed Forces. DCAF, SSR Paper 7
11. Official Journal of the European Union L 345, 23.12.2008, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF, Assessed July 09, 2013
12. "Official Gazette" No. 88/05
13. Procjena ugroženosti Bosne i Hercegovine od prirodnih ili drugih nesreća (2011). Vijeće ministara BiH, Sarajevo
14. Schnabel A. and M. Krupanski (2012). Mapping Evolving Internal Roles of the Armed Forces, DCAF, SSR Paper 7
15. Smedts B. (2010). Critical Infrastructure Protection Policy in the EU: state of the art and evaluation in the (near) future. Royal High Institute for Defense, Center for Security and Defense Studies, Focus paper 15
16. Zuter B. (2011). Strateški krizni menadžment Švajcarske-poređenje švajcarskog modela sa devet stranih referentnih država, Vojno delo, jesen/2011, Beograd
17. Žugić B.R. (2007). Civilna kontrola vojske. VIZ, Beograd

UDC 726.9:75.041.5
ID 176374796

Marjan Đurovski
Faculty of Security, Skopje
mgjurovski@fb.uklo.edu.mk

NATIONAL PLATFORM OF THE REPUBLIC OF MACEDONIA FOR REDUCING THE RISKS OF CATASTROPHES EFFICIENCY MECHANISM

Abstract: Including risks and catastrophes in the category determined by the aspect of surprise, i.e. which means never being able to predict when a situation might occur that in any way could endanger the normal everyday life or could cause material damage to society, strategy for efficient action in case of critical incidents seems to be more than necessary in the Republic of Macedonia. The strategy should correspond to a long-term plan for maintaining minimal criteria of security when speaking of disasters and catastrophes, institutions that are most responsible for taking action in such situations, available measures and resources, cooperation among them and the way of acting in case of actual management of certain crises.

The national platform for reducing risks of catastrophes represents a national mechanism for coordination and gives a political direction in the sphere of reducing risks of catastrophes. It is a multi stakeholder structure with interdisciplinary practice involving state institutions, civil society and the public. The approach of establishing and functioning of the National platform depends on the strategic and political forces of society, as well as on cultural qualities. The National platform provides coordination, analyses and recommendation for priority areas and demands focused activity through processes of coordination and active participation of those in charge.

The paper makes an analysis of the National Platform and it offers solutions for enabling greater mechanism for overcoming risks of catastrophes.

Key words: *risks, catastrophes, platform, security, disasters*

1. INTRODUCTION

Accidents and disasters are inevitable. They have caused and will continue to cause human casualties and material damages. However, in the past decades, we have been witnessing a rapid rise in their intensity fueled by accelerated climatic changes and technological development. The latter in its own respect does not always reflect a developed conscience of the risks that it brings about and lacks the necessary level of risk management skills. As a result, the loss of human life and material damage has attained disturbing proportions, considered academician Georgi Efremov.

Therefore, it was recognized that there was a need for a common and systematical approach through a global strategy that would guide and support the efforts and initiatives for prevention, early warning and response to the effects of natural hazards and human

negligence. The United Nations took a large step forward in this direction by declaring 1990-1999 to be an International Decade for Natural Disasters Reduction. The experiences gained have shown that the success of the long-term prevention strategies depends first and foremost on broad-based, cross-sectoral and interdisciplinary cooperation of all stakeholders – national and international, central and local, governmental and non-governmental.

In that regard, the United Nations International Strategy for Disaster Reduction was established to enhance and strengthen the resilience to what sometimes is unavoidable. Thus, the understanding of the natural hazards in themselves does not inevitably lead to disasters, but that disasters result from the impact of natural hazards on vulnerable individuals and communities, was recognized as a revelation. Therefore, the challenge to make a major conceptual shift from the traditional approach focused on disaster response towards a new, systematical and holistic risk reduction and consequence management has become a global imperative.

The appeal for the nations worldwide to develop national and sub-national mechanisms for systematic and thorough disaster risk reduction had its conceptualization in the Hyogo Framework for Action 2005-2015: Building the Resilience for Nations and Communities to Disasters. Supported by 168 countries, among which is the Republic of Macedonia, the strategic and systematic approach to disaster risk reduction acquired additional legitimacy. The nations were requested to build up their own National Platform models, in accordance with the objective circumstances that are unique for every country.

Macedonia is not an exception when it comes to disaster vulnerability, neither is it significantly immune to its consequences. Facing the disastrous 2007 wildfires, the Republic of Macedonia took major steps in creating a Macedonian model of a National Platform for Disaster Risk Reduction. In its core lies the approach of effective and efficient risk reduction by integrating all available and relevant capacities and resources at all levels. Guided by this methodologically consistent approach, networks were formed of all national and local-level governmental and non-governmental stakeholders whose contribution is important for prevention.

The governmental bodies and agencies, the units of local self-government and the capital City of Skopje, the public enterprises, institutions and services supported this national project, giving strong institutional base for its implementation.

Volunteers altruistically devoted themselves to risk reduction through the engagement of the NGO federations, along with the Red Cross of Macedonia and the numerous professional and humanitarian associations.

The interdisciplinary nature of disasters requires an appropriate response. The scientific-technical and expert backbone of the National Platform is composed of the academic institutions, including the Macedonian Academy of Sciences and Arts, the public and private universities and research centers and observatories. The impressive National Laboratory Network which brought under one umbrella 173 laboratories nationwide only added to the picture.

The inclusion of a number of private companies and the Business Chamber to support the National Platform is the best example of sharing the social responsibility on behalf of the business community.

Finally, worth mentioning is the addition of the religious communities and groups, who, openheartedly and with a joint spiritual message, supported this grand effort.

Noteworthy is the systematic approach taken in the development of the National Platform through the integration of national and international practices as well as the theoretical and methodological consistency and practical usability of system solutions.

Based on the integrated system approach paradigm and the well known transmissions and complex approaches with simple institutional design, the National Platform is actually an exceptional integrating tool which guarantees synergy among all stakeholders. In this regard, it is understandable that it was internationally recognized as a referent model for consistent approach towards prevention, early warning and response to a wide spectrum of risks and possible accidents and disasters, considered academician Georgi Efremov.

2. THE BASIS OF THE NATIONAL PLATFORM IN NATIONAL CONCEPTUAL AND STRATEGIC DOCUMENTS AND IN LEGISLATION

The National Platform of the Republic of Macedonia for Disaster Risk Reduction, apart from the political will expressed by Macedonia's adoption of the Hyogo Framework for Action, has its roots in the following two key conceptual and strategic documents, as well as in several laws, one of which is crucial in this context: The National Security and Defence Conception (2003), the National Security Strategy of the Republic of Macedonia (2008) and the Law on Crisis Management (2005).

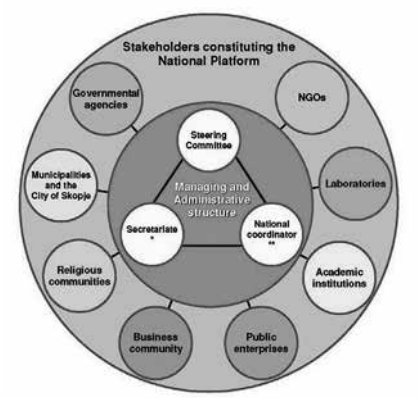
The "National Security and Defence Conception," as a baseline document of the Republic of Macedonia, defines the state's views and positions in terms of security, defence and crisis management. Chapter III is especially important for crisis management, where it is stated that "The basic purpose of the Crisis Management Centre is to maintain the continual preparedness level of the State, consultations, continuity, inter-sectoral and international cooperation, coordination, the production and maintenance of a unified and single assessment of the threats, risks and dangers to the security of the Republic of Macedonia, as well as the proposal and adoption of measures and activities aimed at resolving crisis situations and crisis."[1]

The Law on Crisis Management, adding to the previously-mentioned document, regulates the Crisis Management System, prescribing its composition, competences and way of functioning. In that regard, Article 2 instructs the following: "The Crisis Management System is performed by state administration bodies and state authority bodies (the Parliament, the President and the Government), the Armed Forces, such as the Army of the Republic of Macedonia, rescue and protection forces, and bodies of the municipalities and the City of Skopje. Public enterprises, public institutions and services, and trade associations can participate in the prevention, early warning and crisis management according to this Law. Citizens, citizens' associations and the Red Cross of the Republic of Macedonia, non-governmental and humanitarian organizations, media, and other subjects with legal personality which are not covered by paragraphs 1 and 2 of this Article, can participate in the prevention, early warning and crisis management, voluntary and by contract, according to this Law and the ratified international agreements regulating this matter."

1 „Национална концепција за безбедност и одбрана" www.vlada.mk, 25.02.2010 Скопје

The same Law, in order to achieve continuous consultations and decision making at the highest level, maximal coordination, timely response, effective and appropriate utilization of the available competences and resources in case of crisis and crisis situations, as well as for timely, quality and real assessment of the risks and threats to the security of the Republic of Macedonia, within the Crisis Management System, establishes a Steering Committee, an Assessment Group and a Crisis Management Centre as an independent governmental body.

The position of the Crisis Management System is further elaborated in the "National Defence and Security Strategy of the Republic of Macedonia." Hereof, Chapter 1 of this document entitled "Definition and Principles of National Security" recognizes that the "...main components of the national security system..." (implemented in accordance with Euro-Atlantic and European standards) are also "...the development of a unified system for the prevention, early warning and crisis management and protection of people and goods..." Additionally, Chapter 5 of the same document entitled "Implementation of the National Security Interests of the Republic of Macedonia or Strategic Concept", refers to the "...collaboration with countries in the region, especially by giving high priority to the compatibility and information exchange with regard to accidents and disasters on regional and sub-regional levels, through the strengthening of existing mechanisms and the application of improved communication and coordination techniques, the engagement of national crisis management resources for assisting other countries and the participation in international exercises." These documents are the fundamentals to what already is institutionalized as a National Platform, which is entirely dedicated to providing an integrated, efficient and effective approach to prevention, early warning, management and mitigation of the consequences of natural and man-made accidents and disasters, while ensuring a functional unity of the state authorities, the local self-government, the NGO sector as well as the academic and business communities. Consequently, the above mentioned documents imply the development of a governing system, structure (institutional network) and functional linkages that guarantee timely, systematic and coordinated response by National Platform stakeholders, as well as the planned build-up and optimal utilization of available resources (human, material-technical and financial).

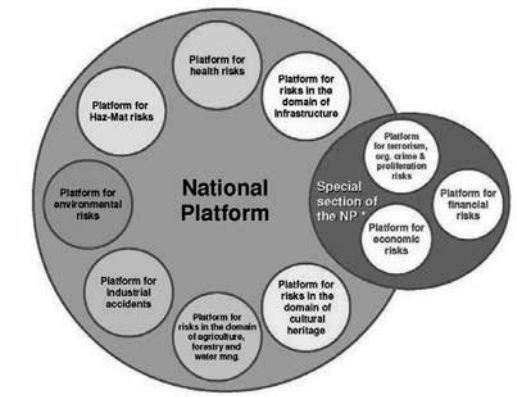


THE NATIONAL LEVEL

3. THE ORGANIZATION AND STRUCTURE OF THE NATIONAL PLATFORM

The National Platform is organized on national and local levels. However, when threats surpass municipal boundaries, the establishment of regional structures covering several municipalities is anticipated. This corresponds with the regional organization of other relevant governmental structures, such as the police.

The managing body of the National Platform is the enlarged Steering Committee headed by a government-appointed minister. Other ministers, a representative of the Security and Defence Commission of the Assembly of the Republic of Macedonia, the National Security Adviser to the President of the Republic, the President of the Association of Local Self-Governing Units, as well as directors of the Crisis Management Centre and the Rescue and Protection Directorate participate in the Committee's work. The Steering Committee determines the direction of the National Platform's development; it verifies the accomplishments and suggests certain operational solutions with system consequences.[2]

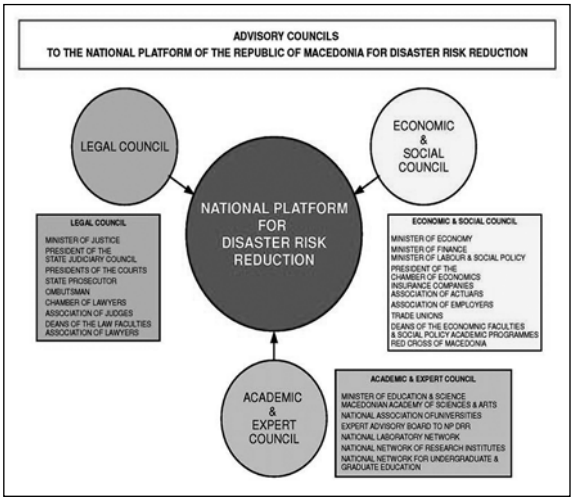


The Steering Committee's authority extends to two bodies: the Council of State Secretaries and the Inspection Council. The Council of State Secretaries is headed by the Secretary General of the Government and is composed of state secretaries of ministries and directors of the independent governmental agencies. If necessary, the directors of bodies within ministries can also be invited to participate in the work of the Council. The task of the Council of State Secretaries is to bridge over the problems and to mark out administrative-expert decisions affecting the accident and disasters risk levels addressed by the National Platform. In that regard, nine working groups have been established composed of high ranking representatives of ministries and independent governmental agencies, whose work is coordinated by the state secretaries of competent ministries or other governmental agencies, according to their competencies and experiences in specific domains.

Within the Crisis Management Centre, the State Operation Centre functions on a central (national) level 24 hours a day, 7 days in the week through the Single Communication and Information 195 Centre (soon to be replaced by the Emergency Call Service 112). The Early Warning and Alert System is also part of the State Operation Centre, and, as such it

2 Лазаревски П. и др. (2010). Национална платформа на Република Македонија за намалување на ризици од несреќи и катастрофи. Скопје

is to be thoroughly reconstructed and modernized in the implementation process of the E-112 system.



When necessary, headquarters in the Crisis Management Centre and the Rescue and Protection Directorate are formed, which according to the National Platform concept are to be united in a single unified command structure. The National Platform, apart from interlinking the various government and non-government stakeholders on the national level, also has its structures on local and regional levels.[3]

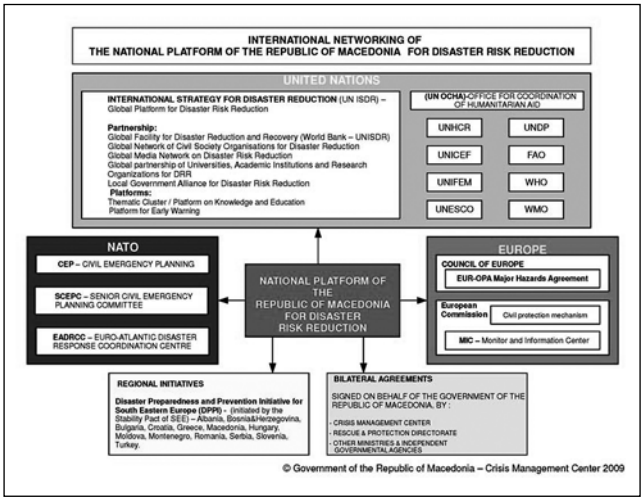
4. INTERNATIONAL NETWORKING OF THE NATIONAL PLATFORM

Within the United Nations system, the networking of the National Platform for DRR of the Republic of Macedonia is multilayered. As a member state of the UN, the Republic of Macedonia participates in the Global Platform for Disaster Risk Reduction, thus contributing to the formulation of the Global Platform's guidelines. The Republic of Macedonia is directly linked to the ISDR and closely collaborates with the UNISDR for Europe through the National Platform for DRR and the Crisis Management Centre, which is a Hyogo Framework for Action Focal Point institution. To that end, participation in the European Forum for Disaster Risk Reduction in the capacity of Co-Chair for 2010 is exceptionally important.[4]

The National Platform is related to several regional European organizations. Within the European Forum for DRR, the National Platform collaborates with the European and Mediterranean Major Hazards Agreement (EUR-OPA), which alongside UNISDR for Europe provides administrative-technical and expert support to the forum. The Republic of Macedonia is represented in EUR-OPA's scientific segment through the European Centre for Vulnerability of Industrial and Lifeline Systems (ECILS).

3 Закон за управување со кризи, Службен весник на Република Македонија бр. 29/2005 Скопје

4 Republic of Macedonia - Structure of civil emergency planning. International CEP Handbook 2009, Swedish Civil Contingencies Agency (MSB), Karlstad, 2009



The National Platform is correlated to the European Union on two levels. Indirectly, the European Commission closely cooperates with the ISDR in promoting and implementing the Hyogo Framework for Action. Also, the EU is UNISDR's partner in the European Forum for DRR. Directly, the EU cooperates with states through its community mechanism for civil protection, which promotes cooperation in the field of civil protection and aims to assist emergency actions.

On the sub-regional level, the Republic of Macedonia and its National Platform cooperate with the Disaster Preparedness and Prevention Initiative for South Eastern Europe (DPPI SEE) in two areas. The Republic of Macedonia is represented in the DPPI SEE through the Rescue and Protection Directorate. The second cooperation channel leads through the European Forum for DRR, in whose work DPPI SEE participates, based on the second European Forum principle which calls for building on existing institutions and organizations.

Relations with NATO are indirect and go through the Crisis Management Centre, which is a National Platform Focal Point institution and is also directly involved in NATO emergency management mechanisms such as the Civil Emergency Planning (qvd), the Senior Civil Emergency Planning Committee (SCEPC) and the Euro-Atlantic Disaster Response Coordination Centre (EADRCC)[5].

5. ACTIVATION OF THE NATIONAL PLATFORM

The activation of the platforms is in stages, from local to the national level. It begins with a risk assessment and local capacity assessment. If the assessment shows the municipality has no managing capacity, then the next, regional level of the platform is being activated, which involves the Regional Council of the National Platform and regional. However, if the Regional Council finds the managing capacities to be insufficient, then the Main (National) HQ is set in motion "...as an operative-expert body heading the prevention and cri-

5 Лазаревски П. и др. (2010). Национална платформа на Република Македонија за намалување на ризици од несреќи и катастрофи. Скопје

sis management activities..." Nevertheless, if there is still lack of managing capacity, then the Main HQ informs the Assessment Group, which, at its end, informs the Steering Committee. The Steering Committee informs the Government and proposes a state of crisis to be declared. Declaring a state of crisis means that the national level is being activated. This implies the engagement of all available resources, including the Army of the Republic of Macedonia.

Relevant international actors are informed about the state of crisis through appropriate mechanisms (EADRCC). When the situation exceeds national managing capacities and resources, then the Government seeks international assistance by activating other multilateral and bilateral mechanisms.[6]

6. CONCLUSION

The general approach to handling accident and disaster risks, regardless of whether the events are natural or man-made, is to prepare a single-doctrine position that will be used as a blueprint to mark out specific strategies, policies and legislation. During a session held on November 19, 2009, the enlarged Steering Committee of the National Platform accepted the following basic doctrine position for accident and disaster risk reduction: PREVENTION AND EARLY WARNING ARE THE BASIS FOR PREVENTING IN TOTAL OR THE DISASTEROUS CONSEQUENCES OF NATURAL HAZARDS OR MAN-MADE ACCIDENTS, WHILE THE PREPAREDNESS OF EACH STAKEHOLDER AND THEIR CAPABILITY FOR COORDINATED AND RAPID RESPONSE ARE PRECONDITIONS FOR REDUCING THE CONSEQUENCES AND RAPID MITIGATION OF SUCH ACCIDENTS.[7]

The general strategies concerning the specific risks covered by the National Platform will be determined based on the basic doctrinary position. In fact, the general strategy answers the question of how the basic doctrinary position will be implemented with regard to each specific risk. The general strategy is then particularized through functional strategies referring to:

- Prevention (how the general strategy will be implemented in terms of prevention);
- Reaction (how the general strategy will be implemented in terms of response to the occurred situation);
- Rehabilitation (how the general strategy will be implemented in terms of rehabilitation).

The strategies provide general directions on where the solutions for the possible problems should be looked for. In other words, they help us find out:

- What should be done to prevent an accident or disaster?
- If, however, an accident occurs, what should be done to prevent it from taking disastrous proportions, or, rather, to prevent more tragic consequences than the initial ones?
- After the event has occurred and the situation has been put under control, what should be done to restore normal life in the community (as normal as it can be)?

6 Senior Civil Emergency Planning Committee (SCEPC)" www.nato.int, 8.02.2010

7 Лазаревски П. и др. (2010). Национална платформа на Република Македонија за намалување на ризици од несреќи и катастрофи. Скопје

Such strategies are the basis for creating appropriate prevention, reaction and rehabilitation policies that refer to various aspects of a certain situation, such as policies concerning public awareness and public relations in terms of the potential problem and the approach to sanctioning improper actions implying risk. Others include how to financially cover prevention expenses (will it be, for example through the budget, insurance or via other means) and how to deal with an occurring accident or disaster. These policies actually answer the question of how the functional strategies will be transformed into specific steps, while having in mind:

- The very nature of the threat and risk;
- The characteristics of available resources (human, institutional, financial and material-technical);
- The general attitude of citizens, their perspectives on their personal responsibility and the responsibility of institutions, and, in that context, their expectations and preparedness for personal engagement.
- These policies are put into practice through the development of:
- Operational strategies for their implementation, which are specific ideas on how the policy will be implemented in practice and who should do what in order to fulfil the purpose of the specific policy. In this regard, the operational strategies are an introduction to operational plans which, while relying on predetermined financial and material-technical resources, point to the order and timeframe of actions to be taken by specific actors in order to achieve a specific goal;
- Programs and projects for policy implementation, such as a program for strengthening individual and collective responsibility as well as citizen pro-activity with regard to a specific risk (e.g. an earthquake). This program will be developed through specific projects focused on increasing the public awareness among various target groups (e.g. minors, people with special needs, women and senior citizens) in how they should behave (or how they should be treated) when faced with a specific problem. The implementation of these projects requires project activity planning, which would fit among the operational strategies of the afore-mentioned operational plans.

The implementation of accident and disaster risk prevention policies (as well as programs and projects developed in this context) implies an appropriate normative framework. This means that the implementation of a specific policy relies on the existing legislation (which can be altered and improved) or requires the adoption of new laws and regulations. Effective policy implementation, besides relying on the conscience of individuals, also requires an unambiguous set of rights and obligations that define proper behaviour and forbid and sanction misbehaviour that could have negative effects on life, health or property. (For example, when implementing a policy that, in case of an earthquake, should prevent catastrophic consequences, it is not enough to count on the goodwill of construction companies and investors in order to ensure that they build a seismic proof building.

Rather, it is necessary to legally define construction standards and to control their implementation in practice. A general strategy, functional strategies, policies, operative strategies, programmes and projects, as well as specific legal solutions should be determined for each specific risk considering each risk (e.g. epidemics or earthquakes) requires a special approach.

7. REFERENCES

1. Лазаревски П. и др. (2010). Национална платформа на Република Македонија за намалување на ризици од несреќи и катастрофи. Скопје
2. Национална концепција за безбедност и одбрана. www.vlada.mk, 25.02.2010 Скопје
3. Закон за управување со кризи, Службен весник на Република Македонија бр.29/2005 Скопје
4. Structure of civil emergency planning (2009). International CEP Handbook 2009, Swedish Civil Contingencies Agency (MSB), Karlstad
5. Senior Civil Emergency Planning Committee (SCEPC) www.nato.int, 8.02.2010

UDC 726.9:75.041.5
ID 176374796

Ivana Simović-Hiber
University of Belgrade, Faculty of Security Studies
ivanassss@hotmail.com

THE ROLE OF THE CRIMINAL LAW IN PROTECTING INFORMATION SOCIETY

Abstract: Post modern society is often characterized as an *"information society"* because of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society lays indeed emphasis on technological innovation, meaning that information and knowledge are key-resources. But, information societies are not solely defined by the technological infrastructure in place, but rather as multidimensional phenomena. So, it is important not to focus only on the technological side, but also on the **social attributes of the information society**, including the social impact of the information revolution on social organizations, including the criminal justice system. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control **(surveillance society**). But, these developments have also led to a situation where the attacks on the integrity of IT have become serious threats that can affect not only individual interests but also the critical infrastructure and the security of states.

Modern information technology also has transformed the habitual dimension of certain assaults on legally protected interests. The special sensitivity of IT to criminal attacks makes it necessary to employ the criminal law in preventing and sanctioning the acts that interfere with the integrity of communications based on IT. But, many of the general problems of criminalization (ex precisely defining the criminal act) pose themselves in this area, and some of them are especially acute when a legislature sets out to incriminate the assaults on the integrity of IT. The following specific problems come to mind: how can criminal law keep up with the quick pace of **information technology development** and of the character and contents of the worldwide web? Does the progress of IT lead to **new legal interests**, and how can they be defined and protected? How can criminal laws be sufficiently precise to satisfy the **principle of legality**? How to protect the ***ultima ratio*** principle in criminal law?

We may conclude that the specific risks and the vulnerability of "information society" create new challenges to the criminal law, testing the limits of the criminal law as we know it.

Key words: *ICT, Criminal Law, surveillance society, new legal interests, protection*

1. INTRODUCTION

Everybody is talking about the information society by assuming a particular meaning and starting from a definition. Meaning by default is in itself a dangerous category, because it carries within itself the capacity of fiction that does not allow for an accurate interpretation of the phenomenon (in this way modern criminal law is also a victim of changed priorities, no matter how ludicrous it may seem). Therefore, some questions will be asked in this paper about criminal law as **an instrumentalized normative order.**

It is an almost indisputable premise that the digital revolution is also a technological revolution that has changed the modern society and modern consciousness. The post industrial society as a whole is faced with new challenges and requires a completely new protection. Criminal law is a repressive response to the functional disruption of relations within or upon the social interaction. Most literally this consequently must mean that it plays no role of preventive mechanism to protect these relationships. Furthermore, the repression of criminal law presumes that its role as a means exhausts *ultima ratio*, that is, it becomes operative after the exhaustion of non-legal and other legal protective mechanisms.

The problem of legal protection of critical infrastructure is an almost non-existent issue (it exhausts in partial and inconsistent norms that respond to a perceived big problem). Inadequate perception of this phenomenon as legal opens many dilemmas. Let us mention the basic ones. Modern language that talks about pushing the boundaries of protection in fact inaugurates the disrespect of the principle of legality in criminal law. The paradigm of September 11 is known to all, with a total misunderstanding of the scope and range of its influence on the irregularity of functioning of modern society as its main effect (Guantanamo syndrome and fragmentary protection of information society in their specific expression are only some basic examples of the confused state of understanding and distinguishing between permissible and impermissible). Law as an instrument, as a concept cleared of system of norms functioning as the protection of (moral) justice and fundamental human rights plays almost a negative role, completely different from the default. Therefore, an attempt will be made in the paper to analyze some of the problems identified.

2. AN ATTEMPT TO DEFINE THE INFORMATION SOCIETY

There is no single concept of a conceptual definition of the information society. There is no doubt that the definition (technical, economic, social, legal and cultural model) depends on the focus of perception. The information society is also the main determinant of what we mean when we talk about post-modern or post-industrial society. In this way the technological innovation (IT systems, transmissions, information technology, nanotechnology, biotechnology) becomes a virtual part of every segment of modern society. From this hypothesis a new one is created - information and knowledge are the basic resources of the new world. It seems that at this point already some other issues need to be opened up and different hypotheses formulated. It is impossible for a society to monitor and "help" the development and protection of the information society outside the context of the society in its base (sociological) sense. The information society as a phenomenon, although it is recognized as multi-dimensional, must be perceived primarily in social attributes, based on the acceptance of the impact of the IT revolution on social organization, including the criminal justice system. First of all, the relationship (or the link) between knowledge and information is fundamentally changed. The transformation of communication into permanent information technology even changes the way knowledge is socially valued. It can be said that the structure of traditional authority (in the state and law) is being gradually superseded by alternative methods of societal control ***(surveillance society)***.

The problem that deserves to be emphasized at this point is the relationship between criminal justice and security. Contemporary moment also in a more and more explicit form indicates the presence of a new and dangerous utopia. If we say that we participated in the "old" utopia of classless society that was realized by the existence of a real dictator-

ship (Mannheim, 2006, p. 200), we can imply that **the new utopia** of a society without risk and danger in "waiting" for its coming into being is realized through the multiplication of criminal offences, tightening of the penal system and most importantly the promotion and justification of the permanent state of exception (Salas , 2012, p. 20), or a legal emergency. In pursuit of a society without risks we are at a "temporary" state of constant, but implicitly uncertain fight against crime. It is believed moreover (Vervaele, 2011, p. 1) that a new type of state (network state) is in formation, which gradually replaces the nation-state model of the industrial era. Here we must stop counting, it would seem, the general outlines of the modern world. The society of control and security necessary brings previously unknown transformation in the diffusion of interactive networking of organizational forms of the public sector. Information and knowledge as the main resources of information society by influencing the political structure of society and the state necessarily affect the structure and content of the criminal justice system. We talk about the new penal code. In reality , the so-called new criminal law is essentially the adjustment of criminal law to new social conditions, by finding new forms and instruments in the protection of new values; for example in addition to protecting IT, economic criminal law and risk criminal law are discussed (Zapatero 2011-2012, p. 43).

3. INFORMATION SOCIETY AND SYSTEM OF LEGAL PROTECTION

3.1 The need for protection of information technology

Until only a few decades ago it seemed impossible that social life depends on information technology (IT below), primarily the global Internet, and that both public and private spheres become vitally dependent on communication networks, and the access to information becomes as important as the access to material goods. Hence the attacks on the integrity of IT, overcoming individual interests, have become an important part of the legal protection of financial interests, economic and security system of any state.

IT in this sense becomes an important tool for the commission of offenses, and the protection from this kind of crime is included in the "large catalog" of global threats such as terrorism, human trafficking, environmental protection, and similar granular problems that are added to the catalog, to the extent that illustrates their real danger, and with which no national government alone can cope. This state of affairs has a special, but very important consequence that national governments are often limited by the influence of transnational actors even when the issues that are still national to a great extent are in question, such as the law. Without opening for discussion here the larger problem of a specific kind of erosion of the absolute importance of the right to vote (and the representative democracy itself) in a new context, we will keep to the identified basic problems of justice reaction.

In the introductory notes the problem of the lack of a stable definition of information society is mentioned, or more precisely its instrumentalization, making it difficult to determine the relevant object of protection.

Dependency of the object of legal protection is a particularly sensitive issue because of the new **quantitative dimension of IT crime** (including the speed of object of protection potential violation). Although quantitative dimension is not crucial for determining the seriousness of a crime (for example, even though the number of victims of terrorism is statistically significantly smaller than the total number of murders per year, it does not affect the special treatment of terrorism) in this case it is a very important dimension. Within the contours of

absolute specificity the fact should be noted that cyber crime allows for anonymity and thus a certain "immunity" of perpetrators from prosecution. **The findings of numerous studies indicate that the dark figure of cyber crime is extremely high.** The reasons for this are many, but first we start with the fact that it is not easy to statistically process any type of crime due to at least three main reasons. Firstly, it is necessary that a certain activity is generally perceived at all, then for it to be qualified as a criminal activity and, finally, to be registered as such and known to the authorities. If any of these phases is absent which is often the case with this type of crime, the undertaken criminal activity will not be recorded in the statistics of the authorities, thus becoming a portion of the dark figure of crime.

The mentioned dimensions of IT crime change **the role of criminal law reaction, which in addition to the basic repressive gets the preventive component.** In reality, it is a new criminal law, as mentioned in the introduction and first of all would be **risk criminal law**. In legal and technical terms this means that in addition to the national criminalization there is a tendency to harmonize the norms at the international level (Albrecht Fijnaut, 2002, p. 100). Not getting into making an analysis of a concrete criminalization at this point, it seems interesting to make a few comments.

At the international level, very indicative are the activities of the Council of Europe. The first international initiative comes about at the European Conference on Criminological Aspects of Civil Crime that took place in Strasbourg in 1976. Criminal offenses of computer fraud, forgery committed by using a computer and damage to computer data in "historic" terms are emphasized as new. In 1989, the Recommendation on criminal activities related to computer use is adopted.[1]

This recommendation contains a binding list of minimum requirements relating to explicitly stated criminal offenses against the security of computer data, in order to be prescribed in a uniform manner by the legislation of the Member States (for example, computer sabotage, and unauthorized access to a computer). In addition to the binding, the recommendation includes the so-called optional list, or the list of offenses the regulation of which is left to the disposition of member states. On this list are computer espionage, unauthorized use of a computer and unauthorized modification of computer data or programs.

Besides the Council of Europe, the Organization for Security and Cooperation in Europe (OSCE) also extensively dealt with issues of this kind of crime (in 1982, an expert group is founded to examine the state of legislation in the field of cyber crime and to formulate the appropriate recommendations to amend national legislation in order to harmonize the legal norms to the real needs). As a result of the work of this group the OSCE adopted the Recommendations on the Harmonization of Criminal Law through the analysis of the laws of the Member States in 1986. In addition, demonstrating the need for cooperation at the international level, similar to the recommendations of the Council of Europe, the OSCE also makes a list of prohibited conduct in cyberspace, which includes computer fraud and forgeries, damage to computer data or programs, and unauthorized penetration of a protected computer program or a protected computer system.

It is a unanimous opinion that the most important international legal instrument in this area is the Council of Europe Convention on Cybercrime adopted in 20012 (we should mention the Additional Protocol to the Convention of 2003, which deals with

1 Council of Europe Recommendation No. R.(89) 9

2 Serbia is on the list of the countries that signed (2005) and ratified (2009) the Convention (Official Gazette of the RS, No. 19/09)

the incrimination of documents and materials that contain messages of racist and xenophobic nature sent through computer systems). The objectives of the Convention are primarily the harmonization of national legislation with regard to the substantive provisions, the introduction of appropriate instruments of national legislation with regard to the procedural provisions in order to create a basis for the investigation and prosecution of these crimes and the establishment of effective institutions and procedures of international cooperation. Therefore, the promotion of cooperation between police and other relevant authorities among the countries of the world is one of the main tasks of the development of mechanisms for combating cybercrime. It is important to note that the preamble to the Convention refers to a number of international documents produced by the United Nations, the Council of Europe and other international organizations, which establish certain standards of respect for human rights, especially the rights of children and the rights to privacy and security of personal data. In this way, the creators of the Convention clearly state their intention that this text is not to undermine the existing standards for the enjoyment of human rights by government interference, i.e. police and investigators in the privacy of individual or business operations, but rather to establish the effective protection elements of the same rights against unauthorized attacks.

The Convention consists of four sections (term using; measures to be taken at national level - substantive and procedural law; international cooperation; and final provisions). The first chapter of the Convention consists of only one article, and provides a brief overview and the definitions of key terms that are used in the text to follow. The second chapter of the Convention is divided into several parts and covers a variety of substantive and procedural measures that States Parties undertake to introduce into national legislation. The purpose of the substantive provisions is to improve the means of prevention and the punishment of crimes that involve the use of modern technology. In doing so, the Convention should establish common minimum standards with regard to the criminalization of the offense (this approach also eliminates the possibility to object to the lack of dual criminality in the event of a possible extradition of the offender).

It is worth mentioning here the so called Millennium Declaration, i.e. the Resolution No. 55/2 of the UN General Assembly of 2000, which establishes as one of the priorities the need that new technologies, especially information and communication, be made safe and available to all at the same time. The basic principle that the said resolution underlines is that all States, through their respective national legislations, should prevent the existence of the "safe houses" for the offenders of cyber crime. This actually points out the need for synchronized legislative action at the global level and indicates a potential danger to any country failing to legally regulate this area that it could attract into its territory a number of potential perpetrators.

The legal response to the threat of cyber crime would have to be directed towards the standardization of prevention in order to prevent or alleviate the effects of committing cyber crime and that the potential victims (users of information technology) become aware of the dangers they are exposed to, and the adoption of the appropriate legislation in the field of material and procedural criminal law so as to create legal instruments to combat cyber crime. Following the general recommendations and the commitments from the international acts States Parties are obliged to criminalize certain actions as acts of cyber crime in their national legislations.

The laws and regulations of the Republic of Serbia in the fight against cyber crime follow the appropriate standards. Legislative solutions relating to the field of cyber crime in the legislation of the Republic of Serbia can be divided into three groups.

The first group consists of the Law on Organization and Jurisdiction of Government Authorities in Fight against Cyber Crime,3 which establishes the organization and jurisdiction of special state authorities to combat this type of crime (by passing this legislation Serbia meets the requirements of the Council of Europe Convention on Cybercrime, which establishes minimum standards that it is necessary, in the opinion of the international community to meet by the national legislations in order to combat cyber crime effectively).

The second group consists of substantive regulations that stipulate which actions are socially dangerous behaviors, or that are considered part of the criminal (criminal offense, misdemeanors or civil offense). The main representative of this legislation is the Criminal Code of the Republic of Serbia.[4]

The third group consists of the Criminal Procedure Code,[5] which establishes a procedural framework that provided the mechanism and powers of the public authorities in the processes of discovery, evidence collection, prosecution and trial of offenders of cyber crime.

The basic provisions relating to the area of cyber crime are contained primarily in the General section of the Criminal Code - in the provisions that prescribe the meaning of the term in the sense of criminal law.[6] The terms are parts of the definitions used in the Criminal Code and their meaning is binding, as suggested by the provision of Article 2, Paragraph 2, of the Law on Organization and Jurisdiction of Government Authorities in Fight against Cyber Crime, which stipulates that the terms used herein have the meaning in terms of the provisions of the Criminal Code.

The concept of cyber crime is defined by the Law on Organization and Jurisdiction of Government Authorities in Fight against Cyber Crime as committing criminal acts in which computers, computer networks, and computer data occur as an object or a tool of committing criminal offenses, as well as their products in the material or electronic form.

Positive Criminal Code stipulates criminal offenses related to the field of cyber crime that are stipulated by the earlier laws, but also some new offenses are stipulated (e.g., the offense of unauthorized use of a computer or computer network). Secondly, crimes against intellectual property rights are taken from the Law on Copyright and Related Rights, in which other penalties for economic offense and violation remain.

Without further analysis of individual instances of criminalization, since it is not primarily in the discussion of this kind, we will mention some basic problems occurring here from the perspective of criminal law.

---

3 Official Gazette of the RS, No. 61/05 and 104/09

4 Official Gazette of the RS, No. 85/2005, 88/2005, 107/2005 and Official Gazette of the RS, No. 72/2009, 111/2009 and 121/2012.

5 Official Gazette of the FRY, No.70/2001, 68/2002 and Official Gazette of the RS, No. 58/2004, 85/2005, 115/2005, 49/2007, 20/2009, 72/2009, 72/2011, 101/2011, 121/2012 and 45/2013.

6 It is the meaning of the terms "computer data", "computer network", "computer program" and "computer virus" - items 17-20, Art. 112 of the Legal Code

The basic problem can be detected already in the matters relating to any new form of criminalization, notably the precise definition of a new criminal act. The absolute specificity in this area is the speed of the progress of information technology, which directly affects the subject of protection (for example, the question may be asked: if only the most common forms of information systems deserve legal protection – is it today Web 2.7 or still 2.3?). So far, in fact, we have not been faced with the phenomenon of speed in criminal matters, the fact that subject to the protection falls into the "ancient past" without having been properly understood and treated. From this the issue of perception and recognition of new legal values that need to be defined and protected (e.g., whether it is necessary to protect "virtual identity" against theft, and how to do it?) necessarily follows.

The most important question that arises here is how to coordinate instrumentalized and functional role of criminal law in a permanent change of subject of protection with basic principles, especially the principle of legality. What is the most interesting about this basic principle is precisely the possibility for it to be often threatened by something new and unknown. Namely, by primary definition the offense is the act of a person, but what if the "act" has been objectively made by an automated computer system or machine? (It is amazing that this issue sets the whole story back to the Middle Ages and the responsibility of animals for the criminal offense). The solution that proposes a general clause "internet abuse with criminal intent", its attraction notwithstanding, incorporates the risk of abuse, even the cancellation of right (the principle of legality) in the most direct and roughest terms.

The next principle that is subject to the impact of contemporary trends in the creation of normative framework for new instances of criminalization is the principle of ultima ratio. Conceived precisely as a fence, a barrier against the ever-present idea that the criminal law is the basic and most efficient threat, that it is the essence of criminal efficiency, this principle suggests that the criminal law is the measure of the last resort in the regulation of violation of, and the threat to social order. Tendency to neglect this important principle by converting criminal law to prima or even sola ratio paves the way for lawlessness and turning the normative system into political (Bavcon , 2012, p. 99).

One of the characteristics of IT system is that it contains protection mechanisms (anti-virus programs and anti hacking). However, the question is whether the users should be legally obliged to install the protective programs, and more importantly, whether the failure to fulfill these obligations can be considered a crime (the assumption is that unscrupulous users "help" spread the virus, and to punish would be based on negligence liability). The question is of the utility that as prima ratio a criminal sanction is used instead of civilian (e.g., a fine is more acceptable for a copyright violation).

An essential problem is also the punishment of preparation to commit an offense of this type. In principle, at the level of comparative law the preparatory actions generally are not punishable (the prevailing opinion is that their vagueness and distance from the commission of the offense does not give sufficient quantum of danger to deserve punishment at a general level). In the context of IT crime, however, some jurisdictions (e.g., the German Penal Code provides for a special act software sales designed to facilitate the execution of computer fraud Art. 263a, sec. 3, Serbian Criminal Code, Art. 304a provides punishable creating, obtaining and administering to others other means of committing offenses against the security of computer data) provide for the punishment of preparatory activities, offers or selling (even owning) software designed for committing Internet Crime; (for

example programs for 'cracking passwords'). The rationale is "quantitative" - that the offer of such software on the Internet is a call to millions of potential perpetrators.

In recent years, the literature mentions some remedies for the preventive restriction of committing these types of crimes. The most important are: limiting anonymity, content control and the establishment of common standards.

Limiting anonymity would mean the protection from the almost unlimited possibilities that web communications provide. The identification of offenders would reduce the challenges of easy commitment of these crimes. However, the implementation of these measures is controversial, and often the example of English law is cited, which establishes the obligation of the owner to register the computer password under threat of criminal sanction, which is a measure that compromises some basic human rights, to name just the privilege of unacceptability of self-denunciation. There is an obvious conflict between the concept of need to exclude "privacy" in the case of investigation of serious crimes and all the more obvious perversion of such justification into abuse of the law and naked power.

The next measure refers to the ability to control the content of material distributed via computer network. The list of hazardous contents would thus grow to a list of blocked content. The list itself is long, incoherent and open - from child pornography through the content of inciting religious and racial hatred, passing military and state secrets to the propaganda of proscribed organizations. The problem is in the international nature of the Internet, which frequently is not in compliance with national standards or the interpretation of standards on freedom of speech.

It is obvious that a major problem in the implementation of the proposed measures for preventive action lies in the difficulty of forming general and common standards. If we agree with the undoubted need for sanctions, for example, child pornography does not mean that we have solved the problem of standards in defining the concept and the concept of child, not even the one of possession of "electronic materials". The problem becomes more serious due to the lack of standards of the relationship between the freedom of speech and criminal behavior, as already pointed out.

3.2 Conclusion - The need for the protection of information technology and the need to protect against the misuse of information technologies

The fact is that IT opens up a whole new world of possibilities for crime. Additional fact that the information society is at risk and vulnerable and, as such, stresses the need to redefine the role of criminal law in the prevention and repression of IT crime.

We should start from the standpoint that the law is not what is written on a piece of paper or in electronic form.

The law is somehow a complex, a normative system that incorporates a minimum of moral standards and the protection of basic human rights. Without that, it often turns into abuse of (political) power. In recent years, the classical category of victims who suffer the consequences of the offense is added those who are the victims of abuse of political power (Ramljak, Simovic, 2006, p. 5).

Identifying a new category of victims – the victims of abuse of power has its own history, and can even be considered as one of the results of the struggle for human rights.

Max Weber says that the human rights violation and the abuse of power involve the use of force by all those who have concentrated power. It can be individuals, groups, organizations, corporations, parties, and even the entire system in the sense of the state. It is believed that the rulers are persistent and ruthless in doing that. They do pay attention to the public opinion and are consistent in implementing their will.

The relationship between the concepts of political crime and the abuse of power by the authorities has not been established for too long. Classical theory of criminal law does not deal with the assessment and verification of the legitimacy of the most serious instances of criminalization that threaten, in principle, the external and internal security of the state. The established fiction is that the state is a victim. The effect of this fiction is a non-standard protection of the "victim", which infringes on basic human rights, even on the minimum standard rules of criminal law guaranteed by general norms such as punishable preparation, agreement to commit a criminal offense, and criminal conspiracy (Simovic-Hiber, 1991, 3:10 to 3:22). This ruling idea of the relationship between the state, the government and the governed through legal norms is best explained by a famous French legal theorist: legal qualification used to ensure punishment (Bouzat 1971, Note, br. 16770).

It remains unacknowledged and obscured that essentially somebody else is the victim here. Moving from the idea that the state, law and government is something abstract and good, protected by ideological platitudes and therefore untouchable to the idea of the state as temporary, meaning a variable group of people in power, who are consequently struggling to stay in that position, leads to the demystification of the relationship between the endangered and the victim. This new category of victims of the abuse of power finds its place in the United Nations Declaration of basic Principles of Justice in relation to victims of crime and abuse of power, which is very important.

Why do we think that a warning about the victims of the abuse of political power is relevant to the topic of the paper? We have pointed out repeatedly that the criminal legal protection in the field of cyber crime usually comes down to the technical protection of selected values thus also indirectly becoming legal.

Millennium Resolution, however, warns that the fight against the abuse of computer technology must maintain a balance between individual rights and liberties guaranteed to every individual, on the one hand, and the right of state to prosecute offenders, on the other. The matter of fact is that repressive measures and the restrictions on the certain rights of citizens in relation to criminal prosecution must be restrictive only to the extent necessary to lawfully collect evidence and conduct criminal proceedings before the competent courts.

This is also the subject matter of the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data. The main objective of the adoption of this Convention is precisely to strengthen the legal framework in the field of personal data protection in the light of the dramatic increase in the use of computer technology for administrative purposes. It should be noted that there is increasing power of the secret services due to the lack of judicial and legal control or erosion of the basic rights. The most recent cases (Assange, Manning and Snowden) are the best indicators of such state of affairs.

In this way the assumption comes true that the Internet is a space without rules, but not as we have hoped. Governments have been trying for years now to convince us that the Internet needs more regulations and oversight so as to stand in the way of crime. All the

while, behind our backs, they have been building a monitoring system that is exempt from the rules of the legal state and that has undermined basic democratic rights.

This is exactly the fundamental difference between the police work and the work of the secret services - the police investigation must be preceded by reasonable suspicion. Only then is the limitation of communication allowed. When it comes to secret service spyware, it is precisely the opposite: every internet user is potentially monitored for pattern recognition and potential culprits capturing, with no presumption of innocence. Former CIA Director Leon Panetta summarizes briefly, "to find a needle in a haystack, first we need a stack." In this way, the state declares all citizens suspicious, and even the enemies of the state. We know about the Prism and the Tempora only because we are informed by a whistler exposing to great personal risk. However, Snowden case is not isolated. Based on the law of espionage (Espionage Act) put into effect in 1917, the current U.S. Administration launches twice as many court cases for disclosing state secrets than any government before it together (Leisegang, Blatter, Brave New World of Surveillance, available at http://pescanik.net//2013/07/31). The afore-mentioned dilemmas and addressed issues are certainly not naive, and certainly deserve serious consideration.

REFERENCES

1. Albrecht, H. J., Fijnaut, C., (2002). *The Containment of Transnational Organized Crime,* Freiburg i. Br., Kriminologische Forschungberichte aus dem Max Planck Institut fur auslandisches und internationales Strarecht, Band 108.
2. Bavcon, Lj.(2012). Čovekova sloboda i/ili bezbednost, *Temida,* 2, str.95-104.
3. Bouzat, P., (1971) *Juris classeur penal*, Note, br. 16770.
4. Leisegang, D., *Blatter*, Vrli novi svet nadzora, dostupno na http://pescanik.net//2013/07/31
5. Mannheim, K., Ideologie et Utopie (1929), Maison des sciences de l'homme, 2006.
6. Ramljak, A., Simović, M., (2006) Viktimologija, JUSTITIA, Banja Luka .
7. Salas, D., (2012). La Justice devoyee, (Critique des utopies securitaires), Ed. des Arenes, Paris.
8. Simović-Hiber I., Stadijumi izvršnja krivičnog dela i prednacrt KZ SFRJ, u: Reforma opšteg dela KZ SFRJ i savremene tendencije u jugoslovenskom krivičnom pravu, Institut za kriminološka i sociološka istraživanja, Beograd, 1991, str. 3.10-3.22.
9. Vervaele, J. A. E., Information Society and Criminal Justice, AIDP-IAPL Congress of Penal Law
10. 2014, Introductory note for the discussion in Paris, June, 2011
11. Zapatero, L. A. (2011-2012), The international harmonization of criminal law, *Cahiers de defence sociale,* 25-59.

UDC 726.9:75.041.5
ID 176374796

Zoran Keković, Sandra Vučić
University of Belgrade, Faculty of Security Studies
zorankekovic@yahoo.com
sandra.vucic@gmail.com

Radosav Despotović
NIS, Novi Sad
radosav.despotovic@nis.rs

Nenad Komazec
University of Defence, Military Academy, Belgrade
nkomazec@gmail.com

COMPLIANCE OF EDUCATION PROGRAMS WITH THE NEED OF PROTECTION NATIONAL CRITICAL INFRASTRUCTURE[1]

Abstract: Critical infrastructure is the basis for the functioning of any efficient modern society, which is why that today its protection has been recognized as one of the top priorities of all subjects. Considering that critical infrastructure does not exist or function in an isolated environment, but on the contrary, a security environment in which fundamental processes within the scope of these systems function is more than hostile and insecure, the protection of infrastructure, systems and resources which are vital for a society requires a broad range of knowledge and skills in various fields ranging from industrial safety through risk management, environmental security to the knowledge of the legal and economic subjects. In Serbia, when we speak about critical infrastructure, we usually think of large technical systems (corporations of special importance for defence) and public companies engaged in activities of common interest in the manner specified by the 'Decision on the determination of large technical systems of special importance for defence' (February 2009). This Decision identifies large technical systems of special importance for defence as well as related technical resources central to the functioning of these systems in the field of telecommunications, information technology, transportation, energy and water supply, as well as other areas of importance for defence. Despite the lack of a related Act on the protection of persons, property and business, critical infrastructure protection measures are regulated by a series of laws and regulations. The need to protect critical infrastructure in the modern age has been recognized all over the world, and our country is not an exception in this regard. Therefore, in the recent past, we have witnessed the expansion of educational and training programs at all levels, which aim to empower high quality staff to possess all necessary knowledge and skills in order to be well prepared for responding to the challenges that the modern environment carries. In this paper, we have analyzed higher education programs in Serbia in terms of employers' requirements in relation to the protection of critical infrastructure in order to identify the level of their accordance as well as possible differences in the provision of higher education institutions and employers' needs. In conducting this analysis, we have used the results of a survey completed by the employer in the Oil Industry of Serbia as an analytical framework for critical analysis of higher education. The survey was created to provide a clear overview of the needs of the em-

1 This research is a part of the ongoing project 47017 "Security and Protection of the Organization and Functioning of the Educational system in the Republic of Serbia", funded by the Ministry of Education, Science and Technology Development

ployer in terms of identifying areas of knowledge that are necessary for the protection of critical infrastructure. It enables the categorization of identified areas in terms of assessing the required level of theoretical and practical knowledge for each of these areas. In addition, employers are asked to name four educational institutions which they consider to take a leading role in educating personnel who will be engaged in critical infrastructure protection, and furthermore, to assess for each earlier stipulated institution which areas of knowledge are the best covered by educational programs, and which areas are the least covered by the program. On the basis of these data, we concluded that in our country there are several higher education institutions, which cover different areas of knowledge, important for the performance of critical infrastructure protection. However, the survey demonstrated that none of these institutions offer a complete and comprehensive system of knowledge that would include all the critical areas of knowledge, and thus would be in complete accordance with the requirements of the employer. Therefore, in this paper we have offered several recommendations and proposals whose adoption would be beneficial for improving the quality of higher education programs, in order to ensure that graduate students who will work one day on the protection of critical infrastructure will be able to successfully respond to the high demands of this job.

Keywords: *education, critical infrastructure, areas of knowledge, protection measures*

1. INTRODUCTION

Technological progress as one of the main driving forces of modern, contemporary society has brought many benefits to the humanity and significantly improved the quality of life. In this sense, the century in which we live in, leads in the number and scope of technological changes that reduced the entire expansion of the world to a "global village". Technological development has contributed to "shortening" the distance between the different parts of the world, better and quicker flow of information, people, goods, knowledge and ideas, thus questioning the traditional ideas of time and distance. Interdependence in the form of globalization replaced isolation and focusing on our own strengths and resources and today it permeates almost all aspects and areas of human activity.

Although with no doubt, the advantages of this kind of world order are going far beyond their disadvantages, in some areas of human endeavour this kind of connection and mutual dependence bring serious challenges. Open markets and the free flow of people and information provide fertile ground for the emergence of new challenges, risks and threats, as well as the transformation of traditional threats which now gain international character thus overcoming the borders of national states and therefore the jurisdiction of the national government.

Prediction, assessment and based on that, planning and conducting the protecting measures, became the main preoccupation of almost every country in the world as well as of all serious corporations and companies. As a strategic function of any company that strives for survival and progress, corporate security is organized and implemented on the basis of forecasting the future events, assessing their probability and consequences and, in this regard, defining possible responses to emerging challenges. In this regard, corporate security management has never been more relied on adequate understanding of the threats that company is facing with, given the fact that today there is no business entity that is completely immune to the surprising factors, which was not the case in the past.[2]

However, not all companies are equally threatened by contemporary risks, as well as the consequences of their regular activities disruption do not affect the population and

2 Mishkin, S.F. and Eakins, G.S. (2005). Financial markets and institutions, Zagreb: Mate, str. 380 – 381.

states at the same level. In this sense, when we talk about protecting infrastructure, the emphasis is put on critical infrastructure systems as systems of particular importance for the functioning of modern society. Critical infrastructure protection requires broad participation of corporate management, and sets high demands before those involved in these activities as a result of ongoing changes in the security environment.

2. WHAT IS CRITICAL INFRASTRUCTURE?

Different countries defines critical infrastructure in a different way, but it almost always comes down to the infrastructure, systems and resources that are vital for a society. High interdependence of these systems with other areas of social life requires devoting special attention to its protection.

The importance of critical infrastructure protection is particularly evident after 11 September 2001, when the sudden terrorist attacks on the trade centre, reaffirmed the need for better critical infrastructure protection. This was soon operationalized in the Patriot Act, passed shortly after the attacks, which defines critical infrastructures as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[3]

Germany defines critical infrastructure as "organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences."[4]

The Australian, State and Territory governments define critical infrastructure as "those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security."[5]

In the European Union, critical infrastructure systems usually consider the systems for the production and transmission of electric power, chemical industry, nuclear plants, manufacturing, transportation and distribution of oil and gas, telecommunications systems, drinking water resources, food production, heating systems, public health systems facilities and services, public transportation, government authorities, financial and security institutions. A complete list of critical infrastructure is clearly identified in the European Programme for Critical Infrastructure Protection.[6]

In our country today, there is no critical infrastructure definition in the way there is in the rest of the world. However, even though systems vital for our society are not explicitly

3 The USA Patriot Act (Public Law No. 107-56, Section 1016(e)) available at: http://www.whitehouse.gov/homeland/book/sect3-3.pdf. 21.05.2013. (approached 21.05.2013)

4 National Strategy for Critical Infrastructure Protection (CIP Strategy) of Federal Republic of Germany, available at:http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf, (accessed on 21.05.2013.)

5 Critical infrastructure resilience strategy, available at: http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf, (accessed on 21.05.2013)

6 European Programme for Critical Infrastructure Protection (EPCIP), available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm (accessed on 17.08.2013.)

indicated with the term "critical infrastructure" in the related literature and documents, it would be wrong if we would say that Serbia does not have critical infrastructure defined and that it does not care about its protection. Most public companies engaged in the activities of common interest were declared by Serbian government as large technical systems of interest for the defence, and because of the importance these systems have great attention was paid to their protection.

Thus, the Law on Defence in Chapter 6, concerning the rights and duties of companies, other legal entities and entrepreneurs in the field of defence, defines the products and services of special interest for defense as well as the facilities of particular importance for defence. According to Article 70, paragraph 3 of the Law on Defence (the Official Gazette of the RS, No. 116/07), the Government of the Republic of Serbia adopted the Decision on determination of large technical systems of particular importance for defence which identifies large technical systems important for defence and technical resources of special importance for the functioning of the systems in the field of telecommunications, information technology, transportation, energy, water and other areas. According to this Decision, "large technical systems are considered to be a complete or a set of inter organized parts and procedures that provide technical and technological unity and independence of the system or its functional coherence with other technical systems of particular importance for defence."[7]

Along with this decision, the Government of the Republic of Serbia adopted the Regulation on the facilities and regions of particular importance for national defence. This Regulation defines the areas of particular importance for the defence in the field of transport, telecommunications and communications, energy supply, and other industries.

Beside the legislation in the field of defence, the Law on Public Enterprises in Chapter 2, concerning the definition of the activities of common interest, also indirectly defines critical infrastructure. According to this Law, the activities of general interest are those activities that are determined as such by the law in the following areas: production, transmission and distribution of electricity; production and processing of coal; research, production, processing, transportation and distribution of oil and liquefied natural gas; petroleum transportation; railway, postal and air traffic; telecommunications; publishing of the Official Gazette of the Republic of Serbia; informing; publication of textbooks; utilisation, management, the protection and promotion of public goods (water, roads, mineral resources, forests, waterways rivers, lakes, coasts, spas, game), and public utilities.[8]

3. CORPORATIVE SECURITY STRUCTURE IN TERMS OF CRITICAL INFRASTRUCTURE PROTECTION

By analyzing some of the related definitions of critical infrastructure, we could see that the government plays a key role in defining those systems that will be considered as critical infrastructure systems, as well as in setting up long-term goals to be pursued. Nevertheless, protecting critical infrastructure requires more concrete activities that fall outside the

7 Decision on determination of large technical systems of particular importance for defense, the Official Gazette of the RS, No. 15 of 27 February 2009, 54/10, 4/11, p.1

8 Law on Public Enterprises, the Official Gazette of RS, No. 25/2000, 25/2002, 107/2005, 108/2005 –amend. and 123/2007 – state law)

jurisdiction of the highest state leadership and consider the engagement of a much larger number of subjects at different management levels.

Operationalization of the objectives set out in various legal documents and planning and organizing the specific activities in each of the critical infrastructure system usually falls under the jurisdiction of corporate security management of the company and corporate security in developed countries was recognized as the highest priority of any company that aspires to survival and development. However, when it comes to planning and organizing the protection of critical infrastructure, it is crucial to understand that the protection is not an end by itself, but a means of ensuring the conditions for the prevention of undesirable events and for keeping business continuity in case that such an event occurs. **Thus, instead of putting infrastructure itself as a physical entity, as an object of protection, the supreme goal should be the protection of services they provide.**

Increased awareness about this caused the changes in a way of defining corporate security. According to the group of Croatian authors "Corporate security is a strategic function of the company that aims to provide safety of the business success of the corporation, which includes: elimination of all risks and threats that may affect the business activities and the achievement of business success; reducing threatening effects to a minimum; business continuity in time of crisis, thus overcoming the crisis and resetting normal operations."[9]

Similarly, Milan Milosevic emphasizes an integral character of corporate security, reflected in the fact that it involves performing several different functions that require synchronization. It is a function of the corporation that controls and manages the coordination of all activities within the business entity related to security, continuity and security. An effective system of corporate security protects company from all threatening activities, establishes the basis for making management decisions, and ensures that top management has access to confidential information and forms processes and procedures to prevent fluxion of protected information out of corporations.[10]

Thus, corporate security is part of the company's every day activities. It permeates almost all activities of the organization, regardless of its business area and it aims to eliminate or reduce the possibility of realizing the risks and threats coming from the company itself or from the environment, without interfering with the regular activities of the company with security measures and procedures, and thus create favourable climate for its smooth functioning.

Planning and organizing corporate security in critical infrastructure systems is a complex and responsible job, because of their importance for the functioning of the whole society, as well as because of the wide range of causes that can cause crisis in these systems and disturb company's ordinary activities performance.

When we talk about the causes of the crises that may affect the company, Professor Kekovic and Professor Kesetovic distinguish two groups of factors. The first group consists of the external factors that operate in the company's environment and on which the company does not have much impact. Such factors are, for example, the global economic crisis,

9 Ivandić Vidović, D., Karlović L.i Ostojič A. (2011). Corporate security, cited according to Trivan, D. (2012). Corporate security, Dosije studio, Belgrade, p.81

10 Milosevic, M. (2010). The concept and content of corporate security, cited according to Trivan, D. (2012). Corporate security, Dosije studio, Belgrade, p. 82

political disorder, changes in global market, legal changes, and natural disasters. The second group of factors consists of the internal factors which exist within the company and they usually include inadequate capacity, incompetence and immorality of the top management, underestimating public opinion and subordination, ineffective performance of managerial functions, frustration and the lack of motivation of employees, poor performance of corporate security system, poor organization and inadequate job creation and operation of internal informal groups, weak organizational culture, unrealistic goals and requirements, poor communication system, unregulated social relations at work.[11]

A map of the risks which is created this way, clearly leads to the conclusion that corporate security does not include only physical and technical protection of the system, but a series of sophisticated, sometimes hardly tangible and measurable activities that are carried out in order to control even those risks which go beyond the frames of the traditional concept of security.

Therefore, as the core functions of corporate security harmonized by several countries, we can most often find: administrative security, physical and technical security, security of property and external partners security, personal safety, fire safety, performing in case of emergency, information security, manager's security, security of various business events, security of business contracts with the government, investigation, education programs and the development of safety culture employees.[12]

Comprehensive approach to the security of critical infrastructure systems, besides creating the conditions for the operation of the specific company in a favourable and safe business environment, at the same time, it increases the immunity against the so-called domino effect, caused by high interdependence of various systems of critical infrastructure. Everything stipulated earlier leads to the problem related to structure and organization of the organizational unit that deals with corporate security and within it, the division of specific authorizations and responsibilities. As in most other activities, there is no doubt that for successful performance in the field of corporate security, human factor is essential, but at the same time the most critical factor. Competence or incompetence of the managerial as well as operational staff engaged in these activities determines the success or failure of the pre-defined objectives. That is why in the following sections we will try to examine this issue on a theoretical level, and then we will consider the situation in practice.

4. COMPETENCES OF MANAGERIAL AND OPERATIONAL STUFF IN TERMS OF CRITICAL INFRASTRUCTURE PROTECTION

The complexity of the system of critical infrastructure, as well as their high vulnerability to various types of undesirable events, necessarily imposes the need to take serious and comprehensive approach when it comes to their protection.

The organization of corporate security includes a number of elements that include the assessment of current risks, the causes and forms of endangering persons, property and operations of the system, defining the authorities and responsibilities of those engaged in protection of the vital values of the critical infrastructure, the organization and operation of physical and technical security, undertaking protection measures relating to health and

11 Kesetovic Z., Kekovic, Z. (2008). Systems of crisis management, Banja Luka, Faculty of Security and Protection, p. 23

12 Trivan, D. (2012). Corporate security, Dosije studio, Belgrade, p. 87

safety at work, environmental protection, the measures for protecting corporation against all forms of corruption, various forms of abuse, embezzlement, fraud, and other methods of disposal of assets, defining measures for classified data protection, defining measures for controlling moving and residence of foreign persons in facilities, the operation of information systems in the security of persons, property and business, harmonization of normative acts, as well as evaluating the vulnerability of those engaged in the protection of company's essential values.[13] Working on these activities, usually requires the involvement of large number of people, therefore the organization of corporate security and the organizational structure of the unit engaged in these activities varies from system to system.

Today, all around the world as well as in our country, there is a growing number of subjects who are professionally engaged in different fields of security, independently of state security structures. As a result, in the last few years, we have witnessed an increased popularization of security manager profession. But, when we speak about corporate security in terms of critical infrastructure protection, we can see that the frame of these activities is usually unjustifiably reduced to the activities related to physical and technical security, thereby leaving aside an entire range of activities that can equally disrupt the regular functioning of the critical infrastructure system. As the basic tasks put before the security manager, a group of authors number security strategy development, risk identification and risk analysis, risk assessment and evaluation, policy, program and security procedures, technology and infrastructure protection, information risk management, business continuity management, crisis management and response to crisis, raising employee awareness of the risks, the activities related to work safety, a survey of business operation and its compliance with laws, the protection of corporation's management, intelligence and counter-intelligence operations in the area of operation, the authentication of the information received from the corporation sources, forensic and investigative services as well as the protection of documents.[14]

Performing these tasks requires not only a certain degree, but also many other skills that a successful security manager should poses. A wide range of theoretical knowledge must be completed by relevant work experience, leadership and managerial skills, the ability to act and make decisions under pressure and stress, and high moral and character traits and integrity.

Due to increasing interest in the security profession, but also because of the great responsibility and seriousness that this profession entails, huge efforts were put in framing body of knowledge that anyone who deals with security issues should possess. Different authors dealing with this issue emphasize that making consensus regarding the creation of the fund-rounded knowledge is essential for several reasons, primarily because it creates the conditions for defining the security standards, competences and qualifications, providing education and certification of security experts. However, knowledge is "more than written scientific facts and theories".[15] Knowledge may be defined as "facts or experiences known

13 Barney J., Hesterly S.W. (2005). Strategic Management and Competitive Advantage, Prentice Hall, London, p. 432-435

14 Ivandić Vidović, D., Karlović L., Ostojič A. (2011). Corporate security, cited according to Trivan, D. (2012). Corporate security, Dosije studio, Belgrade, p. 128

15 Clancey, W. J. (1997). The conceptual nature of knowledge, situations and activity, str.285. u P. J. Feltovich, K. M. Ford, & R. R. Hoffman, Expertise in context: Human and machine (pp. 247-291). Menlo Park, CA: The MIT

by a person or group of people ... specific information about a subject".[16] Knowledge is constructed and, built on previous experience by, using and expanding the existing ideas.[17] Concerning that security managers are often in a position to make difficult decisions usually connected with certain level of risk, the knowledge acquired through experience, continuous learning and improvement is essential for the proper understanding of the situation, predicting future developments and making decisions.

Besides managerial staff, equal attention should be paid to the employees at lower levels of the hierarchy, because only through shared and synchronized actions of all stakeholders, the negative consequences of adverse events that could disrupt the normal functioning of critical infrastructure, and thus affect the normal operation of the entire society that relies on these systems, can be prevented or suppressed.

5. COMPETENCES OF MANAGERIAL AND OPERATIONAL STUFF IN TERMS OF CRITICAL INFRASTRUCTURE PROTECTION – PRACTICAL NEEDS

The need for critical infrastructure protection was recognized in large number of countries all over the world, and our country is not an exception when it comes to this issue. That is why in the last few years, we have witnessed an expansion of different levels of educational and training programs in the field of security, which aim to empower a high-quality stuff equipped with the knowledge and skills necessary to deal with different challenges in the security environment. However, an increasing number of courses and study programs dealing with security issues, does not necessarily lead to an improved quality of education, as well as an increasing number of "experts" for security does not mean that human factor in critical infrastructure protection was improved and brought to a higher level.

At the same time, educational programs often find themselves in discrepancy with the actual needs of the companies or with the practical requirements. In order to verify the extent to which there is compliance between the education for security affairs and the needs of the employers in this field, we have carried out research in one of the system of critical infrastructure - Oil Industry of Serbia. The research involved the employees in different positions in security sector in Oil Industry of Serbia. The sample consisted of 33 respondents from the Oil Refinery Pancevo and Oil Refinery Novi Sad.

After the data processing we came to the conclusion that none of the currently existing educational programs fully meets the needs of the employers in the area of critical infrastructure protection. As leading institutions in our country when it comes to the education of professionals in this area, the respondents identified the Faculty of Security Studies, The Academy of Criminalistic and Police Studies, the Military Academy and the Faculty of Law (Figure 1).

Press

16 Roberston. (1992). Dictionary and thesaurus. Sydney: Harper Collins Publishers, p.552

17 Novak, J. D., & Gowin, D. B. (1984). Learning how to learn. Cambridge: Cambridge University Press.,



Figure 1: Leading institutions in our country when it comes to education for Critical infrastructure protection

Despite the long tradition that these institutions undoubtedly have in providing education for the personnel in the field of security and defence, the respondents are of the opinion that each of them is specialized for some of the areas, but none of them provides the full range of skills required for successful performance of critical infrastructure protection.

However, as we could see from Figure 1, most of the respondents recognized the Faculty of Security Studies as an institution that mostly covers the most important areas when it comes to critical infrastructure protection. Estimating from 1 to 5 the extent to which the above-mentioned institutions' study programs cover the relevant areas of critical infrastructure protection, the respondents felt that the Faculty of Security Studies includes most of the important areas (total 4,033), followed up by the Military Academy (3.93), then The Academy of Criminalistic and Police Studies and the Faculty of Law (Figure 2).

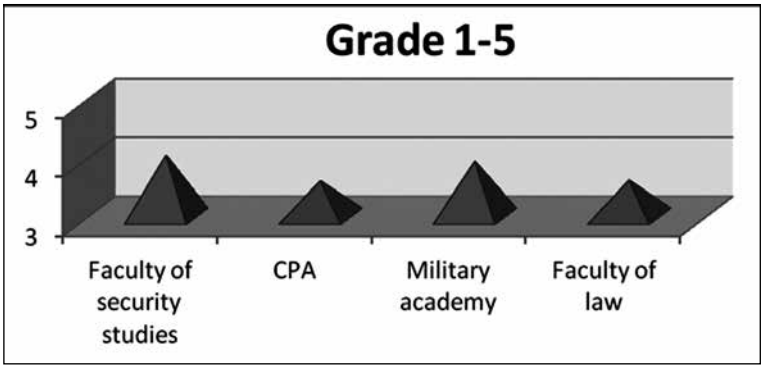


Figure 2: Comprehensiveness of study programs in terms of including all relevant areas for the critical infrastructure protection

According to the respondents, each of the faculties covers specific areas of importance for the protection of critical infrastructure. Figure 3 shows specialization areas distribution among these per institutions respectively.

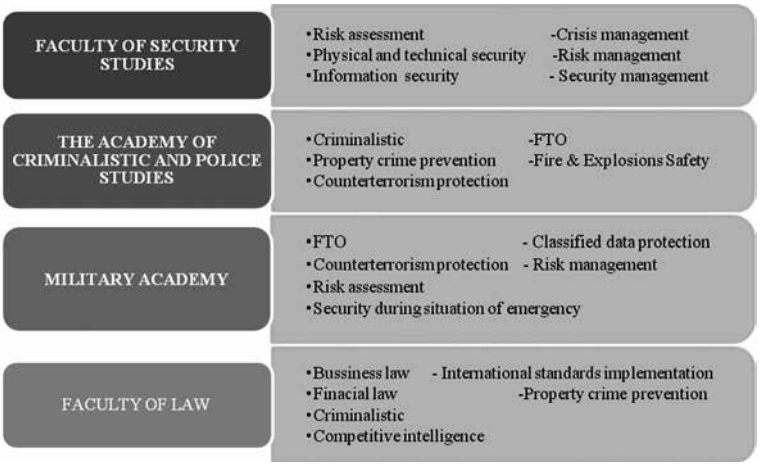


Figure3: Specialization areas distribution mostly covered by the study programs of the above-mentioned institutions

As we have stipulated earlier, this study aims to examine the level of harmonization among the education and the practical needs of critical infrastructure protection. The research results summarized above necessarily lead to the conclusion that there is a large discrepancy between the knowledge that universities offer in this area and the real needs posed by critical infrastructure systems in terms of their protection. That is why, based on the defined needs of the employees in OIS as well as their experience in performing the tasks related to critical infrastructure protection, we have tried to come up with the framed body of knowledge which will consist of the areas of the highest importance when it comes to this issue.

The following diagram shows a group of 21areas of security knowledge identified by the employees in the security sector in the Oil Industry of Serbia, which according to their opinion presents a prerequisite for the successful performance of critical infrastructure protection.

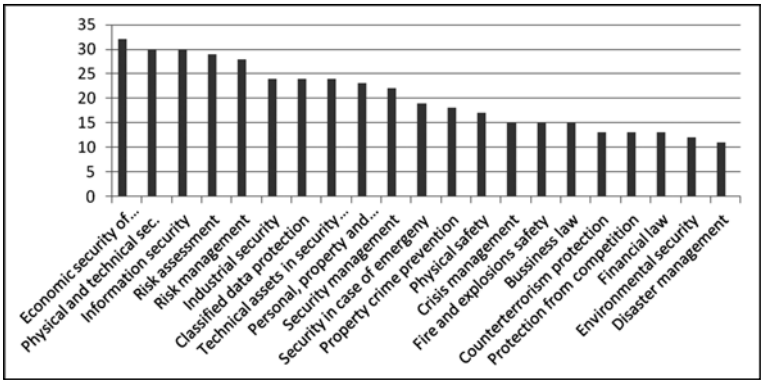


Figure 4: A Framework of necessary knowledge for the protection of critical infrastructure

From this figure, we can see that several categories occupy an identical position. In order to gain a better insight into the level of necessary theoretical and practical knowledge for each category, the respondents were asked to rate each area from 1 to 5 in terms of the necessary theoretical and practical knowledge. By taking the average of each area, we got the following results:

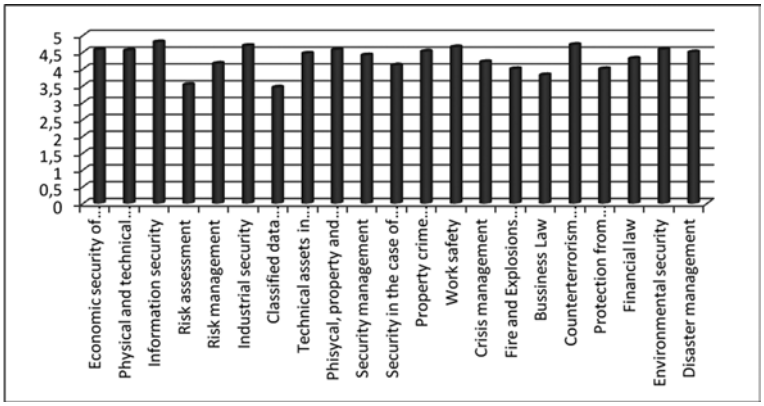


Figure 5: The level of necessary theoretical and practical knowledge for each category

Figure 5 shows that, according to the respondents, successful dealing with critical infrastructure protection requires the knowledge from the following areas: information security, counterterrorism protection, industrial security, work safety, environmental security, economic security of business, physical and technical security and disaster management, technical assets in security systems, security management and financial law.

What we have found interesting is the fact, that those areas which were identified as the most important for critical infrastructure protection are at the same time, according to the respondents' opinion the least covered by the study programs of the above-mentioned faculties.

Thus, according to the research results, the respondents think that there is the lack of knowledge in economic security of business, information security, industrial security, technical assets in security systems and classified data protection.

Besides, responding to the question whether they think that in addition to the studies, conducting additional courses and trainings would be useful for improving student's competences in this field, 27 respondents answered affirmatively, 3 negatively, and 3 respondents were sustained (Figure 6).

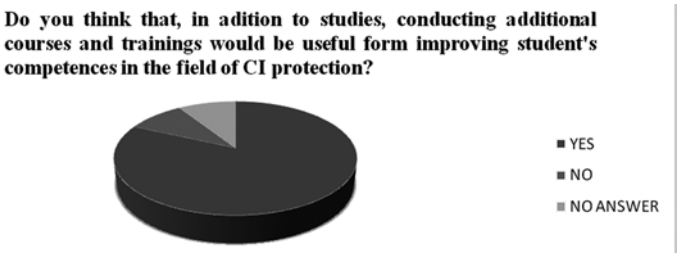


Figure 6: The need for conducting additional trainings and courses

Respondents think that conducting courses in the field of information security, risk management, protecting business continuity would be very useful and it would significantly improve the competences of the future employees on critical infrastructure protection. They also think that organizing courses which would aim to empower the employees for conducting verifications, assessments and analyses of corporate subjects, as well as authentications of partner companies. The lack of practical experience during the studies and insufficient following of the world trends, when it comes to personal, property or business security and protection were identified as the biggest limitation. In this context, they think that conducting educational courses about new trends in this field would be of great importance for better and more effective critical infrastructure protection whose significance for normal functioning of modern society is priceless.

If we would try to compare the derived results with the condition in other countries in the region, we would see that our country is more or less, at the same level in relation to conceptualizing and organizing corporate security in terms of critical infrastructure protection. In our country, as well as in other countries from the region, corporate security is not at the same level as it is the case in more developed countries, and the main reason for that is the lack of high-quality professionals in this field. Thus, for example in Croatia and Macedonia, the activities related to critical infrastructure protection are usually conducted by former police and military officers who do not have specific knowledge in this area. That is why all countries from the region are actively involved in professionalization of the personnel engaged in critical infrastructure protection, and the exchange of experience, knowledge and good praxis is of essential importance for achieving the success in this goal.

INSTEAD OF A CONCLUSION

Great importance of critical infrastructure systems in the contemporary world necessarily imposes high standards when it comes to their protection. The variability of threats and high vulnerability of CI systems on technological innovations abuses, as well as the usage of technological innovations for conducting malicious attack on CI systems, requires involving the highest-quality professionals who will work on their protection.

Critical infrastructure protection is usually under the state jurisdiction and state itself is responsible for the achieved level of protection. Our country is highly independent in planning, organizing and conducting critical infrastructure protection, and the consequences of failure to achieve that are usually limited to the territory inside the national borders. Nevertheless, since Serbia recently became a candidate for the EU, a need for harmonization of critical infrastructure protection with the European programs for critical infrastructure protection will for sure soon come to the agenda.

This program implies creating a few levels of critical infrastructure protection, starting with creating the Action Plan for critical infrastructure protection, then building the Critical Infrastructure Warning Information Network, creating expert groups, organizing CIP information sharing process, and identification of interdependencies.

However, member states still remain the most responsible for the protection of critical infrastructure on their respective territories. As a future EU member, our country will be faced with a number of challenges and requirements in terms of providing better protection of critical infrastructure system which can be achieved only through increased quality of subjects engaged in its protection.

This research indicated a huge gap between the education and the existing needs for protection, which can be overcome only through conducting serious steps aimed to reduce and eliminate this gap. As a long term goal, we should set up an improvement of the educational programs for critical infrastructure protection, and as a result it would significantly improve the competences of the future leaders and others engaged in these activities.

In order to achieve this goal and based on our research result, we think that including new knowledge areas which were identified in this research as important for CIP would be beneficial for future education in this area. On the top of that, since the research also demonstrated that there is a lot of space for improvement in the categories of knowledge which are already covered by the study programs, we think that more efforts should be put in the modernization of the existing approaches through including foreign experiences and following the trends in the developed countries.

We also highly recommend creating specialist curriculum in the field of critical infrastructure protection, created and organized in the way to completely meet the needs of the necessary protection of critical infrastructure systems.

Continuing education along with keeping up with the existing trends in critical infrastructure protection will significantly reduce the vulnerability of these systems and create conditions for the development and progress of society in all areas of life.

REFERENCES

1. Angus & Roberston. (1992). Dictionary and thesaurus. Sydney: Harper Collins Publishers;
2. Barney J., Hesterly S.W. (2005). Strategic Management and Competitive Advantage, Prentice Hall, London;
3. Feltovich P. J , Ford K. M., & Hoffman R. R. , Expertise in context: Human and machine Menlo Park, CA: The MIT Press;
4. Kesetović Z. i Kekovic, Z. (2008). Systems of crisis management, Banja Luka, Faculty of security and protection;
5. Mishkin, S.F. and Eakins, G.S. (2005). Financial markets and institutions, Zagreb: Mate;
6. Novak, J. D., & Gowin, D. B. (1984). *Learning how to learn.* Cambridge: Cambridge University Press.;
7. Roberston. (1992). Dictionary and thesaurus. Sydney: Harper Collins Publishers;
8. Trivan, D. (2012): Corporate security, Dosije studio, Belgrade;

DOCUMENTS:

1. Critical infrastructure resilience strategy, available at: http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf, (approached 21.05.2013)
2. European Programme for Critical Infrastructure Protection (EPCIP), available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm
3. The USA Patriot Act (Public Law No.107-56, Section 1016(e)) available at: http://www.whitehouse.gov/homeland/book/sect3-3.pdf. 21.05.2013.
4. National Strategy for Critical Infrastructure Protection (CIP Strategy) of Federal Republic of Germany, available at: http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pf,
5. Decision on determination of large technical systems of particular importance for defence, the Official Gazette of the RS, No. 15 of 27 February 2009, 54/10, 4/11;
6. Law on Public Enterprises, the Official Gazette of the RS, No. 25/2000, 25/2002, 107/2005, 108/2005 –amend. and 123/2007 – state law)

SECTION III

RISK AND CRISIS MANAGEMENT APPROACHES

UDC 726.9:75.041.5
ID 176374796

Nasir Hussain
Strategy Foresight LLP, London
hussain@strategyforesight.org

USING GENERAL MORPHOLOGICAL ANALYSIS FOR DEVELOPING SCENARIOS AND STRATEGIES FOR EMERGENCY PREPAREDNESS IN CRITICAL INFRASTRUCTURE PROTECTION

Abstract: Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy and include energy generation, transmission and distribution, telecommunications, public health, transportation systems, food production/distribution, financial and security services. Depending on the nature of the business, large corporations have plans for a subset of these critical infrastructure systems. The above is underpinned by the European Programme for Critical Infrastructure Protection, which is laid out in various EU Directives by the Commission. In the UK, the Centre for the Protection of National Infrastructure provides information, personnel and physical security advice to the businesses and organisations which make up the UK's national infrastructure, helping to reduce its vulnerability to terrorism and other threats. This can call on resources from other government departments and agencies, including MI5, the Communications Electronics Security Group and other Government departments responsible for national infrastructure.

Modelling such complex socio-technical systems and threat scenarios presents us with a number of difficultmethodological problems. Many of the factors involved are not readily quantifiable, and one is faced with both antagonistic and non-specified uncertainties. General Morphological analysis (GMA), pioneered by the eminent astrophysicist, Fritz Zwicky in the 1930s and 40s, is a method for investigating the totality of relationships contained inmulti-dimensional, non-quantifiable problem complexes. Since 1995, The Swedish Defence Research Agency, have extended, computerised and applied GMA in a variety of areas such as critical infrastructure system protection, developing both novel scenarios and associated strategies for emergency preparedness. This article outlines the fundamentals of the morphological approach and describesrecent applications in modelling threat scenarios and revised preparedness planning in a number of areas.In this article, we will describe:

1. How morphological analytical models are constructed to give decision support in complex, difficult-to-quantify subject matter;
2. A case study,demonstrating the generation of possiblethreat scenarios and attendant strategies in the nuclear energy sector;
3. How a consensual platform is developed between stakeholders of widely differing positions to analyse the entire problem space and then synthesise a smaller subset of internally consistent solutions;
4. A proprietary software instrument for communicating complex issues to people of varying backgroundsviaa user-friendly graphical program;

5. The potential for collaborationbetween industry, government and academics for tackling intractable worldly problems characterised by over population and diminishing resources that are leading to accidental or deliberate systems failure.

Keywords: *Disaster preparedness, General Morphological Analysis, Uncertainty mitigation, Problem structuring methods, Business contingency planning, Business resumption strategies*

INTRODUCTION

1.0. Current thinking on critical infrastructure systems and protection

Critical-infrastructure protection is the study, design and implementation of precautionary measures aimed to reduce the risk that critical infrastructure fails as the result of war, disaster, civil unrest, vandalism, or sabotage. A modelling environment must be able to weave science, technology, law and policy to craft sophisticated yet practical solutions for securing assets in the various critical infrastructure sectors. These critical infrastructure sectors include: information technology, telecommunications, energy, banking and finance, transportation systems, chemicals, critical manufacturing, agriculture and food, public health and health care, drinking water and water treatment systems, commercial facilities, dams, emergency services, nuclear reactors, materials and waste, postal and shipping, and government facilities. Protecting and ensuring the continuity of operation of critical infrastructure assets are vital to national security, public health and safety, economic vitality, and societal wellbeing (International Journal of Critical Infrastructure Protection, 2013).

In analysing the security challenges that are unique or common to the various infrastructure sectors mentioned above, it is vital to identify the core security principles, possible scenarios and attendant response strategies that can be applied to critical infrastructure protection. This requires elucidation of the dependencies and interdependencies existing between infrastructure sectors and techniques for mitigating the devastating effects of cascading failures. Therefore, the creation of sophisticated, yet practical, solutions, for critical infrastructure protection are required, which involves the interrelation and collaboration of a variety of disciplines emanating from the mathematical and social science domains.

However, structuring and analysing complex socio-technical systemspresents us with a number of difficult methodologicalproblems. Firstly, many of the factors involved are notmeaningfully quantifiable, since they contain strong social,political and cognitive dimensions. Secondly, the uncertainties inherent in such problem complexes are in principle non-reducible, and often cannot be fully described or delineated.This includes both so-called agonistic uncertainty (conscious, reflective actions among competing actors) and non-specified uncertainty (for instance, uncertainties concerningwhat types of scientific and technological discoveries will bemade in the future).Added to this, the extreme nonlinearity of social systemsmeans that literally everything is connected to everythingelse. What might seem to be the most marginal of factors can, under the right circumstances, becomea dominating force ofchange. All of this means thattraditional quantitative methods, mathematical (functional)modelling[1] and simulation alone will simply not suffice (Ritchey, 2006).

1 Such family of methods are known as (Hard) operational research, which originated in Britain during World War II when it was used to apply mathematical techniques to the planning of military operations. Since then it has become recognised as an important input to decision-making in business, industry and government.

To counteract this deficiency, Problem structuring methods, also known as 'Soft' Operational Research, were developed from the 60's mainly in Britain, being almost completely matured in the 80's. Many problems in the management of critical infrastructure protection are too "messy" to be addressed effectively by the standard management scientist's toolkit of mathematically-based techniques. Such problems are typically characterised by complexity, a high degree of uncertainty given the lack of information, and multiple subjectivity (different worldviews, the Weltanschauung, of stakeholders of the problem complex). Structuring them into a form in which they can be addressed is at least as challenging as formally solving them. These methods are generally designed for use in the context of workshops in which the problem owners are central participants, and tend to emphasise qualitative rather than quantitative content. One such method of Swiss-American origin, General Morphological Analysis (GMA), is the subject of this paper. Since the mid-1990s, GMA has been extensivelycomputerized and extended for structuring and analysing complex policy spaces, developing futures scenarios andmodelling strategy alternatives.

Relevant projects where GMA has been used in the critical infrastructure protection area are listed in Table 1. A case study[2] is presented here to describe the methodology, which has seen a renaissance since the mid-90s due to the development of small, fast computers and flexible graphic interfaces capable of structuring and synthesising vast number of configurations and the ability to develop interlinked scenario-strategy duplex models.

Table 1: Selected project list (out of 130 projects) where GMA has been used in the areas of Critical Infrastructure and related projects

Project	**Client**
Scenarios and Strategies for Energy Security	Ministry of Energy - Singapore
Modelling climate change conflict scenarios	Swedish Defence Research Agency
The various structures of economic crime, their cross-links and counter-measures	National Agency on Economic Crime and the National Police Board
Dependencies between Critical Transport Systems in Time of Crisis	Swedish Emergency Management Agency
Futures Projections and Strategic Alternatives for Causality Insurance	Länsförsäkringar - Swedish Insurance Company
Future research areas in societal risk management	Swedish Defence Research Agency
Modelling future land use and food security	Swedish Agriculture Federation
Anonymous communication over the internet	Swedish Ministry of Justice
Evaluation of new techno-innovative systems	Swedish Armed Forces
Design basis model and evaluation instrument for national crisis management	Swedish National Emergency Management Agency

2 This work has been presented and published at the 44th by Dr Tom Ritchey and colleagues at Annual Meeting of the Institute of Nuclear Materials Management - Phoenix, Arizona, July 2003

European political and security scenarios	StiftungWissenschaft und Politik - Ebenhausen
Societal disruption and strategies for financial stability	Swedish Ministry of Finance
Modelling multi-hazard disaster reduction strategies	Earthquake Disaster Mitigation Research Center, Kobe

2.0. PRINCIPLE OF GENERAL MORPHOLOGICAL ANALYSIS

General morphological analysis is a method for structuring and investigating the total set of relationships contained in multidimensional, usually non-quantifiable, problem complexes. Pioneered by Fritz Zwicky at the California Institute of Technology in the 1930s and 1940s, it relies on a constructed parameter space, linked by way of logical relationships, rather than on causal relationships and a hierarchal structure.

The process of GMA is composed of two principal steps – an analysis phase to map out the entire problem space as defined/constructed by specialists in the field, and the synthesis phase where configurations in the multi-dimensional space are selected. Before going into the detailed explanation of the process of building complex multi-dimensional morphological fields for decision support, a short, simple explanation is required.

Figure 1a[3] shows a problem that has three variables – price, promotional method and product type. This can be represented in the form of a cube, which itself can be re-formatted as a 2-dimensional typological matrix as depicted in Figure 1b.

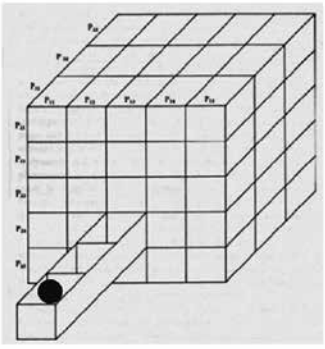


Figure 1a: 3-parameter "Zwicky Box" in typological format, containing 75 (5x5x3) cells (Zwicky, 1969).

Parameter 1	Parameter 2	Parameter 3
P1.1	P2.1	P3.1
P1.2	P2.2	P3.2
P1.3	P2.3	P3.3
P1.4	P2.4	
P1.5	P2.5	

Figure 1b: 3-parameter field in morphological format. (The blue configuration corresponds to the blue marked cell in Figure 1a.)

Very complex problems, however, consist of a multitude of variables that in Cartesian display cannot be depicted easily as visually a typology utilizes the dimensions of physical space to represent its variables, which ends at 3. There are, however, other ways to represent - and visualize - hyperspaces; in GMA this is simply done by placing the 4^{th}, 5^{th} ...n^{th} variable as parallel columns. Figure 2 displays a7-dimensional morphological field in which one configuration out of a possible 186,624 is shown (in blue). This is *not to* be read as a table as

3 From www.swemorph.com

the configuration shown in blue is actually a single point in a seven dimensional universe (a point in a multi-dimensional space is represented as a path cutting each axis at the appropriate value). This type of representation becomes of particular value in wicked problems[4] that pervade the critical infrastructure protection space as there are invariably multi-dimensional, multi-layered sets of issues of qualitative nature that cannot be meaningfully quantified and where one needs to think about multiple problems at once. Furthermore, one needs to remain focused on the desired outcome (i.e., the focus question) and keep an audit trail of how the possible solutions are derived (more on this later).

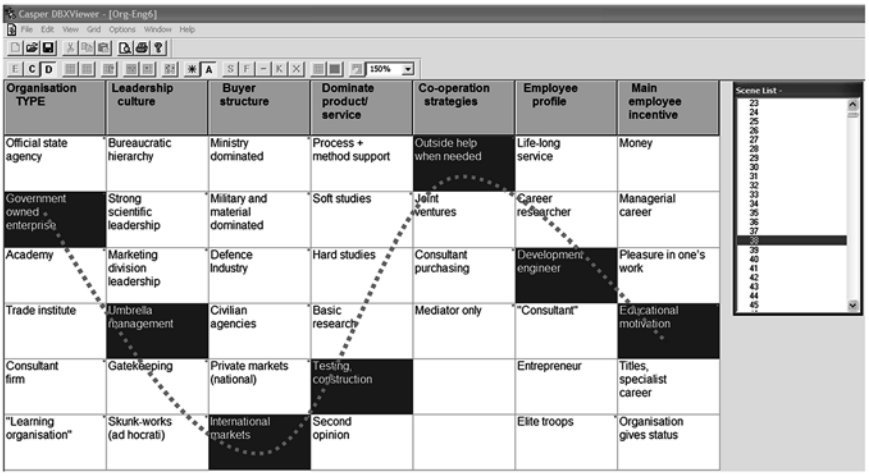


Figure 2: A 7-dimensional morphological field for the possible transformation of an official state agency to alternative organisational structure where the type of leadership culture, employee profile, their incentives, etc. is only compatible in certain situations.

To fully explain the process of morphology in giving decision support to complex issues, the following section will describe in detail how morphological fields are constructed using an actual project where GMA was used to derive possible threat scenariosfor theprotection against sabotage of nuclear facilities for the Swedish Nuclear Power Inspectorate.

4 Wicked problems, a termed coined by Rittel and Webber (1974). Wicked problems are ill-defined, ambiguous and associated with strong moral, political and professional issues. Since they are strongly stakeholder dependent, there is often little consensus about what the problem is, let alone how to resolve it. Furthermore, wicked problems won't keep still: they are sets of complex, interacting issues evolving in a dynamic social context. Often, new forms of wicked problems emerge as a result of trying to understand and solve one of them. Tackling such 'messes' requires the use of problem structuring methods, such as GMA.

3.0. PROTECTION AGAINST SABOTAGE OF NUCLEAR FACILITIES: USING MORPHOLOGICAL ANALYSIS IN REVISING THE DESIGN BASIS THREAT

3.1. Background

The Swedish Nuclear Power Inspectorate (SKI) is the regulatory authority for nuclear activities in Sweden. Its responsibilities include nuclear safety and security issues. Since the middle of the 1970's, in the area of physical protection against theft of nuclear material and sabotage of nuclear facilities, SKI has applied the concept of Design Basis Threat (DBT). The DBT has repeatedly been reviewed over the years. For this purpose, SKI employed traditional assessment methods in association with other relevant national authorities. The DBT formed the basis for SKI in developing regulations on physical protection of nuclear material and nuclear facilities. Moreover, the DBT has been an important input for operators when designing their respective measures for physical protection.

In the late 1990's, SKI decided to modernise its regulations in general, including the regulations on physical protection. This was to better reflect the new supervisory policy of SKI and to make the regulations more transparent. The starting point for revising these regulations was to make a thorough review of the existing DBT. This task wasalmost finalised in August 2001 – then came September 11th, 2001.

3.2. Developing the morphological field for SKI

SKI co-operates closely with other relevant national authorities when defining or revising the DBT. For this project, a multi-disciplinary working group was established with experts from the following areas:

- Nuclear security/physical protection
- Nuclear safety
- Nuclear systems engineering
- International terrorism
- Counter terrorism
- Security policy

Two senior morphologists from FOI supported the working group of 6-8 subject specialists.

The GMA process itself was supported by the software developed by FOI – CARMA® (Computer Aided Resource for Morphological Analysis). The software supports the entire analysis-synthesis cycle which GMA involves.

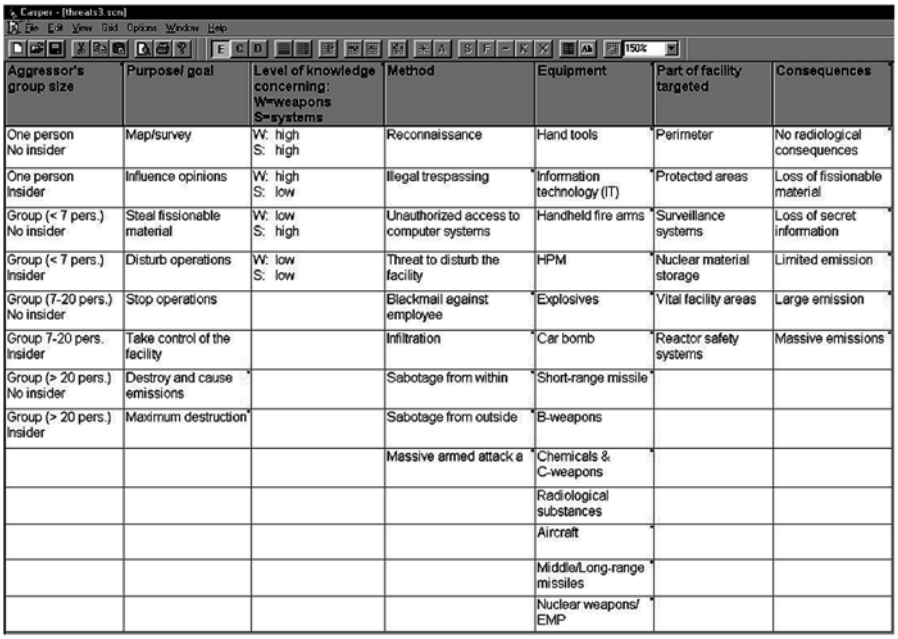
Analysis Phase:

The first step was to identify the variables (i.e., column headings) that defined the threat scenarios relevant for nuclear facilities, e.g. nuclear power reactors. After much deliberation, the workshop group was facilitated to come up with the following parameters or variables:

- Aggressors group size and insider status: i.e., the number of adversaries directly involved in an attack on a nuclear facility and whether there is an insider involved
- Purpose: i.e., the purpose of an attack on a nuclear facility
- Level of knowledge: the aggressors' level of knowledge concerning equipment and weapons that are used and the process, safety and security systems in the targeted facility

- Method: the method used to support the goal
- Equipment: the equipment and/or weapons used to support the method and goal
- Part of facility targeted: the different parts of the facility that is subject to an attack
- Consequences: the possible consequences of an attack

The next step was to define a range of values or conditions for each variable. The variable and variable-condition matrix is the morphological field (Figure 3), which implicitly contains the solution space for the problem complex. However the matrix now contained 1,078,272 theoretically possible threat scenarios (derived by multiplying the conditions under each variable).



Aggressor's group size	Purpose/ goal	Level of knowledge concerning: W=weapons S=systems	Method	Equipment	Part of facility targeted	Consequences
One person No insider	Map/survey	W: high S: high	Reconnaissance	Hand tools	Perimeter	No radiological consequences
One person Insider	Influence opinions	W: high S: low	Illegal trespassing	Information technology (IT)	Protected areas	Loss of fissionable material
Group (< 7 pers.) No insider	Steal fissionable material	W: low S: high	Unauthorized access to computer systems	Handheld fire arms	Surveillance systems	Loss of secret information
Group (< 7 pers.) Insider	Disturb operations	W: low S: low	Threat to disturb the facility	HPM	Nuclear material storage	Limited emission
Group (7-20 pers.) No insider	Stop operations		Blackmail against employee	Explosives	Vital facility areas	Large emission
Group 7-20 pers. Insider	Take control of the facility		Infiltration	Car bomb	Reactor safety systems	Massive emissions
Group (> 20 pers.) No insider	Destroy and cause emissions		Sabotage from within	Short-range missile		
Group (> 20 pers.) Insider	Maximum destruction		Sabotage from outside	B-weapons		
			Massive armed attack a	Chemicals & C-weapons		
				Radiological substances		
				Aircraft		
				Middle/Long-range missiles		
				Nuclear weapons/ EMP		

Figure 3 shows a threat scenario field developed in the study, containing seven variables. For reasons of confidentiality, some of the variable conditions have been modified.

Synthesis phase: The solution space is synthesised by excluding logically impossible and empirical improbable pair-wise combinations of the conditions (denoted by x). This is greatly facilitated by re-formatting or pivoting the morphological field into a form of a cross compact analysis matrix as shown in Figure 4. Any *incompatible* pair 'knocks out' the entire configuration that contains that pair using Cross-Consistency Assessment process (CCA). Here the workshop team is facilitated in a rigorous discussion to consider the binary of assessment whether each pair of cells (conditions)is compatible (-) or not (x).

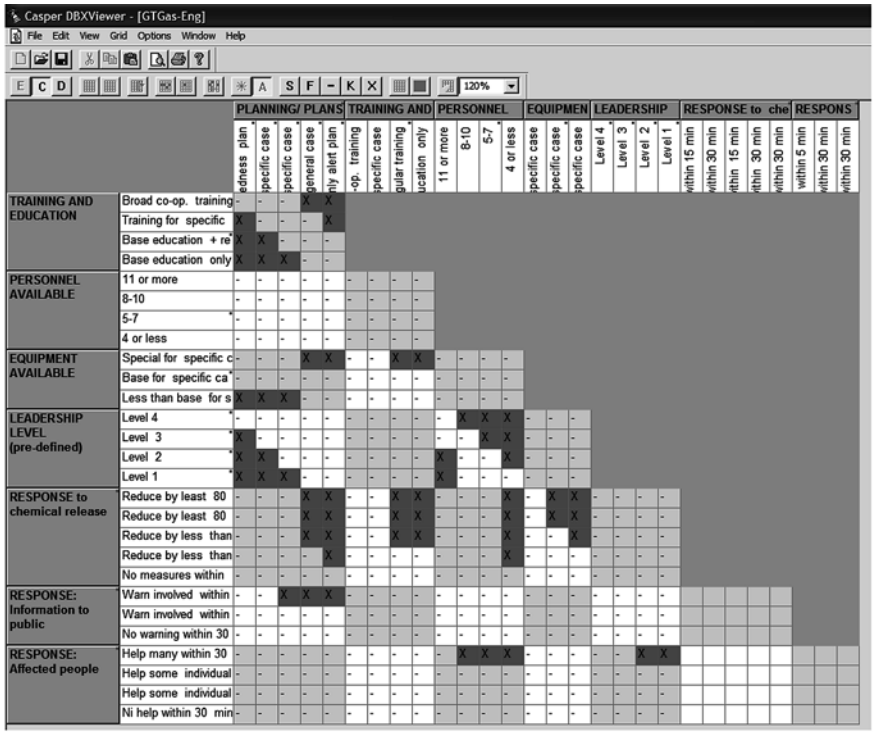
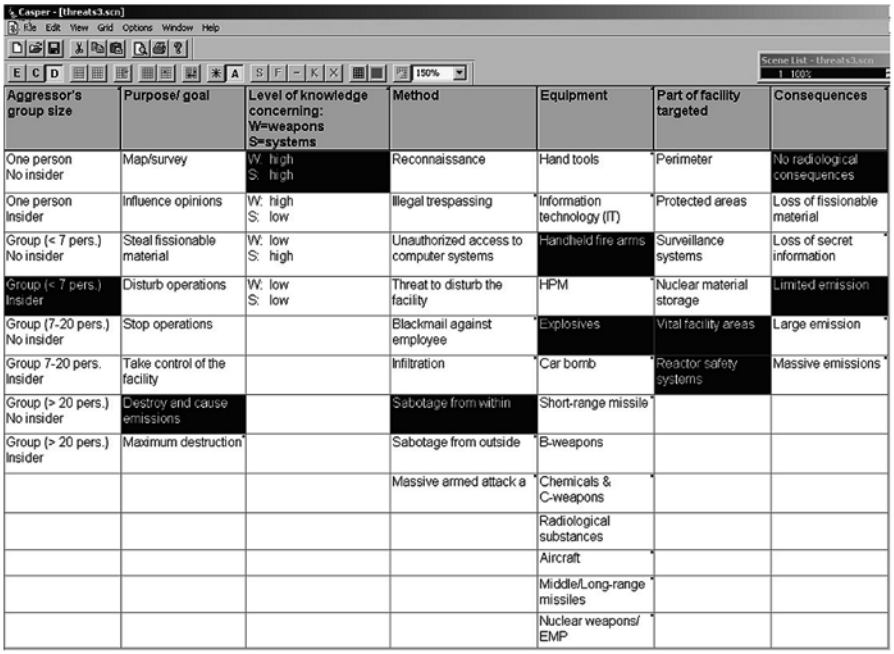


Figure 4: The Cross Consistency Matrix is a form of a cross impact analysis matrix that simply pivots and reformats a morphological field as shown in figure. The one shown here does not relate to the protection against sabotage of nuclear facilities for reasons of confidentiality but is shown to illustrate the principle. There are three levels of assessment: '-'indicates compatibility between the pairs of conditions, 'x' indicates an incompatibility (logical contradiction), and 'k' (not shown) is an empirical constraint, i.e. not possible/compatible now but could be so in the future given the right circumstances (e.g., funding is achieved, a resource is in place, technology has evolved, etc.).

The CCA resulted in the *reduction* to just over 40,000possible configurations, each configuration being a single threat scenario in this 7-dimensional field construct. This smaller subset of *internally consistent* configurations is the solution space - Figure 5 shows one such configuration that describes a small group of aggressors supported by an insider. The group has a high level of knowledge both about the targeted facility and the weapons and explosives they employ. The purpose of their attack is to sabotage equipment in vital areas and/or reactor safety systems and possibly cause a radiological accident. Depending on the effectiveness of safety systems and physical protection measures, the potential consequence would either be no radiological consequences or limited emissions of radioactivity.



Aggressor's group size	Purpose/ goal	Level of knowledge concerning: W=weapons S=systems	Method	Equipment	Part of facility targeted	Consequences
One person No insider	Map/survey	W: high S: high	Reconnaissance	Hand tools	Perimeter	No radiological consequences
One person Insider	Influence opinions	W: high S: low	Illegal trespassing	Information technology (IT)	Protected areas	Loss of fissionable material
Group (< 7 pers.) No insider	Steal fissionable material	W: low S: high	Unauthorized access to computer systems	Handheld fire arms	Surveillance systems	Loss of secret information
Group (< 7 pers.) Insider	Disturb operations	W: low S: low	Threat to disturb the facility	HPM	Nuclear material storage	Limited emission
Group (7-20 pers.) No insider	Stop operations		Blackmail against employee	Explosives	Vital facility areas	Large emission
Group 7-20 pers. Insider	Take control of the facility		Infiltration	Car bomb	Reactor safety systems	Massive emissions
Group (> 20 pers.) No insider	Destroy and cause emissions		Sabotage from within	Short-range missile		
Group (> 20 pers.) Insider	Maximum destruction		Sabotage from outside	B-weapons		
			Massive armed attack a	Chemicals & C-weapons		
				Radiological substances		
				Aircraft		
				Middle/Long-range missiles		
				Nuclear weapons/ EMP		

Figure 5 showing one of the more conceivable threat scenarios. Note all the highlighted conditionsare compatible with each other. This basis of internal consistencyis an essential feature of GMA process.

3.3. Practical implications of the morphological models for SKI

Post-workshop, detailed analysis indicated that certain variable conditions were more important and needed to be addressed specifically in the coming regulations. For example, certain equipment in the hands of an aggressor would increase the possibility of "successful" sabotage. Furthermore, certain parts of a targeted facility were more vulnerable to sabotage than others.

Based on the study and analysis of scenarios in the computer-aided laboratory, as well as a separate strategic threat assessment provided by the Swedish Police Security Service, SKI formulated and proposed a revised DBT. The proposal was further discussed with the authorities involved in the GMA study and appropriate adjustments were made. SKI's advisory board on non-proliferation issues was also consulted before the Director General of SKI finally decided on the DBT.

Given its sensitive nature, the actual DBT is a secret document. However, there is an obvious need to provide both licensees and outside response forces with detailed information about the DBT. In order to promote understanding and acceptance of the DBT, as well as providing information about the process behind its development, SKI arranged half-day meetings with security managers from the licensees and representatives from central and regional police authorities. These meetings were well received and provided the oppor-

tunity for participants to query authorities, which is also a part of the process to establish the DBT.

After having established the revised DBT, the next step for SKI as a regulator was to revise the regulations on physical protection of nuclear material and nuclear facilities. SKI needed to formulate the requirements for physical protection measures necessary to counter the perceived threat and to the new regulations came in force in early 2004.

4.0 METHODOLOGICAL AND PRACTICAL REQUIREMENTS WHEN CONDUCTING MORPHOLOGICAL WORKSHOPS

There are four necessary requirements for effectively constructing morphological models:

1. Deep domain knowledge and experience in morphological modelling(theory, constraints, limitations, ability to bolt on other modelling techniques, e.g. AHP, Monte Carlo simulation, etc.)
2. Extensive knowledge and practical experience of small group facilitation (as opposed to large group facilitation)
3. An appropriate working group of relevant subject matter specialists (or stakeholders): this usually numbers no more than 6-8 participants and can include external experts (e.g., consultants or academics) if this resource is not available within the group provided permission is granted. (Note: observers are not allowed in the modelling exercises due to disruption of the group dynamics. In such cases, a role must be assigned, e.g. a rapporteur, scribe, etc.)
4. Dedicated GMA software – without this, one is not able to produce interactive inference models, to allow the client to experiment with the problem, change initial input conditions and the ability to email the file to superiors or other interested parties).

As with any problem structuring method, there are strengths and limitations with GMA as follows:

Strengths

1. GMA utilises both 'hard' and 'soft' modelling approaches, going through iterations of analysis and synthesis in parameterising a problems space. As such, it can be used with other modelling approaches in framing 'unstructured reality' to create a comprehensible first modelling framework when faced with complex uncertain problems.
2. While the number of configurations in such a space grows exponentially with each new variable, the number of pairwise relationships between the conditions underneath each variable grows only in proportion to the triangular number series. This divergence means that in morphological models, a field with say 100,000 configurations can require no more than a few tens of pairwise evaluations in the CCA in order to rapidly create a solution space.
3. The CCA component is a central feature as poorly defined parameters and conditions thereinbecome immediately apparent when they are cross referenced (pairwise) and assessed for compatibility. This step functions both as an artefact detector and an effective means in ironing out vague concepts and terminological differences. This last point should not be underestimated – it is not uncommon for participants within the same organisation working for a number of years when bought together having vastly

different experiences, perspectives and 'language.'Thus, one of the most important strengths of GMA is the creation of a common terminology, which in turn fosters the development of a common conceptual framework.

4. Finally, GMA leaves an audit trail, which is a particular challenge when working with complex problems as the actual process by which they are formulated and structured is difficult to trace. Without some form of traceability, there is little possibility of scientific control let alone reproducibility, another reason for having a dedicated, flexible software with the ability to document every concept, and each and every pairwise assessment during the CCA (indicated by a red dot in the top right hand corner that open up a dialog box).

Limitations

1. GMA requires strong, experienced facilitation. Creating, structuring and linking the variables takes considerable amount of time than developing an influence diagram with nodes and arrows. Without proper facilitation, it is very easy to create trivial models.
2. Meaningful morphological models cannot be simply created in an afternoon. Depending upon the complexity of the problem and the level of resources available, anything from 2-6 workshops days are needed.
3. GMA cannot be effectively carried out in groups exceeding 7-8 participants as the whole point of the exercise is to foster a dialogue between the subject matter specialists. The threshold of group dynamics, which separates participants talking between themselves rather than addressing the whole group, is remarkably consistent at around 7 ± 2. It is not unsurprising to see, for example, study groups at business schools composed of a similar 'magic' number.[5]
4. Finally, proper morphological modelling requires dedicated computers support. Conducting group modelling, as exemplified by the case study presented in this article is virtually impossible without such support. This is the principal reason why GMA is now fully realising its potential.

5.0 CONCLUDING REMARKS

Morphology isconcerned with the structure and arrangement of parts of anobject, and how these conform to create a whole or Gestalt.The 'object' in question can be a physical system (e.g., an organism, an anatomy or ecology) or a mental object(e.g., linguistic forms, concepts or systems of ideas).

The broad objective of GMA is to formulate and visualize all possible solutions to any given problems and point the way toward the general performance evaluation of these potential solutions. Compared to other 'soft' operational research methods, the major advantage is its organised approach to looking at solution alternatives. It works systematically from the 'morphological space', which is well-identified and commonly known, into a

5 "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information" is one of the most highly cited papers in psychology.It was published in 1956 by the cognitive psychologist George A. Miller of Princeton University's Department of Psychology in Psychological Review. It is often interpreted to argue that the number of objects an average human can hold in working memory is 7 ± 2.

nearby space, which is unknown. The normal procedure is to vary the discrete conditions or options underneath each variable (aka dimension, or parameter) one at a time, keeping the others constant as the examination moves into the unknown region.Additionally, the strength of the technique lies in its total enumeration approach as it proceeds to catalogue all the possible means to a specified end. This cataloguing process can reveal either unintended (negative) consequences of policy action or indeed the opposite - surprising opportunities that might otherwise be either overlooked or disregarded as unfeasible.

Despite Zwicky's persistent efforts to promote the method to technological and social problems, it more or less died with him until being resurrected by a number of researchers in the US and Europe in the field of policy analysis and futures studies (e.g. Godet, 1994; Rhyne, 1995; Coyle &McGlone, 1995). However, the real breakthrough came in 1995, when advanced computer support for GMA was developed at the Swedish Defence Research Agency. This made it possible to create interactive, non-quantified inference models, which significantly extended GMA's functionality (see http://youtu.be/x4zAniSP0FY) and areas of application.

Successful application of GMA requires a subject-matter specialist team being facilitated to develop decision support models using dedicated softwareas mentioned in Section 4. In addition to projects in the critical infrastructure protection space, GMA as the name implies is a general problem structuring method that has been applied across a diverse range of sectors and applications (Table 2)

Table 2: Additional applications of GMA across a diverse array of sectors and applications, highlighted the generic nature of the method

Project	**Client**
Effectively embedding diversity practices in a professional services practices	Reed Smith LLP
Maximising prospects for the corporate development team	Cass Business School
Developing the paediatric drug product development landscape	London Metropolitan University
Future International Market Structures	A leading Swedish international fashion firm
Novel human resource practices in the financial industry following the financial crash of 2008	Cass Business School

A principal requirement is the need for highly-trained facilitators to work face-to-face with the subject-matter specialist workshop team in tackling intractable business and organisational problems. A modelling environment is created thatinterrelates diverse issues such as technology development, policy directives, organisational structure, public perception, financial metrics and training requirements. Furthermore, this process elicits a collective creativity by extracting latent/tacit knowledge of the participants, which gives the team the ability to take account of global shaping forces and novel emergent business models. In short, GMA:

Functions through group interaction and iteration rather than back office calculations to facilitate a process of collective creativity amongst the stakeholders

1. Develops shared concepts, terminology and ownership of the problem formulation through transparency
2. Accommodates multiple alternative perspectives to deal with uncertainties
3. Focuses on relationships between discrete alternatives rather than continuous variables
4. Provides a visual inference model of the entire problem space for the systematic and group exploration for the smaller subset of an internally-consistent solution space.

REFERENCES

1. Coyle, R. G., McGlone, G. R.(1995). Projection Scenarios for South-east Asia and the South-west Pacific, *Futures* 27(1), 65-79.
2. Godet, M. (1994).From Anticipation to Action: A Handbook of Strategic Prospective, Paris,UNESCO Publishing.
3. International Journal of Critical Infrastructure Protection. (2013). Retrieved 28 September 2013, from http://www.journals.elsevier.com/international-journal-of-critical-infrastructure-protection
4. Isakson, S. & Ritchey, T.Protection against Sabotage of Nuclear Facilities: Using Morphological Analysis in Revising the Design Basis Threat (2003),Phoenix, Arizona, *44th Annual Meeting of the Institute of Nuclear Materials Management*
5. Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information,*Psychological Review,* 63(2): 81–97.
6. Ritchey, T. (2006).Problem Structuring using Computer-Aided Morphological Analysis, *Journal of the Operational Research Society,* 57, 792-801.
7. Rhyne, R. (1995).Evaluating Alternative Indonesian Sea-Sovereignty Systems. Informs: Institute for Operations Research and the Management Sciences.
8. Zwicky, F. (1969).Discovery, Invention, Research - Through the Morphological Approach, Toronto, Macmillan Company

Acknowledgment

I am grateful to Dr Tom Ritchey for teaching me the GMA process and allowing access to the work and figures described herein.

UDC 726.9:75.041.5
ID 176374796

Milica Bošković, Violeta Ivković, Nenad Putnik
University of Belgrade, Faculty of Security Studies
boskovicmil@gmail.com
leta@ptt.rs
nenad.putnik@gmail.com

RISK MANAGEMENT IN PUBLIC-PRIVATE PARTNERSHIP OVER CRITICAL INFRASTRUCTURES

Abstract: At the process of system and organization management, beside top, production and financial management, one of the key roles also goes to risk management process and duties. The security and risk management of Critical Infrastructures for its owners (public or private) have tasks to provide business stability and continuity as well as to provide safe work conditions for their employments and to protect the environment. So-called transition countries characterized by weak institutions, legislation and economy, by implementing privatization processes over Critical Infrastructures without the adequate control face the challenge of choosing the right model for re-building systems and institutions, so they could provide better public services and improve socio-economic conditions. This is the reason why public-private partnership has become attractive choice for state government, beside strictly public (state) and private ownership and professional and unprofessional management at critical infrastructures. In this article we analyze the possibilities and capabilities for implementation of preventive phase of the risk management process, at the case of the public-private partnership over Critical Infrastructures. By describing and analyzing various theoretical approaches to the issue of critical infrastructures' management, we will provide scientific knowledge and practical experience of different countries in order to perceive and explain possible benefits of public-private partnerships for risk management process. The aim of this article is to examine the possibility that public-private partnership could have to improve theoretically established approach to elements, processes and activities of prevention and risk management. We will analyze public-private partnership over Critical Infrastructures and eventually recommend this kind of cooperation as the model for improving preventive measures such as risk reduction, risk avoidance, transferring of risk and/or risk acceptance.

Key words: *Critical Infrastructures, risk management, public-private partnership, prevention*

1 RISK MANAGEMENT: CONCEPT AND IMPORTANCE

Management is crucial to the existence and functioning of every organization. Apart from top, production and financial management, risk management processes play one of the most important roles within the process of managing systems and organizations. Appropriate, comprehensive and continuous risk management identifies systemic hazards and risks, as well as corresponding plans, techniques and measures intended for overcoming, eliminating or minimizing the possibility of their realization.

"The term hazard implies the condition which involves the unity of nature destruction and all health and life hazards of a particular social community."[1] The hazards threatening to transform from risks into accidents, may cause damage and different types and levels of negative consequences, from threats to human health and life, material resources, faulty operation of systems/organizations, to threats to the environment. Successful combating various hazards, which only increase in number in the contemporary world, requires the application of methods which enable timely recognition, insight, definition and elimination or minimizing these forms of threats to the safety of organizations and their key elements (manpower, material resources, financial resources, information systems and business information and secrets and the environment).

Risk and threat assessments are aimed at organizations and their elements, with necessary knowledge and understanding of the concept and significance of the existence and functioning of the system.

In case of Critical Infrastructures (CI), the process of risk management becomes more complex and includes characteristics, importance and (security) vulnerability which characterize these systems.

2. CONCEPT OF CRITICAL INFRASTRUCTURES AND RISK MANAGEMENT METHODOLOGY

The concept of Critical Infrastructures (CI) originates from 1960s and 1970s and, in simplest terms, represents all the systems, organizations, goods and services without which the (contemporary) society and the country could not survive, maintain the stability of functioning and develop. CI certainly include the following sectors: energy generation, water resources and water supply; health care system; communication/information technologies; transport; chemical industry; biological substances, banking and financial systems; public administration; the media; research institutes and other. Some definitions of critical infrastructures describe them as "the systems and products – tangible or virtual, of vital importance to the nation, so much so that their incapacity or destruction would weaken economic security of a country and/or public health or security" (US National Protection Plan - NIPP). The European Commission provides the following definition in the document "Critical infrastructure protection in the fight against terrorism" (2004): "Critical infrastructures comprise those tangible and information and technological capacities, networks, services or products which, if threatened or destroyed, would have a serious impact on health, security or economic welfare of the citizens or efficient government functioning in member countries." The importance and role of these systems in contemporary society (which led to the emergence of the term *industrial society*), i.e. human, material, information resources at their disposal, financial and political power they generate, however, do not make them the most stable elements of the society in terms of security; on the contrary, organizational and territorial arrangement, technical and technological characteristics of the resources at their disposal, render them subject to numerous and various risks.[2] From the viewpoint of a (responsible) country, the number of risks and their consequences for citizens increases with the processes in which

1 Jakovljević, V, Etiology of Threats to People, Material Resources and the Environment, "Crisis Management 1: Crisis Prevention", Collection, Faculty of Security Studies, Belgrade, 2006, p. 13

2 See: Bošković, M., "The Challenges of an Industrial Society: New Technologies and Ecological Security", Faculty of Security Studies, Belgrade, 2009.

"public monopolies are transformed into several decentralized organizations subject to competition or privatized organizations".[3] Minimizing or neutralizing hazards, which is a common interest of both the society and the economy, was the starting point for revising the relationship between public and private sectors and establishing the cooperation and understanding regarding risk prevention and control, although the motives of such cooperation vary: the government strives to ensure continuous quality service and goods provision by a CI, whereas the management of a critical infrastructure, by minimizing the risks (certainly including security risks), wishes to achieve the goal of reducing unwanted costs with the aim of achieving the principles of efficiency, cost-effectiveness and profitability. However, nowadays, the necessity for risk management stems from the motivation which is more than just the intention to achieve productivity and profitability at work, or reduce or neutralize risks only with the aim of forestalling economic losses. Risk management and security management of a CI are a reflection of the efforts made by the owners and the management (regardless of the form of ownership) to protect not only business operations (work process in a narrow sense), but also the employees, external entities and the environment.

The methodology of risk and crisis management in a CI comprises the following 5 phases:

1. Preliminary planning;
2. Risk analysis;
3. A specification of preventive measures;
4. Implementation of risk management system;
5. Evaluation of all phases and results.

1) **Preliminary planning**. This phase creates the necessary preconditions for establishing the system of risk management which, among other things, includes the following as well:

- Defining the position of a new risk management system within the existing system of infrastructure management;
- Defining the roles, duties and responsibilities of all the participants in management and executive organizational system;
- Defining the available resources (human, material, information, financial); and,
- Determining the aims of the system of risk and crisis management.

2) **Risk analysis**, as a phase, starts with segmenting the organization into processes and sub-processes. The bigger the differentiation, the greater the efforts and resources are required for analyzing, but the information obtained in such a way is more detailed and valuable.

3) **A specification of preventive measures**. The purpose of creating and implementing the preventive measures and strategies is reducing the possibility of risks to occur-realize and transform into a crisis. Preventive measures are represented by the following instruments:

- Risk reduction
- Avoiding risk
- Risk transfer
- Accepting risk.

3 Johnsen, A., Irwin, L., "Reinventing public sector accounting", Financial Accountability & Management 21(3), 2005

4) **Risk management** - the implementation of risk management systems. The purpose of implementing risk management, as well as crisis management on critical infrastructures, is:

- Maintaining the highest possible efficiency of a system
- Recovery of critical functions in the shortest possible time.

Risk management plan as a base for the creation and implementation of risk management system, as well as crisis management, should include and define the following elements:

1. Purpose and goals of the plan
2. Legal basis
3. Organizational structure of risk and crisis management
4. Risk management team and crisis response team
5. Defining the roles and responsibilities of management team members
6. Creating special procedures for risk and crisis management
7. Chain of command
8. Models of crisis escalation and de-escalation
9. Recovery measures
10. Modes of informing.

5) **Evaluation** as a phase includes the analysis and assessment of the processes of defining and conducting all previous phases and their individual results, as well as final outputs of the entire risk management process. All created plans and adopted management measures are assessed against the obtained data and results, but the existing decisions and activities are also revised.

In this study, the aspect of the form of ownership and critical infrastructure management, as a factor influencing appropriate risk management within those infrastructures, shall be reviewed in the phase "preventive measures and strategies".

Previously specified "Preventive measures and strategies", as one of the phases of risk management, includes the following models and instruments:

1. Risk reduction;
2. Avoiding risk;
3. Risk transfer;
4. Accepting risk.

1. Reduction in probability of risk realization or its neutralization, if possible, is the primary goal of risk management, as well as management in general. All the activities which are being implemented for the purpose of establishing risk management, defining hazards and risks, as well as implementing protection measures, are performed for the purpose of neutralizing the identified risks if possible (which is rare), or the reduction in probability of their realization and causing accidents. 2. Avoiding risk in terms of refraining from all those activities which may lead to risk realization is directly connected to and dependent on the previously mentioned prevention instrument. Since there can be no absolute security, it is therefore difficult to achieve total risk neutralization, but they could be minimized and the circumstances which lead to their manifestation may be controlled. Taking preventive measures and controlling internal and external risk factors and the influence on risk manifestation represent the core of this instrument. Although this instrument is easily explicable, its practical application is actually a very complex process which requires security behaviour with a high level of awareness of the hazards, continuous, directed and

harmonized activities, or the "behaviour" which will not create or contribute to the factors which influence risk realization.

3. Risk transfer is the instrument which is in essence different from previously mentioned instruments. It represents one of the models of preventive action, which implies the transfer of competence and tasks to those sections of the system (sub-systems) or external agents/entities, which can manage certain risks more efficiently in the defined and concrete circumstances. The analysis of any individual risk in fact represents a probability assessment of risk realization and the consequences it may have, and an integral part of this assessment is the process of defining endangerment or vulnerability of a CI, through the recognition of the existing security measures and drawbacks, as well as the possibility for their overcoming and improving the protection measures. When the CI as a complete system is not able to face the challenges with the existing resources, or to control them appropriately, those sections of the system or external entities are explored and recognized (such as public services, state bodies, business partners), whose capacities can successfully neutralize or minimize the risk which the CI delivers or transfers.

All the mentioned instruments and risk prevention strategies require not only mutual cooperation, professional and coordinated activities of management structures within the CI, but the creation and maintaining of cooperation with the entities outside the system as well, primarily with the state bodies, which have a common interest in stable and secure operation of critical infrastructures, that is, the unobstructed provision of services and goods which result from the activities of these organizations and are of importance to the country and the society.

3. CRITICAL INFRASTRUCTURES AND FORMS OF OWNERSHIP IN THE REPUBLIC OF SERBIA

The Critical Infrastructures which include energy industry, industry, transport and infrastructure, health care and social care systems, telecommunications, finance (banking, stock exchange and budget systems, etc.), administration (public administration) in the Republic of Serbia are mainly state-owned and have a monopoly in the market of goods and services, while a small number of companies in the above mentioned sectors are in private ownership (privatization process completed), or certain private companies are established as competitors (the examples in the field of mobile telecommunications, certain branches of industry and partially in aviation industry). Although the process of (complete) transition to business operations in free market economy requires the transition from state control to private ownership (which is almost inevitable from the budget and macroeconomic viewpoint), these activities are performed slowly or almost not at all. Therefore, almost all forms of CI in Serbia exist and operate as public enterprises. A public enterprise is a company which performs public interest activities and is established by the state, or a local self-government unit or an autonomous province (The Law on Public Enterprises and Performing Activities of Public Interest).[4] The greatest development issues are found in the following non cost-effective public enterprises: the Electric Power Industry of Serbia (EPS), the Serbian Railways, JAT and the Roads of Serbia. These data are presented in the analyses of business operations of public enterprises prepared by the

4 "Official Gazette of the RS" 25/2000, 25/2002, 107/2005, 108/2005

Sector for National Development of the Ministry of Finance of the Republic of Serbia for the year 2010.

Global economic crisis additionally slowed down the process of transition reforms in Serbia, which is also recorded by the EBRD indicators. The value of EBRD index of infrastructure reform (2.3) remained unchanged when compared to 2009. In comparison to the neighbouring countries, the value of the index of infrastructure reform in Serbia is at the same level as in Montenegro and Bosnia and Herzegovina, and lower than in Romania (3.3); Bulgaria, Slovenia and Croatia (3.0) and Macedonia (2.7). Serbia is lagging behind most neighbouring countries in the area of privatization of big systems, managing and restructuring enterprises and implementing competition policies. A great number of public enterprises have been operating at a loss for years, and the reasons may be related to the existence of monopolies these companies have in the Serbian market, inadequate management structure and the lack of implementation of internal processes of modernization and restructuring. Operation losses, naturally, do not leave any space for CI management to continuously invest all necessary resources (human, material and financial) in the area of risk management and preventive measure implementation. From the viewpoint of internal as well as general security, this can certainly pose a problem and a challenge for both critical infrastructures themselves and the country, whereas from the viewpoint of privatization processes, this is another reason for changing the policy related to the implementation of certain forms of privatization, i.e. partial or complete change in the method of managing these enterprises.

3.1. Privatization and "Public-Private Partnership": Foreign Experiences

During 1970s and 1980s, complex privatization processes of numerous enterprises were initiated in the capitalist countries, based on the conclusion that state-owned enterprises achieved less effective business results and that they were inefficient compared to the companies in private ownership. Privatization process was in accordance with the accepted neoliberal economic theory which was based on the rule of private property. The government took responsibility for implementing large and complex privatization processes. An active role of the government is reflected in the adoption and implementation of a set of primarily legislative, but also economic measures which define the entire privatization process, as well as prevent disorganized selling (sale) of state-owned enterprises. The adoption of a privatization programme requires a "critical assessment of the state of the economy and society and passing appropriate decisions. The political and institutional environment where privatization will be implemented should primarily be taken into consideration; the identification of groups opposing privatization and the groups accepting privatization; basic documentation about the enterprises which can be privatized; the selection of enterprises to be privatized; ...and later, monitoring enterprise operations."[5] An important segment of privatization process is deciding which enterprises are to be privatized and the proportion of privatization. Reaching decisions on the privatization of enterprises of strategic importance for the country, or CI, such as telecommunications, waterworks, electric power industry and similar enterprises, demands special attention from all relevant decision-making factors. In the majority of cases the transition countries copied the models applied in the capitalist countries when they were changing their systems,

5 Mitrović, B, "Transition in Post-socialist Economies – the Example of Yugoslavia", Prosveta, Niš, 2000, p. 118

so that this particular practice was also applied in the privatization process. However, it seems that privatization in former socialist countries was sometimes conducted without a thoroughly designed plan. One of the consequences of the unplanned and uncontrolled privatization process is the absence of so-called "smart privatizations". Namely, privatization was non-selectively conducted, so that the state was stripped of ownership and/or the control of the enterprises of vital importance, which is quite the opposite of the purpose of privatization in the capitalist countries.

Institutionally, legally and financially "weak" transition countries, having conducted unfavourable CI privatizations and with the dissatisfied population, face the challenge of selecting an appropriate manner of building strong and stable systems, public services, economies and favourable socio-economic circumstances. Therefore, apart from the strict separation of public and private ownership, as well as professional and unprofessional management of CI, so-called "public-private partnership" has increasingly emerged.

Public-private partnership – PPP is primarily a contractual relationship between public and private sectors which can include financing, designing, construction, management and/or maintenance of infrastructure and/or providing services by private sector, which is traditionally provided or performed by public sector. It is considered that the advantage of public-private partnerships lies in the fact that such model combines the advantages of public sector which are reflected in public/social responsibility with the advantages of private sector which implies the possession of financial resources, technology, knowledge about professional management.

"Public-private partnership is widely defined as a cooperative, institutional arrangement between public and private sectors, which is considered desirable throughout the world."[6] One group of authors considers PPP a new government instrument which replaces the traditional model of contracting services through tenders in the field of public affairs and activities, while the other group considers it a new mode of expression in the field of public administration, whose aim is to include private sector in public affairs and subsume it under the existing, already established procedures.

Public-private partnership is certainly not a contractual form whose application is unanimously agreed upon by different experts, but the possibility of its realization, which is a positive point, causes public and expert debates, attracts attention of the managers of public enterprises, competition in private sector, and that is the reason why "nowadays this type of relation is established in a much more sophisticated and far-reaching form than ever before."[7]

After 15 years of war (1975-1990) waged in Libya, only 45% of public resources of this country were operative. In 1999, 52% of its budget was allocated to debt servicing, and 32% to salaries and pensions, which practically left no public resources for restoring and increasing the capacity of CI. One of the greatest issues in the field of CI functioning in Libya was drinking water production and its distribution system. The losses in the field of water management and extremely harsh operating conditions were not only social and

6 Hodge Graeme A., Greve Carsten. Public-Private Partnerships: An International Performance Review, Public Administration Review, 2007, p. 545

7 Hodge Graeme A., Greve Carsten. Public-Private Partnerships: An International Performance Review, Public Administration Review, 2007, p. 544

economic problems, but security problems as well. After establishing a PPP in 2001, the operating costs of water management gradually decreased, the infrastructure was rebuilt, and the production and distribution of drinking water reached the optimum quality and level.[8]

Health care system, as a type of CI, also experienced problems in certain regions and periods due to inadequate or insufficient operational and/or financial support by the state as the owner. "Many diseases in the countries with low or medium gross domestic product appeared as a result of the absence of commercial initiative which could start private investments in research and development in the field of medicine."[9] After 1990s, a great number of PPP with international character filled this gap. The cooperation between public and private sectors in the field of medical and pharmaceutical research and innovations made progress in treating many diseases much faster, and rendered drug market more stable and available to the citizens.

3.1.1. Risk Management in CI through Public-Private Partnership

Most explanations of the importance of PPP establishment boil down to the conclusion that such contractual form is created in order for public and private sectors to reach the desired benefit. The reason for such perspective lies in the fact that "public and private sectors have specific qualities, and if combined, the final outcome would be better for everybody."[10]

Although numerous definitions, explanations and practical examples emphasize economic (financial) and material benefits and better functioning of CI (the provision of services or the production and distribution of goods) as primary benefits of the existence of PPP, a significant benefit can be recognized in the area of security, primarily the activities related to risk management.

Risks, in simplest terms explained as a probability for an identified hazard to realize and have consequences, are multifarious and numerous and can be found in the field of business operations, finance, information systems, human resources, physical and technical security, the environment, capital placement, research and innovation, etc. In the case of CI, many other hazards and risks multiply, and their management becomes more complex.

In a successful and stable functioning of a CI which meets the needs of the society and state (but also its management), economic, market, management and security risks certainly must be treated as equally important, especially if taken into account that the neutralization or on the other hand expression/realization of any of the specified (or other) risks is interacting within the chain of reactions and brings repercussions to other parts of such a complex system – manpower, facilities, finances, information technologies, as well as the near of wider environment.

Considering that the operation of CI in the Republic of Serbia in the past several years, which in most cases has been characterized by operational losses, debts, unprofitable pric-

8 See also: Yamout, G., Jamali, D. (2007). A Critical assessment of a proposed public private partnership (PPP) for the management of water services in Lebanon. Water Resources Management 21.

9 Buckup, S. (2008). Global public-private partnership against neglected diseases: building governance structures for effective outcomes. Health, Economics, Policy and Law 3 (01), p. 31

10 Hodge Graeme A., Greve Carsten. (2007). Public-Private Partnerships: An International Performance Review, Public Administration Review, p. 546

es or non-competitive market offer and the monopoly, and in more than a few cases insufficiently competent management as well, one can ask rightly to what extent the management of various public enterprises could successfully and comprehensively manage their resources, as well as face all the challenges, risks and needs, including the security risks.

Establishing a PPP through the CI which is currently in complete state or social ownership, given the proposed economic indicators, could bring certain benefits, such as:

- Keeping a certain degree of control and ownership of our country over CI, which are vital systems for normal functioning and development of a community;
- Ending or significant reduction of budget financing and/or debt payment of certain CI which is currently underway;
- Establishing an experienced and expert management independent of the executive power of our country or the partner's country of origin;
- Providing private investments in reaching higher competitiveness, productivity and cost-effectiveness, but also social responsibility in the operation of CI.

Relocation and redefinition of the method and goals of utilization and placement of the existing financial and other resources of CI in the case of PPP establishment, also enables finding and investing more resources in the field of secure operation of CI, which implies the establishment of expert management team in this area.

The establishment of PPP certainly causes changes regarding the implementation of all five previously mentioned phases of risk management methodology.

The creation of a public-private partnership with a certain public enterprise, in the area of CI, involves redefining management and supervisory structures, as well as all sub-structures, certainly including security and risk management; also, the strategic and operational aims and achievements of the enterprise are analyzed, amended or redefined, the existing resources, investment volume and dynamics are defined, as well as their renewal and improvement.

The analysis of various risks (business, market, security, etc.) is conducted in the phase of examining and negotiating a potential PPP, whereas the analysis is conducted by the state and an interested private entity. The analysis, after establishing a partnership, is developed and examined by the newly established management team.

Regarding risk management, and especially the phase of preventive measures implementation and selection of strategies, the establishment of a PPP can be significant in many ways. As indicated above, the basic instruments in the phase of "specification of preventive measures" and the selection of risk prevention strategy are: reduction, avoiding, transfer and accepting risk.

a. Risk reduction implies recognizing and mobilizing all available capacities in the direction of neutralizing or minimizing the probability of the identified hazards. The establishment of PPP defines the new management and sub-teams, which consist of experts whose main priority (regarding risk management) becomes minimizing risks, which contributes to the general stability in CI functioning and productivity; every private investor has an interest to minimize security risks in addition to minimizing business risks, since investing in prevention financially and materially represents a significant cost, but certainly lower than the cost of recovery from the effects of a potential accident.

b. Avoiding risks implies refraining from all those activities which may influence or indirectly lead to risk realization and in that sense this strategy is partially connected to the previous one. The implementation of this strategy implies continuous, comprehensive, analytical and constant work on recognizing risks and implementing measures and activities in order to avoid risky behaviour, acts and phenomena. Such a complex process which is required by the strategy in order to be realized is certainly realized much more easily and comprehensively in the case of the existence of a PPP within CI. The experiences private sector gained during operation, with the assistance of the state, make the process of avoiding risks a complex one, but also attainable through professional monitoring and managing the measures of avoiding risks. The education and training of all the employees regarding security behaviour and precautionary and protection measures, recognizing "weaknesses" of the system (facilities, equipment, information systems and the like) and their strengthening, establishing monitoring systems of CI functioning in relation to critical points and constant redefinition of the tasks and methods of avoiding risk, are more comprehensive and can be implemented faster in case of joining the resources of public and private sectors.
c. Risk transfer is a strategy which possibly best reflects the importance of the establishment of PPP. Public-private partnership most often does not include only investments in the existing resources and infrastructure, but building capacities as well by engaging certain sub-systems of a private partner. Thus CI extends its branching system with new organizational units, facilities, manpower, material resources. In such circumstances, the possibilities of risk transfer from the endangered place which cannot appropriately face the challenge with its capabilities are transferred to other sub-systems or organizational units which are able to control and successfully manage the accepted risk at a given moment. Risk transfer can be performed in accordance with the capacities of both public and private partners. In the case of exclusive state or private ownership of a specific CI, the possibilities of transfer of one or more risks are certainly limited. PPP enables a more comprehensive analysis of all available resources and organizational branching of the system, and thus risk transfer, from the point where it is most likely to be realized due to insufficient preventive measures, is facilitated and accelerated by selecting the part of CI which is the most capable of absorbing risks and manage it with its resources at a given moment.
d. Accepting risk is a strategy implemented when the possibilities of all previously mentioned strategies are exhausted. As in the case of risk transfer strategy, it is much easier in this case as well to accept risk when risk management and control can involve various resources, experiences and management teams which are certainly more complex and capable when a public-private partnership with CI is established. The strategy of accepting risk is the strategy which can be the final one or a part of one of the above strategies, primarily reduction or avoiding risk strategies. By entering a public-private partnership, both contractual parties show willingness to take risks – the state for its part, hands over its partial or complete management of a CI, and resources and systems vital for the functioning of the society and institutions, whereas a private partner invests resources, experience and knowledge into those organizations whose balance sheets usually show losses or insufficient

expected income. An interest in partner operations with the aim of restoring and improving CI reflects readiness for recognizing and comprehending risks, as well as methods for their overcoming. The management should be able to express such readiness related to the strategy of accepting risk as well, which pertain to security issues.

In the case when a risk is non-transferable, when prescribed strategies and measures for avoiding or reducing risks are insufficient, the risk should be taken – which implies thorough and complete understanding of the nature and character of a given risk, its source, forms of expression and causing damage. This is the first and the most important step, which is followed by defining the measures for comportment and operation in accordance with the accepted risk and its latent presence is made far easier, more appropriate and comprehensive.

4. CONCLUSION

Providing stable functioning of CI does not imply the selection and implementation of one or two previously described strategies, but all four, which make only a part of complete risk management methodology. That task requires a dedicated expert team, continuous work, human resource management (their education, training and security), but also investing financial, material and technical resources and the preparation of various internal documents which are in accordance with the normative acts of the country in which business operations are performed, or with which public-private partnership is concluded. Risk management of CI which is in exclusive state ownership and management, along with other organizational segments of CI, may not so effectively fulfil its complete function, especially considering that goods and services provided by these companies should be (financially) affordable to the citizens of transition countries (the status of our country as well), and they most often operate at a loss or gain insufficient for investing in all segments of operation and therefore are financed from the (scarce) budget.

PPP represents one of possible and desirable solutions for restructuring, recovery and more advanced business operation of such a CI. Regarding security and risk management, the establishment of PPP results in far more certain professional and comprehensive organization of activities in the area of prevention and risk response as well as in much stronger possibilities for their reduction, transfer and acceptance.

REFERENCES

1. Bošković, M. (2009). *The Challenges of an Industrial Society: New Technologies and Ecological Security*. Faculty of Security Studies, Belgrade
2. Buckup, S. (2008). Global public-private partnership against neglected diseases: building governance structures for effective outcomes. *Health, Economics, Policy and Law 3 (01),* pp. 31-50.
3. Hodge Graeme A., Greve Carsten. (2007). Public-Private Partnerships: An International Performance Review. *Public Administration Review,* pp. 545-558.
4. Jakovljević, V. (2006). *Etiology of Threats to People, Material Resources and the Environment.* In: Crisis Management 1: Crisis Prevention, Collection, Faculty of Security Studies, Belgrade.
5. Johnsen, A., Irwin, L. (2005). Reinventing public sector accounting. *Financial Accountability & Management 21(3).*
6. Law on Public Enterprises and Performing Activities of Public Interest. *Official Gazette RS 25/2000, 25/2002, 107/2005, 108/2005.*
7. Mitrović, B. (2000). *Transition in Post-socialist Economies – the Example of Yugoslavia*. Prosveta, Niš
8. Yamout, G., Jamali, D. (2007). A Critical assesment of a proposed public private partnership (PPP) for the management of water services in Lebanon. *Water Resources Management 21*, pp. 611-634

UDC 726.9:75.041.5
ID 176374796

Dragan Trivan
Serbian Association of Corporate Security Managers
dtrivan@gmail.com

Vladimir Radović
JP „POŠTA SRBIJE“
vradovic@jp.ptt.rs

CORPORATE SECURITY ROLE IN PROTECTING CRITICAL INFRASTRUCTURE

Abstract: An increase of the risk of asymmetric security threats, especially after the terrorist attacks in USA in 2001, has led the protection of critical infrastructure to become one of the priorities of the national security in almost all countries. Although in theory there is not complete consensus yet on the content of the term and concept of critical infrastructure, it usually implies the natural and material resources, assets, technical systems, communications, businesses activities and services that are of particular importance to the country, and whose destruction or interruption in functioning could jeopardize the national security, economic system, vital social functions, public health, public order and the protection of national interests. Technical systems, technological processes and operations in different parts of the critical infrastructure at the national level can be targets of different threatening acts, including terrorism. Therefore, the critical infrastructure facilities are specially protected, along with the creation of regulatory, organizational, technical and security conditions for its normal functioning, in order to prevent or reduce the probability of occurrence of the natural or man-induced incentives that may lead to the catastrophic disruptions within the protected systems. In this regard, the research of the issues related to the role of corporate security in the protection of critical infrastructure requires the use of different scientific methods (historical-comparative method, case studies, content analysis, testing). When it comes to the critical infrastructure in the Republic of Serbia, the protection of its parts pertaining to the energy sector, water supply, postal services, telecommunications and rail transport, is still mostly performed by the former security services of the public enterprises that have been transformed in the past period into independent companies providing security services. Other facilities of the critical infrastructure in Serbia are secured in a combined way - by their own security services and by hiring private firms within the relevant industry (outsourcing), whereby the provision of such services still does not include an adequate legal basis. Functioning of the corporate security in the critical infrastructure facilities in Serbia is adversely affected by the numerous cases of crime and corruption in the public sector, politicized management and the absence of public-private partnerships in this area, and the lack of operational cooperation among the corporate security entities, police and security intelligence services. Bearing in mind the gravity of the threats to the critical infrastructure facilities, it would be optimal to implement the integrated model of corporate security for their protection, along with the outsourcing of the less sensitive functions of the system (physical and technical security) to the external specialized providers. The analysis of the research results suggests the necessity of adopting the encompassing normative regulation and establishment of the appropriate organizational form of the corporate security at the critical infrastructure facilities in Serbia, and in particular the research can help the agencies in the area of private security in their engagement to perform some of those functions according to the outsourcing model.

Keywords: *critical infrastructure, security threats, corporate security, protection, the Republic of Serbia, outsourcing.*

1. INTRODUCTION

End of the 20th century has led to strategic changes in the world, which have significantly altered the contemporary security paradigm and the ways in which states observe their international environment and where they achieve their national interests. State spaces have got a new quality and they are not any longer looked upon within the context of the acquisition of territories by winning, but they have become the area of cooperation and associated economic activities. This especially refers to Euro-Asian zone, which in the last two decades, from a divided area, is gradually transformed into the area of democracy and of market economy. In that context, new security threats are increasingly directed towards different types of economic activities, where one of the key targets of jeopardizing represents the objects and resources of the critical infrastructure. It is certain that the states are obliged to act in direction of prevention and organization of infrastructure aiming to adequately react in crisis situation. Earlier Cold War environment has imposed to the states, through models of national security, to create a strong infrastructure that was intended for the defence of the territory and population. In today's globalized world, the risks are also globalised, so the existing security models are not adequate for the new challenges. In the current circumstances, critical infrastructure is the most sensitive part of the national resources required for the stable development of the country. In order to protect this infrastructure from various types of threats, it is necessary to make big efforts at the national level, but also on regional and international levels, and the systems of its security must be built and aligned at the level of society, and also at the wider state environment. In that process the specific role goes to more and more present non-state security sector, including its important component – corporate security (Cvrtila, 2009, p. 23-24).

2. CORPORATE SECURITY AND CRITICAL INFRASTRUCTURE

2.1. Corporate security

According to some of the current definitions, corporate security is a state and/or a process of absence of intentional, negligent or accidentally caused danger in the biggest business systems in the domain of corruption, organized crime, business secrets, informatics security, physical and technical security and protection at work. In this regard, corporate security is a strategic function of the company, the aim of which is the realization of business success of corporation, which includes: elimination of all risks and threats that may affect the business activities and achieving of business success; reducing threatening effects to a minimum; business functioning in crisis conditions (crisis management), overcoming the crisis and returning to normal business (Ivandić, Vidović, Karlović, Ostojić, 2011, p. 34). Within the frame of corporate security system, security management represents the subject of organizing and management of the system for securing the corporations' personnel and property. Determination of goals, planning, organizing, issuing orders, control, coordination and responsibility for safe work and doing business of the company is within its competence.

In contemporary conditions, corporate security has become a strategic function of business entities and it defines an integrated security policy of corporations as such, and its unique implementation in practice. In this regard, the definitions of some authors indi-

cate that the basic characteristics of corporate security includes the following: overall corporation security; responsibility of corporate security experts, who are nowadays faced with difficult tasks (to simultaneously support growing business needs and to disable all increasingly sophisticated attacks on corporations); professional ethics, belonging to the profession and efforts of all professionals in corporate security area to give the best they can (Murray, McKim, 2000, p. 6).

According to the doctrine and practice of the countries with the developed market economy and a stable democracy, the functions of corporate security include the following: administrative security – procedures and policy in informatics protection area; physical and technical security (Out-Source/Proprietary) of machines, plants and buildings; security of property and of external partnerships (Personnel Security); individual security (Protective Security) – protection of persons and protection at work; fire-protection security; acting in extraordinary situations (Contingency Planning); information security; executive security; security at various business events (Event Security); security of contracts with the government; investigation/crime protection program (Investigations) and security education awareness and training program (Kovacich, Halibozek, 2002, p. 161-162).

In case of corporate security development in the states of South-Eastern Europe, we should have in mind that the type of activity as well as the affiliation of the company to the particular industry determines the nature of security tasks in it and the specifics of corporate security organization. In this respect, the most important industrial branches at the area of the Western Balkans are related to the exploitation of oil, gas, mines and other natural resources, including water. The business of corporations in that area requires large investments and generates big incomes that are to be shared with local authorities, which often becomes a source of disputes and frictions within or between the countries. Corporation practice indicates the big influence which these companies may have to the local surroundings and its existing characteristics (ecological, demographic, technical and technological) in terms of the degree of protection of natural resources and of a decrease of various types of pollution. Corporate security in such corporations has got a great importance in situations related to building and functioning of the big infrastructure projects, especially of the ones which require displacement and relocation of local population, for the sake of realization of access to natural resources which are the subject of exploitation. Mining, oil wells and similar activities that degrade natural resources, may often aggravate local security situation, especially if they are not followed by informing of population about the potential health threats (Trivan, 2012, p. 25).

In the Western Balkans countries an important part of actual functioning of corporate security within business entities is still connected to the jobs which are in the widest sense linked with physical and technical security of persons, property and activities of companies, internal factors which organize and direct these jobs, as well as the engaged external and internal subjects who implement it in practice. Current "epicentre" of corporate security in the countries in this area is a self-defence activity in big technical and technological systems, which leads to mistakes in defining of the corporate security concept and in determination of its content. The problem becomes more complex due to the fact that some of business entities which are mandatory secured (banks, post offices and other) may have almost all categories of private security services represented, more precisely of protection and self-defence activities.

2.2. Critical infrastructure

In the recent time, and especially after the terrorist attacks in the USA in September 2001, the term "key/critical infrastructure" is often used in the professional literature (Rinaldi, Peerenboom, Kelly, 2001, p. 13). Although among the authors there is no complete consensus on the content of that term and concept, it most often includes natural and material goods, assets, technical systems, communications, business' activities and services that are of particular importance to the country and whose destruction or interruption in functioning could jeopardize the national security, national economic system, vital social functions, public health, public order and protection of national interests (Čaleta, 2011, pp. 16-17).

According to a comparative analysis of critical infrastructure in 16 surveyed countries made in 2004, the below stated would belong to that category:

- Banking and finance, (tele)communications, information and telecommunications systems and energy (they represent a critical infrastructure in 14 countries);
- Health services, water and water-supplying (12 countries);
- Central government/government agencies (11 countries);
- Emergency rescue services (10 countries);
- The supply of petroleum products and gas (9 countries);
- The media, public administration (8 countries);
- Other areas, including justice, public order, national security, waste management, Radiological/Chemical/Biological (RCB) protection, the army and military facilities, security systems, social services, nuclear power plants (represent critical infrastructure in some countries).

Having in mind the priority groups in the area of critical infrastructure, it is evident that neither the definition of critical infrastructure nor its contents are identical in all parts of the world; it is therefore necessary to determine them at the national level (Cemerin, 2007, p. 81).

The concept of "critical infrastructure" in the United States of America includes those goods, systems and networks, both, material and non-material which are of such importance for the USA that their disabling or destruction would jeopardize the national security system, economic safety of the country, public health and general security, in fact, any of these systems individually or combined (USA PATRIOT Act of 2001, October 2001). In this regard, critical infrastructure consists of public and private institutions in the sectors of agriculture, food, water, health care, emergency services, government, defence, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, postal and transport. In order to protect and ensure the continuous operation of the national Critical Infrastructure and Key Resources (CIKR), regulation of the U.S. President introduced the labels 7 (HSPD-7), which set forth the guidelines for establishment of the system of protection of these resources from potential attacks and jeopardizing of their functioning (Radvanovsky, 2006, p. 3-4).

Within the USA House Committee on Homeland Security there is a sub-committee which deals with the "security of computer and communications networks, information technologies, production management system, electricity supply system and databases, both governmental and private, from both internal and external attacks, preventing the loss of population and infrastructure." As the cyberspace is the nerve system – management

system of the USA, and the economy and national security of the country depend on it, in February 2003 the National Strategy to secure Cyberspace was brought.

The consequences of the new understanding of security threats to the United States of America, embodied in strategies, directives and laws were the following: the work on development of the National Communications System (NCS), the reorganization of intelligence and reconnaissance community, physical protection of important facilities of critical infrastructure, insisting on the key role of information technology in the increase of the internal security, the support to technological superiority of the USA, the researches in the area of protection of information infrastructure and training of citizens in gaining of habits of survival in conditions of technogenic and natural disasters and terrorist attacks.

The European Union seeks to ensure an adequate and equal security level of the facilities and equipment of the selected critical infrastructure, what is feasible only on the basis of a common European framework for its protection. The interest in the EU critical infrastructure by the member states emanates from a danger that destruction or disturbance of a certain critical infrastructure in one member state may directly jeopardize other member states. In such cases the security measures are as strong as their weakest link is. According to the European Union standards, Critical Infrastructure encompasses electric power production and transmission, chemical industry and nuclear plants, production, transport and distribution of oil and natural gas, telecommunications system, potable water resources, production of basic food products, heating system, public health facilities and services, public transport system, state government bodies, financial and security institutions. In this regard, and on the grounds of the directive of the European Commission/EU COM (2006) 786 final, the EU has adopted the European program of protection of the key infrastructure, which also contains the European list of the key infrastructure (ECI), created on the grounds of the suggestions delivered by the Union member states.[1] In that regard, the European Union defines so called European critical infrastructure as the one which consists of those physical resources, services, information technology devices, security of network and infrastructure, security, economical and social benefit: either of (a) two or more member states, or (b) three or more member states.

In the case of the states from the area of the former SFRY it is apparent that all of them strive to identify and define their own critical infrastructure as precisely as possible. In that way, by the Resolution of the Republic of Slovenia Government from 2010, it has been established that the critical infrastructure in that country includes all goods and services that are essential for the country and whose disruption or destruction would have a major impact on the national security, economy, vital social functioning, health, security, protection, as well as on the overall social wellbeing. The Republic of Macedonia has no special law that specifies critical infrastructure. However, some legislative acts put the protection of critical infrastructure in direct jurisdiction of the Ministry of Interior, the Ministry of Defence, and the Ministry of Transport and Communications. In November 2008 the Republic of Croatia adopted the Strategy for prevention and suppression of terrorism, according to which the critical national infrastructure is defined as the set of assets, services, systems that support the economic, political and social life in the country, and whose partial or complete jeopardizing may result in loss of life, threaten national security and the

1 Council Directive (EC) No. 114/2008 dated 8th December 2008.

functioning of the economy, and can seriously jeopardize a part of the community or the whole state community (Gačić, Šećerov, 2012, pp. 165-166).

In 2009 the Government of the Republic of Serbia brought a Decision on determination of major technical systems of importance for the defence,2 and in compliance with it, eight major technical systems in the domain of traffic and telecommunication were included into the critical infrastructure resources in Serbia – important for the state defence, as well as three public enterprises and four corporations in the domain of energetics, one public enterprise and one company in the domain of coal production and 12 more public enterprises and institutions in the domain of water-supplying, transfer of thermal energy, forest management and broadcasting. This Decision regulates the procedure of reporting related to the selection, building and development of these systems, the procurement of technical equipment and the way of technical equipment providing as well as placing the demands for their alignment with the needs of national defence. The investor is obliged to inform the Ministry of Defence and other competent Ministries about the selection, building of vital and capital facilities and the development of technical systems important for the state defence, and also about procurement of technical equipment important for the functioning of these systems. The investor also encloses to the notification the appropriate investment and technical system documentation and specifications for the purchase of technical equipment and explained program of development of the underlying system.

2.2.1. Vulnerability of critical infrastructure facilities

Technical systems, technology processes and operations in different parts of critical infrastructure are attractive targets of possible terrorist acts. The application of a number of available methods and techniques of attacks may disable their proper functioning, may induce outages, and cause doubts and distrust in their safety, correctness and reliability. Key elements of the national infrastructure, such as transport, telecommunications, production and distribution of electric power and other fuels and energy sources, banking, public health care, state and local administration, water supplies, media, science, education, emergency and rescue services, have become dependent on information and communications systems.

We should not neglect the fact that the persons with limited technical knowledge and relatively limited knowledge of some technological processes and operations, but who are intelligent enough, persistent in searching and skilful in identification of bottlenecks and vulnerable points of the critical infrastructure system, may cause their collapse or fallout from a function, with possible far-reaching adverse consequences. For the increase of their operational capabilities the terrorists may, most of all, thank to a plenty of commercial and easily available sophisticated technical equipment and tools, such as: top computer and communication equipment; means for quality coding of messages of a short-time value; technical systems for motion detection, telephone tapping; night surveillance, constant following and supervision of movement routes; weapons for temporarily disabling and extraction of secret information and data; machines and tools for fabrication of special purpose weapons, and databases and information systems for a variety of information, including GIS and satellite images, which are easily accessible via the Internet (Kulišić, 2008, pp. 225-226).

2 Official Gazette of the RS No. 15/2009, 54/2010 and 4/2011.

It should be noted that the control and management of distribution of electricity, water and heating, air transport, railways, telecommunications and public services, are largely related to the systems whose information are interconnected through the Internet. This "Critical Information Infrastructure" - CII) represents a "critical infrastructure within the critical infrastructure". Targeted entry of software intended for the interruption of computers' work (viruses, Trojan horse viruses) into the systems that process information of critical infrastructure, is realistically feasible and possible. Due to a high degree of dependence of critical infrastructure of CII, a sabotage of internal information system may have long-term consequences for the "physical" infrastructure and it may inflict greater damage to the functioning of critical infrastructure facilities from those that could, for example cause placing explosives in the plants. The risk of these types of attacks on critical infrastructure resources in the peacetime may come primarily from the holders of organised crime and hacker networks, but also from the terrorist organizations, including those sponsored by the state structures of certain countries.

2.3. Protection of critical infrastructure facilities

Critical infrastructure must be specially protected and it is essential to ensure its normal operation, since one of the most difficult disorders that can happen is so called chain reaction, which transmits to other systems, multiplying the consequences. The result of series of disturbances within the systems mentioned is in theory described as the effect of a cascade or domino effect. For these reasons the main task of management of critical infrastructure is the prevention or reduction of the probability of occurrence of natural or man-induced incentives that could lead to catastrophic disturbances in the protected systems (Matika, 2009, p. 54).

The process of European integration, among other things, also requires the establishment of connectivity and interoperability between the regional infrastructure and the infrastructure of the EU as a whole. In this regard, special emphasis is placed on critical infrastructure as the holder of stability of economic development and social relations, and due to that reason the recommendations and legal framework for the protection of these resources are becoming a necessity in national development programs (Kljajić, Mandžuka, Škorput, 2010, p. 78).

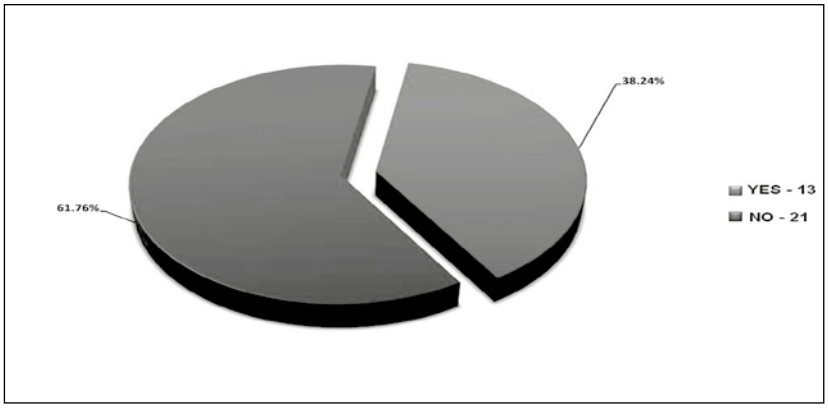
Having in mind a seriousness of consequences of jeopardizing the "key infrastructure", in literature there are the efforts made to apply an integrated model of corporate security in their protection, leaving some less sensitive functions (physical and technical security) of that system to the external, specialized service providers in that area (outsourcing). This integrated model in the systems of Critical Infrastructure could, when the functions (which may be the subject of outsourcing) of corporate security are exempted, according to some suggestions, include: a head security manager and operational security managers that are subordinated to him/her; an organizational unit for security and protection (the protection of natural, industrial, transport and other disasters, the protection of persons, confidential information and business secrets, the protection of information and archives, the protection of electronic communications, the protection of patents, stamps and reputation of corporation, fire-protection and the protection from hazardous materials and protection at work); an organizational unit for safety of documents; an organizational unit for informatics protection; an organizational unit for operational actions; a security control centre (Vršec, 2011, pp. 59-60).

In the case of corporate security in the critical infrastructure facilities in the Republic of Serbia, these jobs in practice are still performed by the former security services in public enterprises, which, during the 1990s passed through the privatization processes and became independent companies for provision of security services. That refers to the public enterprises in the area of energy, waterpower engineering, postal services, telecommunications and railways. Other Critical Infrastructure in Serbia (health institutions, airports, river harbours, water supply pipeline and similar) is secured in a combined way – by their own internal security services and by engagement of members of the private companies from that domain. As the most important problems in corporate security of the key infrastructure we can mention numerous cases of organized and major economic crime and corruption with some public enterprises involved, factual non-existence of their protection and security through public-private partnership (making a difference to the time of communism, the absence of operational cooperation of the subjects of corporate security with the police and intelligence-security services), and drastically politicized management in this area (Davidović, Kešetović, Pavičević, 2011, pp. 207-208).

We should have in mind that the management of critical infrastructure demands relatively high investments in both system maintenance and in the appropriate analytical data bases and information systems. On the other hand, the majority of contemporary strategies for investments and decision making at both public and private sectors mainly focus on one type of infrastructure or to one building as well as up to a certain extent on the significant differences in the aims of the infrastructure owners and operators, comprising a direct impact on the volume and amount of investments in critical infrastructure in particular sectors. Besides that, in practice there is a significant difference whether the investing in infrastructure is conducted by the private sector of state bodies, in fact the local administration bodies. In private sector only justifiable investments are conducted, in fact investment are being performed only if the goal is to keep the existing clients, the expansion of the market and of the number of the existing clients or benefit for stockholders, with a certain risk that the investment will not be worthwhile. Oppositely, state and local administration must provide services to all citizens, even if it is not financially profitable. In this regard, it is not that only the public services must be realized, but also, it is a special challenge for the government to keep the rates of taxes low, as well as the expenses of services. Special feature of the most of infrastructure advancements is that the investment period is between 15 and up to 30 years, so that not only the support of the local electorate is required but also finding the appropriate mechanisms of financing that include public and private associating, public funds, and also privatization of individual infrastructure systems and objects. Certain models of investing into critical infrastructure have led to the situation that making decisions about the investments into public and private sectors are being realized on project-by-project principle, in which way a segmentation of financial sources between different levels in the government and between organizations in private sectors is being conducted (Bojović, Knežević, Macura, Milenković, 2010, pp. 29-30).

In 2011, regarding the above mentioned problems on the territory of the Republic of Serbia, D. Trivan, within the framework of his PhD thesis, conducted an empirical research in the form of an expert's interview with an aim to describe and explain the level of influence which, by performing of function of corporate security, was being realized on various areas of the national security and on the grounds of collected and analyzed data and expressed value statements and assessments of the directors/managers who manage the security jobs

in corporations in Serbia, as well as the experts from the national security services (BIA and VBA). One of questions in the interview referred to the role of corporate security in the protection of critical infrastructure system in Serbia (see Scheme 1): "Do you consider that the existing level of self-protective actions in big technical and technologic systems and other mandatory secured business entities represent a sufficient protection of various external and internal jeopardizing activities?"



Scheme 1: Assessment of the level of self-protective actions in the critical infrastructure facilities in Serbia (Source: Trivan, 2011)

The answers of participants of the empirical research have shown that the level of self-protective actions in Serbia are relatively satisfactory in big technical and technological systems (primarily in "Naftna industrija Srbije" (Serbian Oil Industry), whereas in other mandatory secured business entities the situation is significantly worse and it requires organizational and other changes.

3. CONCLUSION

Corporate security represents one of the basic criteria for realization of economic goals and bringing of economic measures for crisis situation and it constitutes an important segment of economic politics at the national level. Corporate security, among other things, contributes to the energy security of the state, which includes divergent supply directions, the stability of delivery and production of energy-generating products, the creation of necessary autonomy and the strengthening of regional position in supplying with energy-generating products and other products. One of corporate security goals is that corporations, in accordance with their possibilities, support the defence and security preparations at national level, and in case of endangering the state security, help ensure the needs of the population and provide logistical support to the key agencies in the national security system. In order to have these measures undertaken timely, it is important to harmonize the existing regulations and to bring new regulations which would affect the operation of the state in response to different situations.

One of the consequences of the actual global economic crisis is absolute and relative decrease of investments in corporate security, what is present with the most of the companies in the countries of the South-Eastern Europe. Lowering of the internal protection

level makes corporation vulnerable to internal and external security threats and to jeopardizing influences, which especially refers to various types of crime and corruption. In that regard, it is also necessary, under the conditions of a global economic crisis, to invest one part of the profit of corporations which operate in this area into the establishment and advancement of corporate security system, since it is the function that represents a significant support to the business success of companies. This refers especially to the protection of critical infrastructure, information technology protection area, as well as to the security education of employees.

The application of concept of Outsourcing may also represent a solid basis for a successful protection of critical infrastructure capacity and usage of secondary resources in its securing. In that regard, it is considered that the non-state sector does not represent a competition to the state and to its security services, but that the private and corporate security is an expression of needs that in cooperation with the state institutions at national level, personal and property safety is improved. The fact is that the non-state and especially the private security sector have become a significant commercial activity which realizes the profit, employs high number of workers, and in Serbia it is liable for almost 80% of property.[3] Also, it is generally known that in the non-state sector researching, the development and application of the most modern technologies have been concentrated in the area of security and protection. By further development and improvement of overall resources – technical, human, institutional, at all levels and in all spheres of protection, the state guards one of its most important public interests – the protection of critical infrastructure.

3 At the end of 2008, the Institute for Standardization of the Republic of Serbia, passed a national standard of private security services (SRPS. A.L. 2.000, 2008, Društvena bezbednost – Usluge privatnog obezbeđenja (Social Security – Private Security Services)), which may significantly contribute to the efficient market control of quality of security services at the market.

REFERENCES

1. Bojović, N.; Knežević, N.; Macura, D.; Milenković, M. (2010). Model upravljanja kritičnom infrastrukturom za održivi razvoj poštanskog sektora. *XXVIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2010* (str. 25-30). Beograd: Saobraćajni fakultet Univerziteta u Beogradu.
2. Cemerin, D. (2007). *Kritična infrastruktura – objekt i sredstvo: kako se štitimo od klatastrofa*. Zagreb: Državna uprava za zaštitu i spašavanje.
3. Cvrtila, V. (2009). Strukturalna geopolitika i zaštita kritične infrastrukture. U: Krajcar, S. (ur.) *Energetska sigurnost i kritična infrastruktura* (str. 14-24). Zagreb: Fakultet elektrotehnike i računarstva.
4. Čaleta, D. (2011). A Comprehensive Approach to the Management of Risks Related to the Protection of Critical Infrastructure: Public-Private Partnership. In: Čaleta, D., & Shemella, P. (eds.) *Counter-Terrorism Challenges Regarding the Processes of Critical Infrastructure Protection* (pp. 15-26). Ljubljana-Monterey CA: Institute for Corporative Security Studies (ICS) & Center for Civil-Military Relations.
5. Davidović, D.; Kešetović, Ž.; Pavičević, O. (2011). National Critical Infrastructure Protection: The Role of Private Security. In: Čaleta D. & Shemella P. (eds), *Counter-Terrorism Challenges Regarding the Processes of Critical Infrastructure Protection* (pp.201-210). Ljubljana-Monterey CA: Institute for Corporative Security Studies (ICS) & Center for Civil-Military Relations.
6. Gačić, J.; Šećerov, P. (2012). Resursi Republike Srbije u zaštiti kritične infrastrukture od terorističkih pretnji. *Bezbednost*, Vol. LIV, broj 3 (str. 160-178). Berograd: MUP Republike Srbije.
7. Ivandić Vidović, D.; Karlović, L.; Ostojić, A. (2011). *Korporativna sigurnost*, Zagreb: Udruga hrvatskih menadžera sigurnosti – UHMS.
8. Kljajić, Z.; Mandžuka, S.; Škorput, P. (2010). Primjena ICT-a u upravljanju kritičnom infrastrukturom u tranzicijskim zemljama. *18. Telekomunikacioni forum TELFOR 2010* (str. 75-78). Beograd: Društvo za telekomunikacije – DT & Elektrotehnički fakultet Univerziteta u Beogradu.
9. Kovacich, L.G., Halibozek, E.P. (2002). *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program*. Boston: Butterworth Heinemann.
10. Kulišić, D. (2008). Mjere sigurnosti od terorističkih i inih zlonamjernih ugroza kritične infrastrukture (I dio). U: *Sigurnost*, Vol. 50, No. 3 (str. 201-226). Zagreb: Zavod za istraživanje i razvoj sigurnosti.
11. Matika, D. (2009). Energetska sigurnost i kritična infrastruktura – pregled rezultata istraživanja. U: Krajcar, S. (ured.) *Energetska sigurnost i kritična infrastruktura* (str. 45-55). Zagreb: Fakultet elektrotehnike i računarstva.
12. Murray, T.; McKim, E. (2000). *The policy issues in policing and private security*. Ottawa: Canadian Association of Ciefs of Police Publication.

13. Radvanovsky, R. (2010). *Critical Infrastructure - Homeland Security and Emergency Preparedness*. New York*:* Taylor & Francis Group.
14. Rinaldi, M.S.; Peerenboom, P.J.; Kelly, K.T. (2001). Complex Networks – Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. In: *IEEE Control Systems Magazine* (pp. 11-25). Ann Arbor MI: IEEE Control Systems Society.
15. Trivan, D. (2012). *Korporativna bezbednost*. Beograd: Dosije studio.
16. Vršec, M. (2011). The Role and Risks of Outsourcing in the Processes of Providing Corporate Security in Critical Infrastructure. In: Čaleta D. & Shemella P. (eds), *Counter-Terrorism Challenges Regarding the Processes of Critical Infrastructure Protection* (pp. 47-68). Ljubljana-Monterey CA: Institute for Corporative Security Studies (ICS) & Center for Civil-Military Relations.

UDC 726.9:75.041.5
ID 176374796

Ivica Đorđević, Zoran Pavlović
University of Belgrade, Faculty of Security Studies
ivicadj@fb.bg.ac.rs
zorpav55@yahoo.com

CRITICAL INFRASTRUCTURE PROTECTION IN HUMAN SECURITY CONCEPT

Abstract: Critical Infrastructure is mainly considered in the literature in the context of functioning of the economy, i.e. the state in a state of emergency. Modern trends in this area are going towards reviewing a new context of social environment. New approaches related to contemporary threats and risks to which people are exposed in their daily activities suggest the need to extend the content of the concept. Classic military and infrastructure elements that are necessary for the functioning of the economy and maintaining the functionality of the administrative system must be viewed in the context of the state of affairs prior to the occurrence of extraordinary circumstances. Some areas that are important for the functioning of the system and before the unexpected circumstances also deserve the epithet critical infrastructure. Preparing the population for functioning in the conditions of disruption of daily routine requires the proper role of the social and educational structures. In this context, we talk about the growing importance of preventive action sooner than about the act of eliminating the consequences of realized risk. In the mentioned context, the paper presents the analyses of seven dimensions of human security by the UNDP methodology. Within each dimension there are significant elements of the system that can be attributed to the concept of critical infrastructure.

Economic system and the distribution of the achieved work results can be an important source of threat to critical infrastructure, but in certain conditions also its additional system of protection. Nutrition and food safety control, as well as the functioning of the health care system may also have a dual role. The struggle against criminal activities, building team spirit and preserving cultural heritage contributes to the stability of the system and the efficiency of its protection. Civilian control of performing a public function is crucial to the stability of the community, and therefore its protection from all forms of threats. If any of the above dimensions is ignored, there is a disturbance in the functioning of the system and the resulting consequences that are difficult to repair. Ignoring a holistic approach in terms of globalization of all aspects of human life and activities can be a source of problems, not only in the communities where the problem appears first, but also on the entire planet. Comprehensive knowledge of these facts is a prerequisite for the survival of civilization as we know it.

Keywords: *human security, critical infrastructure, prevention, early warning systems.*

1. INTRODUCTION

We live in a world that is loaded with many contradictions. Differences between the rich and the poor, both locally and globally, are a significant source of risks and threats to the security of people and the system. In addition to further emphasizing the mentioned problem of difference, the ruling economic paradigm contributes to the devastation of the environment, endangering the survival of life on Earth. Ideological fundamentalism based

on neo-conservatism as a model for the structure of human activities prioritizes the implementation of the principle of the free hand of the market in all areas of human endeavour. The results of the current implementation of the said principles lead to the fact that the system becomes increasingly unstable due to the tightening of the contradictions that are built into its foundations. Economists explain the cyclic repetition of the crisis with the nature of economic processes. While one school of economics says that we should intervene in the process in order to reduce fluctuations, other economists are against it. We forget the fact that the greatest accomplishments and prosperity were achieved at the time when the state used its mechanism of influence to reduce the amplitude of the oscillating waves of business. The period after the Second World War was burdened with the so called Cold War and the threat of nuclear holocaust, but, in effect, there was a system of social care and the protection of workers' rights within the boundaries of Western Europe and the United States, which allowed a more equitable distribution of the national product. After the implosion of the Eastern bloc and the collapse of the ideological opponent, the system in the West develops very disturbing characteristics. What is collectively called the welfare state is offered on the altar of orthodox CAPITALISM for the sake of profit maximization. The withdrawal of the state from economic trends results in a crisis which in its effects is compared with the Great Depression of 1929. Interestingly, the emergence of the crisis of which we are contemporaries, among other things, comes as a result of the abolition of laws enacted after 1929 in order to prevent the occurrence of similar crises.

Historical dimensions given in this introduction are necessary so that we can explain the thesis of the necessity of change of approach to contemporary problems of humanity. Insisting on territorial and institutional security without having to worry about individuals leads to even bigger problems and may increase the probability of risks that are commonly referred to in the analysis of the vulnerability of critical infrastructure. In this context, the concept of human security offers an analytical framework for comprehensive troubleshooting the security problems of modern civilization, regardless of cultural differences. It is an undeniable fact that through the protection of critical infrastructure the level of security of the citizens also raises. The problem may occur only in regards to priorities of protection and the timeline of events and measures to be taken to protect critical infrastructure.

2. BASIC THEORETICAL FEATURES OF THE CONCEPT OF HUMAN SECURITY

The concept of human security as an alternative view of the security issues of the contemporary world appears for the first time in the 1994 UNDP Human Development Report (UNDP, 1994). To understand the essence of the ideas and motives of its authors, one should bear in mind the historical conditions in which it develops. The fall of the Berlin Wall and collapse of the Soviet Union and the Eastern Bloc release intellectual energy that in the past dealt with Armageddon scenarios and the nuclear holocaust threats as a result of permanent tension and the destructive potential of the two great superpowers. The concept itself has its roots in the period of the Enlightenment and the centuries-old tradition of struggle for human rights formalized in declarations and conventions of international organizations.

What is particularly important in this context is the process of globalization that gets its full importance along with the process of opening previously inaccessible areas to the

capitalist business network and the system that literally becomes global. The exceptions in the form of islands - North Korea and Cuba, or mixed economies of China do not reduce the global reach of transnational capital that meets its global ambitions even in this region. Globalization opens a new issue that comes as a result of the imposition of globalism based on a neo-conservative organization of economic and social activities that favours the market as the only corrective mechanism. Minimizing the role of the state and its institutions leads to the domination of the profit centres of power and their interests in relation to the citizens and communities they belong to. Global capital is no more in need for national institutions; instead they are made instrumental to realization of its interests. The effects of the described process are the devastation of the achievements of the welfare state in the West and the huge number of the poor and underprivileged people in the east. The process of transition based on the principles of the Washington Consensus leads to the catastrophic situation in the countries in transition. Many people lose their source of income and experience a total disappointment in the system of which they dreamed when they were in the so called communism and socialism. At the same time, in the third world countries that enjoyed some sort of security due to the former balance of power the processes that cause instability and change of the local rulers occur to empower the structures that act in compliance with the will of transnational capital (Djordjević, 2007).

Recognizing the consequences of the described process, the UNDP analysts realize that global problems arise that threaten the security of citizens regardless of their ethnic, religious or other affiliation. Wanting to draw attention to the concerns of citizens in an emerging global society, the authors of the UNDP report offer an analytical framework called human security, by which they highlight the difference relative to the previously dominant approach based on a national or state security. The human in the name caused a lot of controversy in the academic community and the lay public, but the idea was to emphasize the qualitative difference in approach: man versus territory and institutions. It is not superfluous to emphasize that the new approach is not necessarily in collision with the old. Where the institutions of the system are in accordance with the interests of the citizens, national security is almost identical with what is meant by human security. Unfortunately, there are far more states whose institutions are at the service of informal power centres, completely alienated from the people whose interests they should promote and that there is a qualitative difference between what is proclaimed the imperative of security in one, and the other approach.

The concept of human security, as shown in the UNDP Human Development Report of 1994, is not linked only to the resultant state of affairs, but also includes those things that lead to a state of insecurity. The essence of the new approach to security promoted by the UN is best illustrated in the following quote: "To most people, the sense of insecurity comes more from everyday concerns than the fear of cataclysmic world events. Will they and their families have enough to eat? Will they lose their job? Will they be coerced by the repressive state? Will they become victims of violence because of their affiliations? Will they be a target of persecution because of their religious or ethnic background? ... In the final analysis, human security is a child who did not die, an infectious disease that has not spread, a job that is not taken away, an ethnic tension that did not explode in violence, a dissident who was not silenced. Human security is not an issue of arms - it is the issue pertaining to human life and dignity" (UNDP, 1994).

The concept of human security links direct threats to acquired values to subjective fears for their violation. Safety is associated with the lack of danger such as hunger, disease, crime, repression and sudden adverse changes in patterns of daily life (at work, at home, in the community or the natural environment).

The authors of the Human Development Report for 1994 state the following seven areas of importance for the determination of the security and insecurity in some areas (UNDP, 1994):

1.	Economic security,	5.	Personal security,
2.	Food security,	6.	Community Security, and
3.	Health Security,	7.	Political security.
4.	Ecological security,		

This analytical seven-dimensional framework allows for the quantitative analysis of security in an area and taking preventive action to avoid the realization of risks resulting from poor conditions. The special importance of the concept of human security lies in the fact that it draws attention to the real problems of modern civilization, and the place of man in the current socio-economic environment.

3 EXTENSION OF CRITICAL INFRASTRUCTURE TERM CONTENT

For the analysis of the links between the concept of human security and critical infrastructure we take the definitions which are two dominant directions in relation to critical infrastructure:

- "Critical infrastructures are organizations and institutions that are important to public welfare; such that failure or disruption of them will result in long-lasting supply bottlenecks, significant disturbances in public security or have other dramatic consequences" (Federal OfIS, 2004).
- "Critical infrastructure is the backbone of our nation's economy, security and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on to stay in touch with friends and family. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (DHS, 2013).

As can be seen from the enclosed definitions, the critical infrastructure presumes systems considered of particular importance for the functioning of public services and the preservation of security of the community. In view of the above presented concepts no objection can be made in terms of human security. However, it often happens in practice that the protection and the functioning of the system are too emphasized whereas less attention is paid to an individual. Certainly there are times when the system is essential to minimize the consequences of any emergencies and to avoid the increasing the number of victims, but it is not acceptable that any steps contrary to the interests of citizens be undertaken in situations in which it is not necessary. Bearing in mind the said seven dimensions of human security we will try to make a parallel with the concept of critical infrastructure protection within each of them. The analysis is

based on the previously mentioned sources: German Federal Office for Information Security and the USA Department of Homeland Security.

Table 1: Critical infrastructure areas in the USA and Germany
(Source: Presidential Policy Directive, USA and National Strategy for Critical Infrastructure Protection, GER 2013)

No.	USA	No.	GER
1.	Chemical	1.	Technical basic infrastructure
		1.1	Power supply
2.	Commercial Facilities	1.2	Information and communications technology
3.	Communications	1.3	Transportation
4.	Critical Manufacturing	1.4	(Drinking-) water supply and sewage disposal
5.	Dams	2.	Socio-economic services infrastructure
		2.1.	Public health; food
6.	Defence Industrial Base	2.2.	Emergency and rescue services; disaster control and management
7.	Emergency Services	2.3.	Parliament; government; public administration; law enforcement agencies
8.	Energy	2.4.	Finance; insurance business
9.	Financial Services	2.5.	Media and cultural objects (cultural heritage items)
10.	Food and Agriculture		
11.	Government Facilities		
12.	Healthcare and Public Health		
13.	Information Technology		
14.	Nuclear Reactors, Materials, and Waste		
15.	Transportation Systems		
16.	Water and Wastewater Systems		

From the above table, the reader may notice that the number of areas of critical infrastructure on the Internet site of the Ministry of Internal Affairs of Germany is smaller relative to the US approach. However, with careful analysis it can be seen that more or less the same areas or sectors of critical infrastructure are included in either source and that it is only a matter of methodological approach and their grouping. From the above two cases, one can see the difference in the approach to ranking priorities in critical infrastructure.

The US dominated by military logic is oriented towards sector bodies which are essential for the defensive actions in relation to the potential threat from the outside. The German approach shows that it is a society which puts emphasis on social solidarity and systems to allow for the normal functioning of the community in exceptional circumstances. One should not lose sight of the fact that in Germany the possible war scenarios are taken into account, too. Given the low probability of their realization they are not represented in public but are probably part of the plans that every serious country keeps as military secrets or otherwise prevents their appearance in public.

3.1. Economic Security

As we can see from the table, the financial and economic system is included in critical infrastructure. Serious disturbance in the area of financial management can destabilize the system and bring about economic collapse. In addition to the fact that macroeconomic stability is in jeopardy at the subject of economy level, that is on the level of companies and citizens, this may be a threat to their existence. The status of the global economic system becomes a reflection of the problems of the current civilization model based on neoconservative principles of operation. Individual citizens are left to the mercy of the effects of the action of market laws in the United States whereas in Germany, economic dynamics is maintained even in the circumstances of the deepest crises of other capitalist countries owing to the social market economy. In this context, it is not without reason that the part: socio-economic services infrastructure makes a special section, because to the individuals who are in existential crisis a far more important issue is how they can overcome the crisis on the personal - existential level than to what extent and how many banks are saved from destruction.

The protection of the economic system ensures the functioning of the state and of course, to some extent, contributes to the protection of citizens. What planners and policy makers need to take into consideration are the elements of the analysis that would indicate possible instability even before the crisis is manifested in its worst form. There is a trend to simplify economic processes and reduce them to statistics on the level of GDP (or, more recently GNI) and its trends. The fact that there is growth in the volume of economic activity in an area does not mean there is growth of standard of living. The qualitative analysis of the process may reveal that the growth of statistical indicators results from a higher degree of exploitation of labour, that the standards in the protection of the living environment are lower, and so on. If the above case is in question, the long-term economic growth gives adverse effects, and it may happen that its effects are detrimental for the citizens who live in a certain area. After a while the observed area may result in social instability that could hypothetically lead to the eruption of discontent and revolutionary developments.

Ignoring the grey economy is not only linked with the issue of efficiency in tax collection, but also points to the deeper social problems with corruption and functioning of the system. Inability to control and the taxation of economic activity leads to the problems in collecting revenue. The lack of money in the budget affects the stability of institutions and effectiveness of the system, which entails lower costs for the social and health systems, leaving many people out of social and health care. People who find themselves out of the system and are left to themselves, become offenders by force of circumstances, which leads to the issue of sustainability of the community. In such circumstances, the state is not able to provide any funds to carry out basic activities but is forced to borrow; which

in turn leads to the growth of the public spending in relation to the registered total spending, there is a budget deficit and growing public debt, which inevitably leads to higher inflation. This situation is very common in the former Third World countries or transition economies. Because of all this it is not enough just to pay attention to the financial infrastructure. It takes a far more comprehensive approach to the issue in order to act preemptively to maintain system stability and state institutions. In addition to traditional economic indicators in the analysis of the security of people in an area, it is necessary to take into account: cost of living index, poverty index, percentage of households that have at least one member whose income is sufficient to meet the needs of the household in relation to the total number of households with at least one employed member, the percentage of households with incomes below the poverty level and percentage of those who feel economically insecure (in terms of employment and income stability). By taking into consideration the indicators on the status of human security in the economic field the causes of many of the crises could be timely rectified (Djordjević, 2013; UNDP, 1994).

3.2. Food Security

Food chain from production to processing to distribution is a significant part of the critical infrastructure. From the fact that the lack of basic food items is a nightmare to those in power, to the fact that every link in the above-mentioned chain must be monitored in order to guarantee the quality and health safety of foods that people use. Given the increased volume flow of goods across national borders, it is increasingly difficult to perform quality control of food products on the market. The affairs that emerge due to inadequate quality of meat products and fresh meat are frequent. The differences in shelf life standards is misused in the way that the goods is shifted from a market where it is at the end of its shelf life to a market where standards are not as rigorous. In the security context the topic of food security is a strategic issue because it links with other important aspects of the functioning of the system. Poor state of agriculture and the food industry affects the quality of life, burdens health funds, and reduces the efficiency of the economy. The problem becomes particularly important with the intensification of global economic activities and liberalization of food markets. There is a risk of traffic of foods contaminated with various pathogens increases. The imposition of GM crops as a solution to the problem of feeding the population carries many risks. Small and underdeveloped countries do not have enough power to deal with blackmail and influence of TNCs that enforce their GMO patents throwing out native species from the food chain.

Getting the right perspective of the situation in the field of nutrition requires a qualitative analysis that, in addition to classical indicators in this area, should include: food and energy value of average daily servings of residents and their deviation from the recommended value; the percentage of children with low birth weight and height for a given age; the effects of risk factors (insufficient quantities of vegetables and fruits) in premature mortality and the impact of diseases and injuries on the society; the percentage of physically, chemically, and microbiologically contaminated samples of fresh/processed food, and general use items; and citizens' opinions of the quality of the food (Djordjević, 2013; UNDP, 1994).

3.3. Safety of Health

It is difficult to separate the health status of a population from other dimensions of human security. However, the authors report on human development want to draw attention to the importance of health infrastructure for citizens' safety. When it comes to this area, it should be kept in mind that it is a reflection of economic conditions, but at the same time that its status has a significant impact on the economic system of analyzed space.

The concept of human security emphasizes the qualitative analysis of statistical indicators that are commonly available in the annual status reports regarding a certain area. For example, population growth is an important indicator of the vitality of the people who live in a certain area. Based on this information, we can extrapolate trends. Negative birth rate indicates the unsustainability of the system and failures in population policy of a certain country. But information data on births and deaths should be cross-referenced with the information such as life expectancy and the main causes of premature mortality, maternal mortality rate, infant mortality rate per 1,000 live births, the number of cases of infectious diseases and the percentage of the population vaccinated. Only on the basis of these data, we can have an insight into the true state of the health system in a particular area. The depth of the analysis would be contributed to by the data about the diseases and injuries of the population, the acquired knowledge about infections, the degree of work disability, to what degree are health services conditioned by the financial status of the citizens, the "hidden" costs of treatment (transport, the lack of medicines in the public sector, forcing the citizens to seek medical care in private hospitals, bribery), the existence of discrimination in the provision of medical services, violation of the right to health and the ethical principles of health policy, and citizens' views about the quality of health services (Djordjević, 2013; UNDP, 1994).

3.4. Environmental Safety

Ecological security can be compromised during various emergencies, technological accidents and natural disasters. However, a life environment can also be under a threat due to systemic deficiencies in the control of economic activities and inadequate attitude of institutions towards the sources of pollution such as waste disposal, wastewater treatment and air pollution. Long-term consequences of system failure can be worse than the results of accidental situations and natural disasters. Because of the impact on the health of the citizens, it is very important to monitor the indicators that give a more realistic picture of the ecology of a particular area. In addition to the analysis of official statistics, it is necessary to take into account the information such as:

- The legal framework for access to information on the state of the environment;
- The percentage of newly constructed buildings with the analysis of the environmental impact made prior to their construction (relative to the total number of newly constructed buildings);
- Citizens' views on the degree of endangerment of adequate protective measures relating to the environment;
- The existence of a cadastre of air pollutants;
- The number of patients with respiratory disease and the correlation with the percentage of households using coal as an energy source;

- The quantity of treated wastewater (% of total quantity), the availability of safe drinking water and the number of patients suffering from diseases caused by contaminated water;
- The percentage of arable land affected by erosion caused by human activities and natural processes, reducing agricultural land due to change of land designation;
- The percentage of waste recycled and status of landfills;
- The percentage of protected plant and animal species relative to their total number;
- The percentage (and causes) of deforestation relative to the total area under forest.

When the analysis is made on the basis of these parameters, then the development of the strategy for the elimination of the causes of the poor state of the living environment ensues.

The state of the environment is one of the greatest contemporary security challenges. Unacceptable living conditions that arise as a result of climate change and over-exploitation of forests and other natural resources can be a cause of migration to more developed regions. Large migratory pressure leads to changes in the structure of local population, its absorption potential is exceeded, which leads to endangering the safety of local population (Djordjević, 2013; UNDP, 1994).

3.5. Personal Security

Personal security of citizens means an objective state of security at the individual level but also a subjective perception of this state (safety). The fundamental difference that exists in some situations between the national (state) and human security can come through at this level of security. The state as an entity can be safe with respect to threats from inside and outside, but citizens can be threatened by local gangs or a source of pollution in their immediate environment. All the dimensions of human security, from the economic situation to the functioning of the institutions, retract through the prism of personal safety. The poor economic situation threatens the citizens on their existential level, in addition it leads to a higher crime rate, and civil servants are more vulnerable to corruption, so the funds for health and education in the budget are lower. The politicians in the poor and underdeveloped countries team up with big business, and often criminal organizations, which leads to the problems in the functioning of the judicial system. There are cases where the legislation is in the interest of the informal centres of power which directly affects the state of personal security. The information about the situation in this area we get through indicators such as:

- The percentage of reported crimes that end up with final judgment;
- The number of reported crimes committed by unidentified perpetrators, and the estimated number of unreported crimes ("the dark number");
- The assessment of daily consumption of narcotics relative to the amount of narcotics seized, and an assessment of the ratio of number of registered drug dealers and sentences for drug-trafficking offenses;
- The spreading of types of anti-social behaviour (prostitution, gambling, gangs, incidents at sports events, begging) and the number of criminal charges for the offenses related to anti-social behaviour;
- The degree of confidence in the police and judicial authorities;
- The percentage of people who feel unsafe from crime risk;

- Attitudes about: the prevalence of juvenile delinquency and the threat of it; the corruption in the public sector; the prevalence of organized crime and the threat of it; the prevalence of human trafficking and the threat of it; citizens' attitudes about the prevalence of anti-social behaviour and the threat of it.

As can be seen, citizens' perception in terms of their status and subjective perception of security that can only be obtained through the appropriate research in the field in direct contact with people is very important in this segment of the analysis of human security. We should be somewhat suspicious towards the official statistics in this field because it is not uncommon for the authorities to conceal the true state of affairs (Djordjević, 2013; UNDP, 1994).

3.6. Community Security

When it comes to the security of community, in addition to all these elements based on which we assess the state of security at the individual level, the elements of analysis indicating a wider context are introduced. The elements such as the appearance of compromising the security of minority groups, and events that affect the character of the whole community are taken into account. Domestic violence and mechanisms to combat it are good indicators of the stability of a community because domestic violence is not an issue only on the level of family members' relations but it gets a wider context due to its consequences. Housing conditions also affect the social environment in which young people are growing up and on which the conditions in the community depend in a later stage. Independence of the media and their role in the analysis of socially unacceptable phenomena, the motivation of citizens to participate in local government and their views regarding the solutions to common needs, the perception of communal utilities performance and the cooperation with the police, the attitudes toward labour unions and non-governmental organizations, all the above listed elements provide a cumulative view of the situation in a particular community. There is a number of factors not mentioned here, that can be analyzed such as confessional and national structures, the historical context of modern relations, geopolitical position, etc. Limited space does not allow for listing all the elements of analysis. The readers can get further information on the concept of human security and all its dimensions using the attached list of references.

3.7. Political and institutional security

Citizens should exercise their rights through state institutions that are controlled by their elected representatives. That is the theory, anyway. Because there is a large gap between the theory and practice, the following elements should be taken into account when analyzing in order to get a complete picture of the functioning of the political system:

- The adequacy of regulations governing the field of establishment and the operation of political parties; the existence of regulations that prohibit the establishment and the operation of political parties the program and activities of which endanger the constitutional order; the existence of legislation prohibiting minors to join political parties;
- The existence of legislation prohibiting the party organization in the state bodies;
- The adequacy of regulations governing the electoral process to ensure its regularity;
- The equality in media coverage of political parties during the election campaign;

- The trends in voters turnout by the type of election;
- The citizens' attitudes about the regularity of electoral process;
- The institutionalization of the division of powers and judicial independence from political influence;
- Minimizing the benefits from party membership, and the efficiency of administrative system;
- Civilian Control of the Military;
- Professionalization of the police (Djordjević, 2013; UNDP, 1994).

4. CONCLUSION

From all this we can conclude that the issue of critical infrastructure must not be simplified and reduced to the elements of the system that are relevant to the macroeconomic processes and activities that enable the work of institutions of the system in emergency conditions. It is very likely that cases of threatening the primary target will occur if the strategy in this area is based only on ensuring the continuity of institutions and the protection of the territory because it does not take into account the needs of the citizens . There are a lot of examples from practice like the rescue of the banking sector in the United States after the crisis of 2008 that cost the state tens of billions of dollars while on the personal level it was allowed that many people remain homeless because they could not repay mortgages. The citizens paid the cost for the consequences of banking speculations that undermined the foundations of the system. This sends the message that the state does not care about individuals but about the interests of big business. The connection between the institutions and the citizens breaks, which is best manifested in the level of turnout in elections.

If the institutions of the system are not in the interest of citizens, it undermines the main principles of the democratic system and leads to long-term instrumentation of the institutions for the sake of big business. The domination of interests of the profit centres can lead to the loss of sense of common interest of the citizens who live in a certain area. This is partly an explanation of why there is no adequate response to the process of global warming, the global network of organized crime, and why problems with terrorism and infectious diseases that were once eliminated occur again.

The education system is one of the most important elements of the critical infrastructure. The future of humanity depends on it. Unfortunately, there is no room for educational system in the list of elements of critical infrastructure. Young generations are deprived of a large amount of knowledge that is essential for the understanding of the functioning of modern world and the responsibilities of individuals in this process. The consequences of current processes are evident in both the developed and underdeveloped countries. Our region is particularly paying a high price for retrograde processes of market laws glorification. The analytical framework that the concept of human security offers could help perceive the depth of problems the modern civilization and all the people on Earth are faced with, regardless of their religious, ethnic or other affiliation.

4. REFERENCES

1. Department of Homeland Security (2013): *What Is Critical Infrastructure?* USA: DHS, on http://www.dhs.gov/what-critical-infrastructure (1.IX 2013).
2. Djordjević I. (2013): *Ljudska bezbednost: globalni kontekst i primena u Srbiji*, Beograd: Institut za uporedno pravo i Dosije studio.
3. Djordjević I. (2007): *Bezbednosna arhitektura u uslovima globalizacije*, Beograd: Fakultet bezbednosti – Službeni glasnik.
4. Federal Ministry of the Interior (2009): *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Bonn: Federal Republic of Germany.
5. Germany Federal Office for Information Security (2004): *Analysis of Critical Infrastructures - The ACIS methodology - (Analysis of Critical Infrastructural Sectors)*, Bonn: BSI. on: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/acis_paper_en_pdf.pdf?__blob=publicationFile (1.IX 2013).
6. Кондратьев А. (2012): „Современные тенденции в исследовании критической инфраструктуры в зарубежных странах“, Зарубежное военное обозрение №1, 2012, С.19-30.
7. The White House (2013): *Presidential Policy Directive /PPD-21- Critical Infrastructure Security and Resilience,* Washington, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (2.IX 2013.)
8. United Nations Development Programme (1994): *Human Development Report*. New York – Oxford: Oxford University Press.

UDC 726.9:75.041.5
ID 176374796

Ljubinka Katić
University of Belgrade, Faculty of Security Studies
ljkatic@gmail.com

EDUCATION AS THE CRITICAL INFRASTRUCTURE PROTECTION FACTOR

Abstract: The topic of this paper is to note the necessity of reassessment, different emphasis and interpretation of some of the critical infrastructures' aspects. Apart from particular, direct and obvious elements of critical infrastructures, which specifically involve material resources and facilities, there is a detailed exposé of new social-cultural circumstances, together with modern understanding of security, facilitating inclusion in this discourse, together with the systems and processes which are essentially non-material in nature. A wide area of education, containing a significant material component as well, becomes a dominant potential in the contemporary knowledge society, with its quality of operation to be freely considered prerequisite for the operation of other societal systems. The paper elaborates education as the critical infrastructures' protection factor, having the instrumental value, as well as the independent protection value. In the first instance, it is to contribute to security culture development for the entire population, as well as professional education for security staff and security aspect of engineering-technological staff professional education.

The author concludes that human development humanistic model, which observes the economic development as the means to achieve human goals, positions education among critical societal systems and processes. Throughout the history it was proven to be a powerful resource – not just for knowledge acquisition, but also for developing values assuring permanence of a given culture. If we are to apply the commonly used metaphor of critical infrastructure being the "bloodstream" of a society to the field of education, this field may be considered its "nervous" system, probably superseding everything else in vital significance.

Keywords: *Critical Infrastructures, Critical Criteria, Education, Protection, Education Strategy*

1. INTRODUCTION

The *critical infrastructures* phrase is probably not being associated by the majority of security experts or general public with upbringing and education. In spite of that, individuals and historical examples verifying that these complex activities are often considered to be vitally important for individual and society survival are not rare. When establishing critical criteria, if the first pillar is the essential significance of an activity or a sector for society development and survival, the upbringing and education are becoming not just an important critical infrastructure protection factor – in fact, they turn to be the essential, vital value, subject to protection.

Multi-layer terms, such as *upbringing* and *education* can be understood in confusingly various ways, which may furthermore imply very different assumptions of their roles and

functions. Their common denominator is a certain enriching and refining role, which facilitates achieving comprehensive potentials throughout all of the society stratification levels, developing common nucleus of values and increasing total volume of knowledge, skills and understanding – whether by the individual or by the society as a whole. Some of the terms, holding the most direct link with upbringing and training,[1] which are often yet inappropriately identified with those such as *schooling, training, capacitating, instructing* and similar, cover only individual dimensions of human being, i.e. they are focused on narrower, specific goals, thus contributing to the development of some dispositions or competences necessary to perform a certain function. In the comprehensive individual and societal development process, listed educational activities are not inter-exclusive, but are neither identical. Education helps understand the importance and the value of a given content or activity, creating something new from that foundation, evaluating moral justification, interiorizing values and standpoints, which even with the most efficient training does not have to hold any significance.

In most of the societies, the significance of education is being emphasized by considering it "public good and public responsibility" (*Prague Declaration:* 2001). Numerous authors elaborate various understandings of public good and public responsibility, mostly to agree on the standpoint that the education is not "pure public good" (Blaug, from Schonenberger, 2005), thus the responsibility of a society on all levels of education is not the same.[2] Nature and scope of public responsibility for education vary from state to state, but to make the common, essential characteristic of European educational heritage, even at the university level (Veber, Bergan, 2005).

Insisting on public good and public responsibility constitutes the intersection field, which encompasses the context of education and the context of critical infrastructures protection, which are also being called public infrastructure. These fundamentally economic terms designate "the goods available and enjoyed by all" (Štiglic, 2004). Principally, but not absolutely, these goods are considered non-rivalry and non-exclusive, which means that everyone may use them under identical terms. The majority of currently predominant understandings of critical infrastructures mostly include complex systems in their corpus, with functioning being prerequisite of economic, cultural and social development of all individuals, national states, and global society even, which mostly makes them the field of public interest and responsibility.

2. DILEMMAS WHEN ESTABLISHING CRITICAL ITEMS

Necessity to recognize critical infrastructure in fast changing environment implies permanent reevaluation of their existing, mostly not fully consistent, classifications and seldom definitions. The common path of development for numerous terms used in science indicates their historical property and evolution of meaning in time. The main elements of numerous phenomena and terms often exist for a long time in life *practice*, before they are constituted in theoretical system.

---

1 Hereinafter, we shall be using the term *education*, although narrower in its scope and content, mostly because in English speaking area upbringing and education are brought under the same term – education.

2 It is fascinating how long ago the discussion on public responsibility for education initiated was. Two and a half millennia ago, Aristotle, having in mind state education in Sparta and mostly private education in Athens, had written in *Politics*: "Since there is but a single goal for the entire state, therefore education must be equal for all, and the responsibility for it must be public instead of private matter, as it is today" (Politics, 1337a).

In search for *theoretical* foundation of this phrase, we note that seemingly clear formulations are becoming ambiguous, insufficiently established, even controversial. Categorization tools are still insufficiently developed in this segment of security studies. The majority of relevant papers consider material, physical objects and systems to be critical infrastructures, although rarely noting them as such. The latest definitions also involve virtual systems in the critical infrastructure corpus. Classifications, being more common than definitions of this phrase, indicate what is considered under critical infrastructures; which societal sectors are considered relevant in that sense, but the critical criteria may only be deducted in an indirect manner. The foundation is being searched and found in international legislation, the EU documents, presidential statements and directives. Administrative discourse domination is also notable in its uptake, without going into the issue, in some scientific papers.

Changes in the environment, the priorities of the given time and political reality *change the nature or the relative importance of the individual elements or sectors*, with operation considered the most important. Some of the current critical infrastructure did not exist in the past, or they had no or quite a limited range and influence, while presently marginalized fields used to be in the very focus of social attention. The example for the first statement is the fascinating history of the Internet, which had, since early 1960's up to true boom in 1990's, gone from ARPAnet American Military network with mere four nodes (Kurose, Ross, 2008, p. 59), down to the present scale, hardly even imaginable at the time. The introduction of Web applications (World Wide Web), bringing internet to the companies and homes of millions had moved the focus onto the issues of network security and indisputably qualified the Information-Communication Technologies as the critical infrastructures' segment. On the other hand, the historical facts indicate that in some societies, even in the most difficult and dangerous times of war, the provision of education had the same ranking as the provision of basic needs, such as food. The most prominent example is the ancient Athens, in its hardest period in history – long war with the Persians. Women and children of Athens, taking refuge from the city which was subsequently burned down and destroyed, had gotten refuge in allied city of Tresen, providing them, apart from food, "paid tutors for the children" (Plutarch, from: Bralic, 2006, p. 63). It is also known that the refugees were imposed "the ban to educate their children" as the most difficult penalty (Elijan, from: Bralic, 2006, p. 63). If we agree that the exceptional ancient Greek history is in fact the foundation of the entire Western civilization, it may not be prudent to forget some of its fundamental spiritual messages and lessons.[3]

The scope of critical infrastructures interpretation indicates the existence of variations, which may induce new and useful questions. A table of similarities and differences which may be established indicates various approaches in critical infrastructure determination, or in more detail – critical infrastructures in various states, by different authors and in diverse contexts. The starting points of critical infrastructures identification are also not common. Some determinations start from establishing the basic needs to be satisfied for the society to operate, determining against them which infrastructures support them and

3 In an essay by T. S. Elliot, we may find a warning, stating that apart from spatial, there is also a *temporal provincialism*, which is characteristic for those "for which the history is a mere chronicle of human inventions that had served their purpose and are being thrown in the dump". That type of provincialism is a potential danger for those who "equalize wisdom with being informed" (T. S. Eliot, *Izabrani tekstovi*, Beograd, Prosveta, 1963).

if those structures may be considered critical. The second approach firstly identifies key infrastructure in each sector, afterwards appraising the influence on the society invoked by their collapse. The third possible approach identifies the key operator in each critical sector, which then determines which infrastructures are being critical for undisturbed delivery of their services (Smedts, 2011; Hamidović, 2012; Lewis, 2006). These choices are not always relying on a single concept – rather, they use various aspects of management, resources management, capital theories, public goods, business process optimization, risk management, network theory, and various economic and social standpoints. Apart from that, there are also different contexts for considering vulnerability, sometimes as jeopardy of terroristic strikes (Colins, Baggett, 2009) or threats outside the system in general, as well as vulnerability hidden not in omissions, but in standard working circumstances and procedures or the lack thereof.

The characteristic approach to the critical infrastructures, predominant in the security studies, relies on the practice of public infrastructures protection in the USA, which is becoming the relevant point for the majority of European states. Formal and methodological principles of the CIP (Critical Infrastructure Protection) programme, promoted in the presidential statements (Clinton,[4] Bush) and the EPCIP (the European Programme for Critical Infrastructure Protection) of the European Union are the foundation of critical infrastructure protection in the Member States. The directives and suggestions of these programs are founded on administrative, rather than scientific authority. In the EPCIP, the critical infrastructures inventory had initially listed eleven sectors with 37 related services, later to be reduced to 11 sectors and 29 sub-sectors. The very Directive (2008/114/EC) from 2011 notes two sectors (energy and transport), with eight subsectors: electrical power, oil, gas, road, railroad and air traffic, followed by inland watercourse transport and seas and oceans transport (Smedts, 2011, p. 73).

Critical infrastructures register and the responsibility for their protection remains at the national level, although it is noted that they may be located on the territories of other states, and may be relevant for the security of several countries. For easier practical implementation and operative capacity of public government, this approach is sector-oriented, with listing the sectors considered relevant.

The starting point of critical infrastructure identification is therefore the existing administrative organization, instead of the needs satisfied by a sector. The application of a different principle, such as the societal needs-based approach, may bring some other segments into the focus – such as education. Arbitrary determining eleven, ten, six (Colins, Baggett, 2009) or two critical sectors already indicate the unreliability of criteria for considering individual infrastructures as critical. Critical infrastructures sectors are usually considered to be systems, networks and facilities related to the production or delivery of goods and services in the field of food, water and energy provision, followed by all types of transportation, Information-Communication Technologies, banking and finance, public government operation provision, public health care system and seldom schools (Stanarević, Ejdus, 2009, p. 61). This list is not exhaustive, and its individual elements are differently grouped or interpreted. If we would consider essential importance of the individual systems for satisfying societal (and individual) needs (Figure 1),[5] it would be obvious that the

4 Full text of presidential statement in: Brown, 2006, p. 176-190.

5 Taken from: Hamidović, 2012.

usual, predominantly technical-technological approach in critical infrastructures identification would reduce human needs by neglecting the higher level needs, which make the human society - humane.

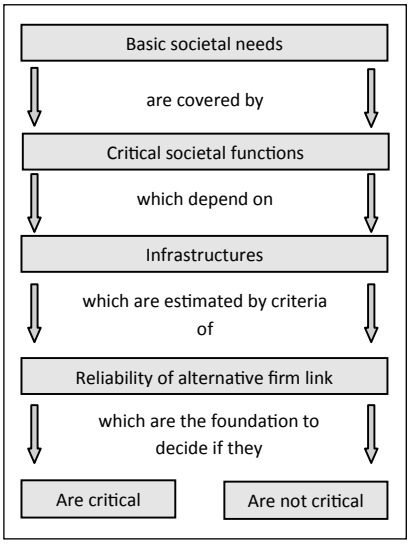


Figure 1: Critical infrastructure identification process starting from the needs (Hamidović, 2012)

Professional and dictionary references indicate the term *critical* in the context of critical infrastructures as to be indirectly interpreted as an attribute of a phenomenon or item, which indicates that its collapse would significantly weaken national security or other values, followed by the issue which cannot stand delays, as decisive characteristic, and even turnaround property. The existence of a reliable criterion, or combination thereof, in each individual case creates a foundation for decision-making on the alternatives – if it is a critical infrastructure or not. Otherwise, it remains unclear which reasons motivate the inclusion of one and exclusion of another system in the corpus of critical infrastructures.

The existing legislation of the states that had promulgated the laws on critical infrastructure rarely provides explicit qualifications. The Croatian Law on Critical Infrastructures, before listing them, for instance, stipulates: "Sectors of national critical infrastructures *may include* in particular...", instead of "*are*",[6] which indicates that the list of potential critical infrastructures is not final; that the state understands that and leaves the option for the Government "to decide upon critical infrastructures from other sectors".[7] Such formulations indicate that the legislators could not even follow clearly established European of wider practice, thus having to stipulate the obvious – that the critical infrastructures register is open.

6 (Italic: Lj. K), *Zakon o kritičnim infrastrukturama (Law on Critical Infrastructures)*, Narodne novine, Zagreb, 56/13.

7 Sector-wise approach is appended in this Law by including "national monuments and values" as an element of critical infrastructures.

There is no strategy or policy of critical infrastructures protection defined in the Republic of Serbia. There is an institutional framework, being the Sector for Emergency Situations, competent ministries and regulative bodies, however lacking the appropriate documents and legislation. Some aspects of this field are noted only in the Strategy for Information Society Development (hereinafter: the SISD), while the National Security Strategy (hereinafter: the NSS), stipulating that it is "the foundation for strategic documents development in all fields of societal life" (NSS, 2009: 3), fails to even mention this matter.

3. EDUCATIONAL DIMENSION OF PROTECTION

The complex field of education can be a relevant factor of critical infrastructures protection in several forms. Since education responds to societal and individual needs, it becomes the important fact – decisive for individuals and society development. Material or natural wealth of a country do not operate on their own as favourable or unfavourable for its development, as it might have happened in the previous phases of human history. The main leverage of development and preservation of the existing wealth is becoming intellectual and cultural, i.e. educational investment. Chances for social promotion at the individual level as well, to the greater extent than in the past, grow with the educational level increase. In the contemporary conditions of accelerated changes, education is not only human *right*, but increasingly the necessity and *obligation*.

Contemporary narrative on education and its function in the society indicates significant duality of key protagonists' standpoints. According to some estimates, neoliberal ideology transfer to education theory and practice threatens to repress nearly predominant emancipator concept (English, Mayo, 2012). Contrary to humanitarian rhetoric, positivistic standpoint of educations brings narrowed understanding of numerous educational phenomena, reducing education to training and professional development; human being to resource, and knowledge to market-oriented competences. On the other hand, the reality of environment undergoing accelerated change implies the examination of all assumptions underlying educational perspectives, to factually prevent it from becoming obstacle to the societal development.

The concept of life-long or whole life education, promoted in the second half of twentieth century, notes inevitability to comprehend the modern society as "information society", "learning society" or "knowledge society". Knowledge-based economies, using it as a key resource, consequentially place education at the very top of societal priorities. Numerous unquestionable advantages of education are substantiated in its positive correlation – not only to the economic development, but also to the social cohesion of the society, public health, better parenting, lower crime rate and broader political participation (OSCE, 1998). Fundamentally, the economic capital theories understand and note, apart from financial and material, the significance of *human capital*, proving that the investments in human capital provide greater returns against other types of capital (Bralić, 2010, p. 240). Economic indicators testify of the firm link between human and social capital and macroeconomic performance of a society. The empirical data indicate that "the increased rates of school enrolment for a single percentage lead to GDP per capita increase for 1 to 3 percentage points" (Sijanezi & Rinen, 2003., from: Šonenberger, 2005, p. 61). Knowledge, skills and properties embodied in an *individual*, together with networks of relationships, structures and communication methods, operating within an *organization or the entire society* constitute the base for knowledge activating and capacitating it for creating

profit or desired change. Activated or inactivated knowledge establishes the difference between success and failure of an endeavour. On the other hand, from the societal point of view, the investments in education may also be bad investments and failed investments. An example of contemporary critical infrastructures, as exist in "information society" or "knowledge society", Information-Communication Technologies, may unambiguously illustrate the importance of knowledge and education, as a necessary prerequisite for their operation. Sophisticated[8] technologies are not "smart" on their own – the active knowledge, acquired through education makes them so. Without people holding quite specialized knowledge and certain skills, these technologies, on the contrary, may become more susceptible to the risks against less complicated substitutes. Also, without the appropriate personal properties, ethical and other standpoints held by the users of these technologies, which are among other things shaped during upbringing, the security risks are being increased and multiplied.

The direction of education development in a society always depends on the character of given society. In the context of critical infrastructures protection, the greatest importance belongs to the development of quality scientific and technical education, without permitting for the "other, equally important capacities to be lost in the rush of competitiveness" (Nussbaum, 2010, p. 4). Humanitarian sciences disciplines are intertwined with the capacity for development of critical thinking, imagination, reflexive observation and values, which also need to be intricate for the human society to help strengthen human dignity, instead of economic performances *only*.

In line with the new security concept, which equally treats human and national security, both society and individuals should enjoy the benefits of vital social infrastructures operation. The human security concept had been incorporated in the National Security Strategy of Serbia, although it is not equally treated in theoretical and analytical sense. Possible security threats for the individual, which may be brought on by the implementation of Information-Communication Technologies, such as breaching privacy or intellectual property protection, had been recognized only in the SISD (SISD, 2010, p. 23). Previously mentioned SISD, which highlights the importance of critical infrastructure protection, is essentially compatible with the Education Strategy, in the part covering the necessity for stronger IT schooling. This designation has implication both in general population education and IT professionals' education. Adjusting the contemporary information society and global democratization of societal relationships is nearly impossible without an educated citizen.

The general framework of education in Serbia is based on the functional literacy concept. In modern context, it is being understood as the need for the education, at the level of general capacity building, to cover "fundamental and wide knowledge and intellectual skills, which facilitate understanding natural and societal processes and active, critical standpoint against them, active foreign languages knowledge, technical culture and IT knowledge, value system providing for sustainable development and capacity building for life-long (permanent) learning" (Alibabić, 2002, p. 72). In the new context, literacy is not only linked to educational levels, since the four-level UNESCO scale considers highly educated persons not using computer in everyday work to be the persons of third, instead of fourth level of literacy (Mitrović, 2010, p. 142). In Serbia, the educational structure of

8 From Greek word *sophia*, meaning wisdom, smarts.

population, as per the level of educational achievement, is far from desirable. There is an unacceptably high number of citizens finishing only primary school, and very low share of the ones with university-level education, indicating that the degree of general security culture in the society is low, therefore there is scarcity of highly-specialized staff, especially in the information technologies sector.

The foundation of education management in Serbia consists of two intertwining strategies: the Strategy of Education Development by 2020 and the Strategy of Adult Education Development. Those link the system description to the prescriptive expressions, stipulating how things should be. Establishing the educational needs of the society in fact should be "drawn by the future" – not only satisfying the existing needs, but also developing the new ones. If the education programs are to be formed on deficit concept only, based on the expressed needs of employers for certain number and quality of staff, then in insufficiently developed societies, where deficit practically does not exist in most of the professions, there would be no need for such types of education. "The key role of the education system is not to compensate for the deficits and fill in the gaps; instead, it should design and shape the labour market, in line with the expected changes and results in knowledge and skills at the global level" (Despotović, 2009, p. 83). The expected changes may be anticipated by political and educational authorities, and prominent scientific and educational institutions and individuals for higher level of learning.

In line with such standpoints, the lecturing practice may approach the development of programs of importance for critical infrastructure protection. At the general population level, the protection may be contributed by the appropriate contents or themes, incorporated in the contents of the existing courses or establishing the separate course, with the content covering security culture. At the higher levels of education, the decisions would mostly depend on specific cultural context and estimation if critical infrastructures management requires a sufficient level of specific knowledge and competences not obtained within the existing programs, the educational level for establishing this group of professionals, if the barriers in the knowledge of the existing professionals can be brought down by short training, experience or using other methods, and finally if the specific traits of individual infrastructure require more specialized knowledge. In the higher education domain, due to the closer connection of lecturing and science, diversified, flexible programs would probably be necessary, mostly relying on several faculties or several scientific disciplines, with multi-disciplinary or inter-disciplinary outcomes. The nature and functioning of multi-sector positioned infrastructure also requires different models for combining scientific and lecturing disciplines in education of professionals, which would have the critical infrastructure protection as sole or one of the duties.

4. CONCLUSION

We may say that in contemporary conditions, there are in fact societal functions and activities with continuous functioning holding the utmost importance for society survival and security of individual. Their functioning relies on foundations, which may be of material or non-material nature, commonly referred to as infrastructures. Some of those are considered critical, since their breakdown would have long-reaching consequences, worsening operation of all other societal systems. Establishing critical criteria is not only technical, but also supreme philosophical and ethical question, to be the root of any decision-making on infrastructures. It appears that the existing approaches were dominated

by the standpoint favouring the significance of material assets and facilities, sophisticated virtual systems and systems with breakdown causing momentary or short-term negative consequences.

In this paper, we have attempted to elaborate some of the indicators, which suggest the necessity to question the mentioned criteria, include elements in the analysis with the functioning observed in long-term being of vital importance and, based on that, suggest the inclusion of the education system in the set of vital societal systems. Education as a branch, which also has the appropriate material infrastructure, is being considered as value per se, but also the prerequisite for enjoying many other values. The importance of education for critical infrastructures protection therefore may be observed at the general security culture level with population and as a constitutive part of the issue of specialized staff education in the field of risk and crisis management. At the first level, it depends on general educational level and population education quality; and at the second one, on strategic decisions of the society, which should be recognized as the constitutive part of security education, as well as professional education for staff being educated in life and technical disciplines.

REFERENCES:

1. Alibabić, Š. (2002), *Teorija organizacije obrazovanja odraslih*, Beograd, Institut za pedagogiju i andragogiju Filozofskog fakulteta Univerziteta u Beogradu.
2. Aristotel, (1984), *Politika*, Beograd, BIGZ.
3. Bergan, S. (2005), „Visoko obrazovanje kao „javno dobro i javna odgovornost": šta to znači?, u: Veber, L., Bergan, S., (ur.) (2005), *Javna odgovornost za visoko obrazovanje i istraživački rad*, Strasbourg, Council of Europe Publishing, 13-29. (http://book.coe.int)
4. Bralić, Ž, (2010), „Od intelektualnog do ljudskog kapitala", *Godišnjak Fakulteta bezbednosti*, Beograd, Univerzitet u Beogradu, Fakultet bezbednosti, 233-246.
5. Bralić, Ž. (2006), *Antička Atina kao društvo učenja*, Beograd, Univerzitet u Beogradu, Fakultet bezbednosti.
6. Brown, K. A. (2006), *Critical Path: A Brief History of Critical Infrastructure Protection in the United States,* Fairfax, Spectrum Publishing Group, Inc.
7. Colins, P., Baggett, R. K. (2009), *Homeland Security and Critical Infrastructure Protection,* Westport, Praeger Publishers.
8. "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection", *Official Journal of the European Union* L, pp. 345-375, 23.12.2008.
9. Despotović, M. (2009), „Primena koncepta deficita znanja i veština u politici i planiranju obrazovanja – slučaj jedne tranzicione ekonomije", *Andragoške studije*, Beograd, br. 1, 67-87.
10. English, L., Mayo, P. (2012), *Learning with Adults – A Critical Pedagogical Introduction*, Roterdam/Boston/Taipei, Sense Publishers.
11. Gospić, N., Murić, G., Bogojević, D. (2012), „Definisanje kritične telekomunikacione infrastrukture u Srbiji*", XXX Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel*, Beograd, 04. i 05. XII 2012, 367-376.
12. Hamidović, H. (2012), „ICT pripravnost za zaštitu kritične infrastrukture, Objektivne opasnosti – subjektivna mjerila", *InfoTrend*, Zagreb, br. 190.
13. http://europa.eu.int/comm/education/policies/2010/et_2010_en.html
14. http://europa.eu:int/comm/education/policies/2010/et_2010_en html
15. Kurose, J. F., Ross, K. W. (2008), *Computer Networking: A Top-Down Approach*, Boston, Addison-Wesley.
16. Lewis, T. G. (2006), *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation,* Hobocen, Wiley-Interscience Publication.
17. Matika, D. (2009), „Energetska sigurnost i kritična infrastruktura – pregled rezultata istraživanja", u: Matika, D., Poljanec-Borić, S. (ur.) (2009), *Kritična infrastruktura u Hrvatskoj, Prema novom sustavu sigurnosti i zaštite*, Zagreb, Institut za istraživanje i razvoj odbrambenih sustava MORH i Institut društvenih znanosti Ivo Pilar, 42-55.
18. Mitrović, M. (2010), *Pismenost i obrazovanje: perspektiva Novih studija pismenosti*, Beograd, Filozofski fakultet Univerziteta u Beogradu.

19. Murray, A., Grubesic, T., (ed.), (2007), *Critical Infrastructure. Reliability and Vulnerability*, New York, Springer Publishing.
20. Nussbaum, M. (2010), *Not for Profit. Why Democracy Needs the Humanities*, Princeton, Princeton University Press.
21. OECD (1998), *Human Capital Investment/An International Comparison,* Paris, OECD Centre for Educational Research and Inovation.
22. Praška deklaracija (2001), *Ka evropskom području visokog obrazovanja*, Kominike sa sastanka evropskih ministara za visoko obrazovanje, Prag, 19. maj, 2001.
23. Republika Srbija, *Strategija nacionalne bezbednosti Republike Srbije*, (2009), Beograd. (NSS)
24. Smedts, B. (2011), „Critical Infrastructure Protection et the European Level", *Studia diplomatica,* LXIV, 1, 71-78.
25. Stanarević, S., Ejdus, F., (ur.) (2009), *Pojmovnik bezbednosne kulture,* Beograd, Centar za civilno-vojne odnose.
26. Stiglic, J.E. (2003), *Knowledge as a public good*, http://www.worldbank.org/ knowledge/chiefecon/articles/undpk2/
27. *Strategija razvoja obrazovanja u Srbiji do 2020. godine*, (2012), Službeni glasnik RS, br. 107.
28. Šonenberger, A. (2005), „Da li su visoko obrazovanje i akademski istraživački rad javno dobro ili javna odgovornost? Pregled ekonomske literature", u: Veber, L., Bergan, S., (ur.) (2005), *Javna odgovornost za visoko obrazovanje i istraživački rad*, Strasbourg, Council of Europe Publishing, 45-95. (http://book.coe.int)
29. Štiglic, Dž. (2004), *Ekonomija javnog sektora*, Beograd, Ekonomski fakultet.
30. Veber, L., Bergan, S., (ur.) (2005), *Javna odgovornost za visoko obrazovanje i istraživački rad*, Strasbourg, Council of Europe Publishing. (http://book.coe.int)
31. Vlada Republike Srbije, *Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine*, (2010), Beograd, Službeni glasnik RS, br. 51. (SISD)
32. *Zakon o kritičnim infrastrukturama*, (2013), Zagreb, Narodne novine, br. 56.

UDC 726.9:75.041.5
ID 176374796

Vesela Radović
University Educons, Faculty of Applied Security,
veselaradovic@yahoo.com

Husam Majeed Hameed
College of Wassit Medicine University, Iraq
husam_majeed@yahoo.com

THE IMPORTANCE OF CRITICAL INFRASTRUCTURE DURING DISASTERS: THE GREAT CHALLENGE FOR THE FIRST RESPONDERS

Abstract: The importance of critical infrastructure is significant for every society, especially in the time of disasters. During disaster the first responders (police units, emergency services and fire department) should be at the first line to demonstrate the effectiveness of plans, policies and procedures in its work. In this paper the authors present the need to organize protection of critical infrastructure during disaster as a necessary part for the successful work of first responders. The methodology used in this paper is appropriate for social science and based on numerous reports and data about different kinds of disasters. This paper has special value because it presents the results of research authors from countries which were often connected in the global policy: Iraq and Serbia. The disasters made by human beings form a numerous threats to health and life of population in those countries and so far represent a great threat for their future development. In both countries population faced the lack of organization, inadequate help to the affected population which need shelters, food, and other related services. In a part of the paper the authors present how the first responders are faced with a lack of resources in the most important sectors such as health sector, communications sector, energy sector, sector of water supply and waste management, etc. During disaster the first responders are completely aware of risks to which they are exposed but they are thinking primarily about the safety of the affected population. So, the critical infrastructure has to be protected as one of the most important preconditions for adequate response to disaster. At the end, in the final chapter, the authors presented the study which confirms that critical infrastructure protection, if it is adequately protected, contributes that the first responders conduct appropriate level of disaster management. This paper contributes to the academic and public community by addressing the urgent need of improvement activities in the protection of infrastructure as the top priority for the successful response to disaster. The decision makers in both Iraq and in Serbia also have to understand that the protection of critical infrastructure and efficient response to disasters could be obtained only if the first responders build critical skills and have necessary conditions.

Keywords : *autocratic regime, critical infrastructure, protection, risks, first responders*

1 INTRODUCTION

The global community is faced with numerous risks the consequences of which sometimes overwhelmed its capacity. The question of paramount interest for the humanity is how to prevent, eliminate and mitigate the impacts of those risks. The modern security theory addressed the significance of providing adequate level of critical infrastructure protection as one of the most important conditions for the efficient response for all stakeholders, but primarily for the first responders in emergencies.

The main subject of this paper tackles the importance of critical infrastructure protection before, during and after disaster and raises the question how it is valuable for efficiency response of the first responders. In disasters they have to demonstrate the effectiveness of plans, policies and procedures for critical resource logistics and distribution of food, water, fuel, ice, generators, shelter, supplies, to communicate within their region of the responsibilities and ensure that affected populations are provided with all needed goods and services. Are they able to provide all of it, and how much efforts and devotion they put in those activities is the next question? The paper discusses how Iraq and Serbia today, after so much devastation of infrastructure are moving forward to the path of integral disaster risk reduction approach. In that action Serbia follows a path to the European Union and global policy in disaster management.

The main goals of this paper are: to initiate the public discussion of the protection of critical infrastructure; engage stakeholders to include the risk of breaking of critical infrastructure in disasters which already have been seen in some disasters (New Orleans, tsunami in Indonesia, etc.) and discuss about the future strategies and strengthening of critical infrastructure protection in emergencies. The methodology used in the paper is usual for social researchers: historical analysis, comparative analysis, and data analysis, as the most appropriate for this "desktop study." All data were arranged and used for the purpose of achieving the paper's goals.

For the purpose of achievement of paper goals, the authors recognized the need to explain two main terms used in the paper: "first responders" and "critical infrastructure."

The definition in the majority of strategic documents is: "The first responders include fire, police, and emergency medical personnel." In general community "the first responder" is a term which names "the first emergency person to arrive at the scene of a traumatic or medical situation. This person is trained according to a national standard curriculum set up by the U.S. Department of Transportation" (Mosby's Medical Dictionary, 2009).

For the purpose of this paper the authors choose a definition of the "First Responder" as outlined in the Homeland Security Presidential Directive/HSPD-8 (White House, 2011):

- The term 'first responder' refers to those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002, as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations.

During disasters there is a need to protect critical infrastructure in the affected area. Natural disasters as well as manmade disasters (like war, cyber attacks, and other terrorist attacks) can lead to the destruction of critical infrastructure and so on to the reduced trust of the government. Therefore, there is a need for creating "specific solutions and good practices in the area concerned, concentrate on dilemmas such as different national views on and approaches to defining and protecting critical infrastructure" (Čaleta, 2011, p.17).

From all of the above mentioned and for the purpose of this paper, the authors choose the definition for the term "critical infrastructure" from the United States of America (USA). The term "critical infrastructure" has the meaning provided in Section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c (e)), namely systems and assets, whether physical or

virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (White House, 2013)

This directive supersedes Homeland Security Presidential Directive 7. PPD-21 identifies 16 critical infrastructure sectors:

1. Chemical Sector;
2. Commercial Facilities Sector;
3. Communications Sector;
4. Critical Manufacturing Sector;
5. Dams Sector;
6. Defense Industrial Base Sector;
7. Emergency Services Sector;
8. Energy Sector;
9. Financial Services Sector;
10. Food and Agriculture Sector;
11. Government Facilities Sector;
12. Healthcare and Public Health Sector;
13. Information Technology Sector;
14. Nuclear Reactors, Materials, and Waste Sector;
15. Transportation Systems Sector, and
16. Water and Wastewater Systems Sector.

In this paper the authors also present short overview of the disaster management system in Iraq and Serbia. Managing disasters of any kind in country characterized by fragile infrastructure is a hard task but the Government conducted numerous activities to provide prerequisites for the improvement of safety of its citizens and the future development.

In both Iraq and Serbia, as well as in many other countries all over the world it is very hard to respond adequately to disasters when you are faced with budget shortfalls and fragile political situation. While conducting vital services, the first responders are always faced with physical danger. They have to handle desperate civilians at times out of control. In New Orleans during the hurricane Katrina the National Guard and Louisiana Correctional Officers provided the needed security protection for the first responders. Communication sector is the fundamental capability within disciplines and jurisdictions that practitioners need to perform the most routine and basic elements of their job functions. Therefore, the authors present how all efforts of the first responders could fall down if the communication system is destroyed or is out of function.

Conclusion remarks present few recommendations which should be implemented in order to strengthen the nation's ability to protect the critical infrastructure.

2 THE BRIEF EVALUATION OF INFRASTRUCTURE IMPACT IN DISASTER MANAGEMENT ACTIVITIES IN IRAQ

Iraq is a country which has the second oil reserves in the Middle East. Political history of Iraq during 1997-2003 was characterized first of all by brutal regime and autocratic rule of Saddam Hussein, a decade of international sanctions and the effects of wars. The consequences of the wars and fragile political situation caused infrastructure damage, broken trade relations and chronic insecurity within the country.

He report titled *Costs of War*, (Brown University's Watson Institute for International Studies, 2011) stated that "3.5 million Iraqis have fled their homes and have not returned" since 2003. That number includes 1.7 million internally displaced persons and 1.8 million Iraqi expatriates.

For much of the past decade, the Iraqis have cursed about two things: '**maya**' and '**kahraba**' which means: water and electricity (Integrated Regional Information Network-IRIN, 2013). A recent survey found that 42 percent of 2,000 Iraqis surveyed considered basic services - like water and electricity - among the top two concerns they want the current government to address (the National Democratic Institute – NDI, 2012).

Iraq is a country jeopardized by numerous kinds of threats, both natural and manmade. Natural threats are: earthquakes, floods, landslides, sand storms, drought, depletion of natural resources, health epidemics, etc. The manmade risks presented in Iraq are a great number of internally displaced persons and refugees, transport and industrial accidents, toxic environmental pollution, terrorism/civil unrest, high risk of structural collapses and landmines.

The destruction of infrastructure in numerous armed conflicts caused most civilian casualties. Hence the fact that the first Gulf War, according to the first post-war UN mission, had caused "apocalyptic damage" to the infrastructure and had reduced the Iraq to "the pre-industrial age" (Normand, 2003). A 1991 report to the United Nations on restoring Iraq's infrastructure back to its prewar condition estimated a cost of $22 billion in 1991 prices. The infrastructure was destroyed: energy sector was affected, oil refineries too, food storage facilities, industrial complexes, sewage pumping stations, telecommunication facilities, roads, railroads and dozens of bridges were destroyed during the war (WHO/UNICEF Team Report, 1991). One of the most comprehensive assessments of consequences of the first Gulf War concludes that "the lethality of indirect effects of warfare can be much greater than the direct lethality of the weapons themselves" (Osborne Daponte, 1993).

The facts from a series of factual studies, reports and comments on the state of Iraq's infrastructure before the war in 2003 were disturbing. UN reports showed that the country's basic services stood "on the brink of collapse, as a result of 12 years of UN sanctions."[1]

The state of health system in Iraq before the intervention was so far from adequate. Iraq's 130 hospitals, built in the 1960s and 1980s, were in an advanced state of disrepair with cracked and broken windows, damaged doors and leaking roofs. In April UN agencies reported that looting and lawlessness obstructed their operations for normalization of life conditions in

1 Sanctions were imposed by UNSC Res. 661 (6 August 1990). UNSC Res. 687 (3 April 1991) created the regime of weapons inspections after the 1991 Gulf War. To mitigate the adverse humanitarian impact of sanctions, the Oil-for-Food Program (OFFP) was proposed by UNSC Res. 706 (15 August 1991) and finally adopted by UNSC Res. 986 (14 April 1995).

Iraq. As soon as Baghdad was under U.S. control, "the medical system of Baghdad has virtually collapsed" (International Committee of the Red Cross–ICRC, 2003).

By 2003, the new government had managed to provide acceptable levels of electricity supply to Baghdad, but other governorates received less financial means than the capital. Within a month of the incursion, daily energy production had dropped from 4,075 megawatts to 711 due to post-war looting and sabotage; according to the US Special Inspector for Iraq Reconstruction long-term investments made into electricity-generation capacity in recent years have not been adequate because those investments in producing electricity have not been matched by additional investments into electricity transmission. The similar situation was in almost every part of critical infrastructure as communications sector, transportation sector, water and waste management sector and emergency services sector.

Historically, Iraq has followed an emergency response approach in emergencies. Disaster risk reduction functions are not centralized within one agency. They are placed within a line of Ministries and the Office of the Prime Minister. Other institutions in charge of different actions in the area of the disaster risk management are:

- The National Operations Center responds to terrorism and civil unrest incidents;
- The Ministry of Environment which addresses chemical and biological threats in addition to sharing responsibility with the Ministry of Defense;
- The Ministry of Displaced and Migrants addresses the resettlement of returning refugees and the welfare of the internally displaced persons;
- The Ministries of Agriculture and Water Resources share responsibility for responding to seasonal impacts of water scarcity on agriculture and animal husbandry production;
- The Ministry of Health which is in charge for creating protocols and capacities to respond to emerging threats.

At the Governorate level (currently in Iraq there are 18 governorates) exists the so called Governorate Emergency Cell which is operational under the leadership of the Governor. Its main task is to address humanitarian emergencies in accordance with a "Master Plan" for response functions. Civil society institutions appear to be plentiful and offer diverse services to urban and rural populations even if they are characterized by limited capacity. Linkage to disaster risk reduction appears limited in number to agencies such as the Iraq Red Crescent Society.

The Government of Iraq maintains scientific institutions within a line Ministries established to support preparedness for seasonal and unanticipated natural disaster episodes including:

- Iraq Meteorological Department;
- Geological Survey Department of Iraq, and
- Parliamentary Scientific Committee.

In situation where emergencies happen daily the first responders are faced with enormous dangerous in performing their duties.

3 DISASTER MANAGEMENT IN THE REPUBLIC OF SERBIA

In Serbia the Sector for Emergency Management has been organized for the first time within the Ministry of Interior. Law on Emergency Situations was passed, but the system still does not have all necessary legal and organizational prerequisites for reaching maximal efficiency (Radovic, 2012). The Sector for Emergency Management has approximately 4,000 employees, and its central mission is to protect and rescue citizens, material and cultural property and the environment in emergency situations.

On the basis of the Law on Emergency Situations, the Sector for Emergency Management is divided into four offices: prevention, fire rescue units, civil defense and risk management office, and a separate division of the National Training Center for Emergency Situations. Law on Emergency Situations was passed, as well as numerous legal framework documents, but the entire legal framework has not provided necessary legal and organizational prerequisites for reaching maximal efficiency. The activities of the Sector for Emergency Management in regional and international cooperation in the field of cooperation and mitigation of consequences of natural disasters are encouraging but there is still a lot of room for its improvement. One of those expected improvements should happen in the area of critical infrastructure protection.

Critical infrastructure of national importance in the Republic of Serbia is not defined by any specific law. In Serbia it is defined partially by the Defense Law. In this law there is a need for protection of large technical systems, as well as other systems important for national defense: communications, information technologies, air and railway traffic, electricity distribution system, water supply system, etc.

In future Serbia should adopt the EU framework for the protection of critical infrastructure. "European Critical Infrastructure" (ECI) means critical infrastructure located in Member States, the disruption or destruction of which would have a significant impact on at least two Member States (European Council (EC) Directive, 2008).

The Sector for Emergency Management in Serbia is not the only representative for the first responders because in Serbian legal system the services are not united as in the USA. This is also obvious from the fact that Serbia does not use the single European emergency number -112. Despite the plan that Serbia will start to use emergency number 112 which was introduced to enable citizens to call the emergency services (i.e. police, fire and ambulance), the Sector did not realize it. The EU Member States ensured that anyone can call the emergency services from fixed and mobile phones by using the 112 number from anywhere in the EU (European Council (EC) Directive, 2009).

The Sector is faced with numerous problems caused by both subjective and objective impacts. The most important problem in its work is permanent budget shortfalls followed by unplanned and irrational spending for some procurement. In 2013 the planned financial means from the total sum of 1.7 billion dinars, was cut down to the sum of about 400 millions. This fact puts the Sector in an almost impossible situation to handle any kind of response in future emergencies. From all the mentioned above it is clear that system still needs serious reforms in future.

4 THE STUDY CASE ABOUT IMPORTANCE OF COMMUNICATION IN EMERGENCIES – "WHEN TIN CANS AND YARN WON'T DO"

It is vitally important that the first responders have access to reliable, interoperable communications to assist those in need during emergencies. Therefore, for the study case in this paper the authors present the importance of communication system in emergencies. During any crisis, the need for situational awareness and the ability to interoperate with others in the field is critical and hinges on the availability and effectiveness of communication. "The government's ability to communicate depends upon the viability of the commercial network's infrastructure" (United States. Cong. Senate, 2006).

It is the well known that during hurricane Katrina the entire communications infrastructure on the Mississippi Gulf Coast was destroyed, and thirty-eight 911 call centers went down. Thirty days after the landfall, two call centers in Louisiana remained out of service. Two telephone company switching stations in New Orleans responsible for routing 911 calls for the surrounding parishes were knocked out by flooding, resulting in the one of the most significant losses of capacity in and around New Orleans.

The lack of communication sometimes could not be only technical question. On September 2, 2005 Governor Kathleen Blanco wrote a letter to President Bush detailing the needs assessment of the Louisiana government. In this letter, she asked for assistance in restoring critical governmental communications. The letter cites that the New Orleans area radio system was only designed, "to support 800 users." This system was being greatly inundated by over 2,500 users after hurricane landfall (United States. Cong. Senate, 2007, p. 277).

In disasters many local and state officials lacked situational awareness and were unable to establish command and control capabilities. Agencies do not possess adequate communication technology and even when they did it was often incompatible with others and did not allow for interoperability. Some experts proposed the use of satellite communication as useful to fill the communication and control gap created by the devastation of the terrestrial network. Despite those recommendations, it is known that satellite phones could suffer inoperability at times of strong wind or cloud coverage. In addition to numerous communication systems the fuel is needed. Cell towers and control stations could be operable in emergencies if they are running on generators. The trouble in some disasters is that the trade of fuel could be stopped and rerouted in some instances so that the fuel could be used for other purposes. Truck drivers and commercial officials sometimes need military escort into the affected areas due to fear of being held up at gunpoint.

In disasters it is hard to work on infrastructure repair in unsafe condition. The example from Iraq confirmed the need for efficient communication system as an issue of top priority in a process of repair of critical infrastructure after the military intervention. Lucent Technologies World Services Inc., a subsidiary of Alcatel-Lucent, was awarded a $250 million U.S. Army contract to build the emergency system for Baghdad and 15 other cities in 2004. The project's former manager, Geoffrey Willson witnessed in federal court in Seattle that Lucent informed the U.S. government about completed testing of the system's radio transmission sites and of the network as a whole, even if they had done it partially. The U.S. special inspector for Iraq reconstruction audited the "Advanced First Responder Network" in 2006, but its report made no mention of the similar issues. Instead, the report focused on the fact that system remained largely inoperable at that point, with seven of nine new dispatch centers unable to receive calls from the public and other problems. Hence,

there were facts that the emergency communications system failed to work properly, and many of the problems identified in the audit were subsequently resolved.

The communication system is one of the most important parts of critical infrastructure because its lack severely impedes command and control functions, situational awareness, and therefore the disaster relief and recovery efforts.

5 CONCLUSIONS

The global risks are great threat for the development of any country. In Iraq despite the rich oil resources, the expectations of future investment in infrastructure are not so certain. The fragile political situation is not so favourable and has created a lot of uncertainty amongst investors. The similar problem is visible in Serbia where the budget shortfalls affect the work of emergency services and the development in the Republic in general. It is not so easy to repair and modernize critical infrastructure sectors like electricity, health system, communication, etc. However, the Iraqi government has ambitions to realize plans but all efforts made by the government are hampered by the permanent attacks and internal conflicts. Priority Areas for Disaster Risk Reduction in Iraq is a reform of national disaster management agencies, from response-oriented to preparedness; development of national-level policies: raise public awareness of hazard threats and development of strong bilateral relationships between regional and international disaster risk reduction stakeholders.

The provisioning of effective communication during a disaster may need to be taken from the local government and be made into a statewide mandate to ensure interoperability and homogeneous training of officials in all regions. Emergency call centers need to have in place a plan for rerouting when lines go down. The first responders must be able to communicate with each other as well as within their chain of command in order to respond effectively. Public safety managers must be able to manage and control their field resources and be able to communicate their needs and response to the rest of the world. The national security depends on the adequate response to emergencies and the first step for decision makers is to create adequate conditions for emergency services. The first-responder community deserves a better understanding of the resources which are vital for its success. By understanding the wide range of technical capabilities and limitations of the technology, the public safety community will be better prepared for the next disaster.

REFERENCES

1. Čaleta, D. (2011). *A Comprehensive Approach to the Management of Risks Related to the Protection of Critical Infrastructure: Public-Private Partnership*. In Čaleta, D. and Shemella, P. (Ed), Counter-Terrorism Challenges Regarding the Processes of Critical Infrastructure Protection (pp. 15- 27). Ljubljana, Slovenia: Institute for Corporative Security studies - ICS and Center for Civil-Military Relations
2. Eisenhower Research Project. Group ''Costs of War.''. (2011). *Costs of War*. Brown University's Watson Institute for International Studies, Providence, USA. Retrieved August 15, 2013 from http://news.brown.edu/pressreleases/2011/06/warcosts
3. European Council (EC) Directive. (2008). *European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* Official Journal of the European Union, L345/75.
4. European Council (EC) Directive. (2009). *European Council Decision of July 29, 1991 (91/396/EEC) and Universal Service Directive of March 7, 2002 (Directive 2002/22/EC), amended by Directive 2009/136/EC, of 25 November 2009.* Official Journal of the European Union.
5. Integrated Regional Information Network-IRIN. (2013). *Iraq ten years later. Are the taps flowing?* Retrieved August 15, 2013 from http://www.irinnews.org/report/97894/are-the-taps-flowing
6. International Committee of the Red Cross–ICRC. (2003, 11 April). *The medical system in Baghdad has virtually collapsed*. Daily Bulletin. Retrieved August 16, 2013 from http://www.icrc.org/eng/resources/documents/misc/5lhjp6.htm
7. Mosby's Medical Dictionary. 8th edition. (2009). St Louis, MO: Mosby/Elsevier
8. National Democratic Institute (NDI) and Greenberg Quinlan Rosner. (2012). Research: National Survey. A Major Shift in the Political Landscape. Retrieved August 15, 2013 from http://www.ndi.org/files/NDI-Iraq%20-%20April%202012%20National%20Survey%20-%20Report.pdf
9. Normand, R. (2003). *Special Report: Water under Siege in Iraq. US/UK Military Forces Risk Committing War Crimes by Depriving Civilians of Safe Water* .The Center for Economic and Social Rights. NY., USA. Retrieved August 16, 2013 from http://www.cesr.org/downloads/waterundersiege.pdf
10. Osborne Daponte, B. (1993). A Case Study in Estimating Casualties from War and Its Aftermath: The 1991 Persian Gulf War. *The PSR Quarterly, 3*(2), 57-66. Retrieved August 16, 2013 from http://www.ippnw.org/pdf/mgs/psr-3-2-daponte.pdf
11. Radovic V.: (2012). *Climate Change and Adoption Strategies: A Report from the Republic of Serbia,* In: National Security and Human Health Implications of Climate Change. Ed, HSJ Fernando, ZB Klaic, JL McCully. Springer Publishing, NATO Science for Peace and Security: Series C Environmental Security, Dordrecht, Netherlands, pp. 95-102.

12. United States. Cong. Senate. (2006). *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*. 15 Feb. 2006. 109th Cong. 2nd sess. Washington: U.S. Gov. Printing Office.
13. United States. Cong. Senate. (2007). Committee on Homeland Security and Governmental Affairs. *Hurricane Katrina: the Defense Department's Role in the Response*. 9 Feb. 2006. 109th Cong. 2nd sess. Washington: U.S. Gov. Printing Office.
14. US Homeland Security. (2011). *Presidential Directive/HSPD-8*. White House Press Office, Washington, DC, USA. Retrieved August 12, 2013 from http://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf
15. US White House. (2013). Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. White House Press Office, Washington, DC, USA. Retrieved August 18, 2013 from http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
16. WHO/UNICEF Team Report. (1991). Report to the Secretary-General dated 15 July 1991 on humanitarian needs in Iraq prepared by a mission led by the Executive Delegate of the Secretary-General for humanitarian assistance in Iraq, S/22799, 17 July 1991. Retrieved excerpts August 16, 2013 from http://www.cam.ac.uk/societies/casi/info/undocs/s22799.html>.

UDC 726.9:75.041.5
ID 176374796

Dane Subošić, Dragan Mlađan
The Academy of Criminalistic and Police Studies Belgrade
dane.subosic@kpa.edu.rs
dragan.mladjan@kpa.edu.rs

MAIN FEATURES OF FIRE FIGHTING INTERVENTIONS CARRIED OUT BY BELGRADE FIRE AND RESCUE BRIGADE

Abstract: Fire and rescue units are an important subject for the protection of the critical infrastructure. Detrimental consequences of fires and other safety and security threatening events and occurrences depend considerably on their performances, both in terms of their types and the scope of damage. One of the key factors of affected values is the length of time during which the protected values (the objects of critical infrastructure) have been exposed to hazards, such as fire, etc. The shorter the time is, the smaller the damage to these values is. In order to make this time shorter, fire and rescue units should arrive to the scene of intervention at objects of critical infrastructure in the shortest possible time in order to put out the fire. This also represents one of the fundamental performances (abilities) of fire and rescue units. Therefore, this paper considers the time of arrival to the scene of intervention at the objects of critical infrastructure and its influence on the duration of fire fighting at these objects carried out by the Belgrade Fire and Rescue Brigade, in the period 1986-2009. The research was conducted in the way that all the interventions at objects of critical infrastructure have been sorted by years in the mentioned period, where for each year mean values have been calculated in the form of the arithmetic mean of the arrival time of fire and rescue units to the scene of intervention and of the duration of the fire fighting intervention at the above mentioned objects. After that, dispersion measures have been determined for the mean values in question, in a form of standard deviation, variation range and variance. Then, the co-variance has also been set down, in order to determine the homogenous/heterogeneous elements of the statistical data set within the considered features. Finally, there have been derived linear diagrams of arrival times and fire fighting times, and their analysis has been made in order to determine the factors that contributed to the increase, stagnation or decrease of the arrival time to the scene of intervention, i.e. the time of its duration, as well as the regression analysis of interventions per mentioned parameters. Such an approach created the conditions for the prediction of further engagement of fire and rescue units, in Belgrade and in other major cities.

Keywords: *critical infrastructure, fire and rescue brigade, arrival to the scene, intervention, duration.*

1. INTRODUCTION

Critical infrastructure can be put in danger in various ways. One of these dangers comes from fires. Fires, as a hazard to the critical infrastructure, cause numerous damages to lives and health of people, to material goods and the environment. Indirect detriments caused by fires through destroying or damaging the critical infrastructure can lead to serious consequences wherein normal lives of people are affected, particularly through endangering the areas of national security, of health and lives of people, property and environment,

economic stability and continual functioning of the authorities (The Law on Critical Infrastructure: 3). Fire and rescue units represent a significant stakeholder which offers the protection of critical infrastructure facilities.

While the EU member states had already passed the laws concerning the area of protection of critical infrastructure, Serbia has not done it yet. Instead of a clear identification what critical infrastructure is and what it is not, there are regulations in force in Serbia offering identification of: objects,[1] buildings,[2] ancillary buildings,[3] outbuildings,[4] line infrastructure objects[5] and communal infrastructure.[6] Apart from that, there is an implicit mention of the concept of a *construction object*[7] in the doctrinal literature of the fire and rescue units (Guidelines for filling in of forms ID – 1, ID – 2 and ID - 2a: 6.13).

In conditions of non-existence of a clear distinction of the term of critical infrastructure and the use of the mentioned terms in domestic practice, we have decided to convey the meaning of the term "critical infrastructure" by the approximate term of "construction object".

The subject of this research is to determine the influence of the arrival time of a fire fighting unit to the site of fire fighting intervention on the duration of fire fighting in a construction objects, in the area of the city of Belgrade, in the period between 1986 and 2009.

The objective of this study is to explain the impact of the time of arrival of a fire brigade to the site of fire fighting intervention on the time needed to put out the fire in a construction object, in the area of the city of Belgrade, between 1986 and 2009.

---

1 *An object* is a construction structure connected with the ground, representing a physical, functional, technical-technological or bio-technical structure (buildings of all kinds, traffic, water industry and energetics objects, objects within the electronic communication infrastructures – cable sewage, communal infrastructure objects, industrial, agricultural and other manufacturing objects, sporting and recreational facilities, cemeteries, shelters, etc.) (*The Law on Planning and Construction*: 2, 1, 22).

2 *A building* is an object with a roof and outer walls, constructed as an independent functional structure offering protection from weather and atmospheric influences, and is intended for residing, performing an activity or for accommodation and animal keeping, keeping of goods, equipment for different manufacturing and servicing businesses, etc. Buildings also include the objects that have roofs, but do not have (all) the walls (for example, canopies), as well as the objects that are mostly or completely located beneath the earth surface (shelters, underground parking lots, etc.) (*The Law on Planning and Construction*: 2, 1, 23).

3 *An ancillary building* is the object in the function of the main object and is constructed at the same ground lot as the main residential, business or any other object of public purpose (garage, warehouse, septic tank, well, water tank, etc.) (*The Law on Planning and Construction*: 2, 1, 24).

4 *Outbuildings* are the objects for breeding animals (horse stables, cowhouses, facilities for breeding chicken, goats and sheep, as well as the objects for breeding pigeons, rabbits, ornamental poultry and birds); ancillary objects for breeding domestic animals (livestock outlets, concrete lanes for disposal of hard manure, objects for storing the sedge); objects for storing fodder (threshing barn, stockrooms for storing concentrated fodder, concrete silo pits and silo trenches); objects for storing agricultural products (barns, baskets) and other similar objects within an agricultural compound (objects intended for machines and vehicles, smokehouses and drying rooms, etc.) (*The Law on Planning and Construction*: 2, 1, 24a).

5 *Line infrastructure objects* are public roads, public railroad infrastructure, transmission lines, oil pipeline, product lines, gas pipeline, an object for height transport, line infrastructure of electronic communications, etc. that can be over or under the surface, whose construction has been designed by appropriate document plans (*The Law on Planning and Construction*: 2, 1, 26).

6 *Communal infrastructure* is all infrastructure objects for which the approval for construction works, i.e. the construction permit is issued by a local self-government unit (*The Law on Planning and Construction*: 2, 1, 27).

7 *Construction objects*: residential building, cinema, theatre, museum, business building, warehouse, goods shed, residential-business building, school, agricultural building, stable, hotel, hut, shed, chimney, kindergarten, thermal plant, water plant, silos, parking lot, garage, airport facility, children home, nursing home, construction area, trade-craftsmanship shop, electric plant, catering business, transformation station, shopping mall, gas plant, refinery, manufacturing plant and other construction objects (Guidance for filling in the forms ID – 1 , ID – 2 and ID - 2a: 6.13).

The hypothesis to be verified by this micro-research is: "The time of arrival of the fire brigade to the site of fire fighting intervention influences the duration of the fire fighting in construction objects in the area of the city of Belgrade, in the period 1986-2009." The indicators of such a hypothesis are: 1) the arrival time of the fire brigade to the site of fire fighting intervention, in a construction object; 2) the duration of the fire fighting in a construction object, in the area of the city of Belgrade, between 1986 and 2009; 3) linear dependence of the mentioned times; 4) the correlation coefficient of the mentioned influence; 5) the reliability of the obtained correlation intensity; 6) the linear trend of the mentioned times, and 7) the regression of the linear and real trend.

The method of research has been decided by means of the statement of the hypothesis in question, or more precisely, by the way in which it has been indicated. Therefore, the implementation of the contents analysis method will be dominant in this study, and will be applied in the process of collecting and sorting of statistical data. Also prominent will be statistical methods that will be used in the function of processing the above mentioned analysis method (arithmetic mean, standard deviation, variance, variance and co-variance span, Pearson's correlation coefficient and functional analysis). The collected data will be sorted by years, followed by their arithmetic mean and dispersion measures, which will be used for the implementation of the method of statistical analysis, leading to the data that will enable the verification of the hypothesis set. In addition, software packages SPSS Statistics 10.0 (SPSS for Windows 10 FFK9FFK 123488521) and Microsoft Office Excel 2003 have been used for this purpose.

The main part of the work has been processed in two complementary sections. The first one relates to the sample and the methods, and the second one – to the results of the research and their analysis (discussion).

2. THE SAMPLE AND RESEARCH METHODS

Belgrade fire and rescue unit performed 63,596 interventions between 1986 and 2009 (*Records of interventions, 1986*), but the statistical sample has been formed by eliminating the extreme values of the independent variable (t_1) – *arrival time of the fire brigade to the site of intervention (fire)* and of the dependent variable (t_2) – *duration of fire fighting,* meaning that only values $1 \leq t_1$ and $t_2 \leq 90$ *minutes* have been analyzed. A statistical sample formed in this way contained 54,362 interventions, with n = 9.234 interventions having been eliminated. Therefore, a part of these interventions:

1. has been wrongly entered into official records as lower extreme values, i.e. time of arrival of the fire and rescue unit to the site of intervention (fire) and duration of fire fighting in minutes, in cases where
   t1 and t2 = 0,
   as they are illogical (do not have any duration), i.e. only the following values have been considered:
   t_1 and $t_2 \geq 1$,
2. and as *higher extreme values*, in cases where *fire fighting time* in minutes is
   $t_2 \leq 90$,
   which is considered an unusually long intervention time by experts, having as a result the following value, due to the same number of interventions (number of

arrivals to the site of intervention and number of fire fighting cases)
$t_1 \leq 90$.
The number of 54,362 (85.48% out of 63,596) fire fighting interventions was thus obtained, where 9,234 (14.52% out of 63,596) interventions were eliminated as being the ones that contained the above mentioned extreme values. This was necessary as all the analyses that included the extreme values t_1 – *time of arrival of the fire brigade to the site of intervention (fire)* and t_2 - *duration of fire fighting in minutes,* had a bigger standard deviation from the arithmetic mean, i.e. the following non-equation applied:
$\sigma > \bar{X}$,
which could not be accepted as the statement that the whole sample had to be included with three standard deviation has been applied.

Out of 54,362 interventions representing interventions that do not contain the mentioned extreme values, in relation to the statistical set, 33,363 (61.37% out of 54,362) interventions represent the cases of fire fighting that have been carried out in construction objects (as a function of approximation of critical infrastructure objects in the area of the city of Belgrade in the observed period), which makes the statistical sample of this study. The area in which Belgrade fire and rescue brigade intervened is the City of Belgrade (3222.68 km^2, population 1,576,124) (City of Belgrade – Population, 2013). All fire fighting interventions of the Belgrade fire and rescue brigade carried out in construction objects are sorted by years in which they had been performed, after which the mean values have been calculated in the following way:

- t_1 – arithmetic mean of the arrival time to the site of intervention, in a construction object, per year, in minutes,
- t_2 – arithmetic mean of the duration of fire fighting in a construction object, per year, in minutes,
- σ_1 – standard deviation of the arithmetic mean of the arrival time to the intervention, in a construction object, and
- σ_2 – standard deviation of the arithmetic mean of the duration of intervention, in a construction object.

The relevant data are shown in the following table.

Table 1: Main statistical features of fire fighting interventions carried out by Belgrade Fire and Rescue Brigade in construction objects in the period 1986-2009 (Source: Records of interventions, 1986)

Year	t1	t2	σ1	σ2
1986	6.54	33.85	2.2080	20.6273
1987	7.41	33.91	2.7741	21.2313
1988	8.75	33.23	4.3418	20.8212
1989	7.75	33.68	5.0121	19.6661
1990	7.77	34.37	4.6777	19.9304
1991	8.06	34.68	5.2475	19.5187
1992	7.90	35.60	5.1134	20.5706

Year	t1	t2	σ1	σ2
1993	7.61	34.46	4.9140	20.4921
1994	7.26	33.76	4.7296	19.8079
1995	7.24	33.66	4.3384	19.6386
1996	7.80	35.22	5.2400	20.2624
1997	7.65	34.16	4.6533	19.6645
1998	8.20	37.11	5.2795	20.5476
1999	8.56	36.46	6.8503	20.0410
2000	8.33	38.48	6.3909	23.2539
2001	7.88	36.73	4.7121	19.7778
2002	8.78	36.70	7.7023	20.2138
2003	8.31	36.16	6.2333	19.8148
2004	8.50	35.34	6.8681	19.4404
2005	8.08	35.67	6.3666	19.4445
2006	8.05	36.43	6.2302	20.1370
2007	8.39	35.66	6.9372	19.6465
2008	8.01	35.22	5.8628	19.5184
2009	8.30	35.81	6.4990	19.5859
$\overline{X}$	7.96375	35.26458	5.382592	20.1522

Descriptive statistical methods are applicable to both variables, i.e. t_1 and t_2. The arithmetic mean t_1 – *time of arrival of the fire brigade to the site of intervention (fire),* in a construction object, in minutes, is calculated by using the mathematical model:

where:

$\overline{X}$ – arithmetic mean,

x_i – value of the numerical range (i = 1,...n),

f_i – frequency of the numerical feature (i = 1,...n),

N – total number of units in a range.

$\overline{X}$ (t_1) = 7.96375 minutes (median M_e = 8.03 minutes),

with the average standard deviation

σ = 5.382592,

i.e. average variance

σ^2 = 28.97229 (standard deviation square, i.e. σ^2).

The covariance has been also determined, in order to define the homogeneous/heterogeneous nature of elements of the statistical set per features of *arrival time of the fire brigade to the site of intervention (fire)*, in a construction object, in minutes.

$cV_1\% = \sigma / \overline{X}\ (t_1) \times 100 = 68\%$.

Dispersion measures in a form of variation and variance span have been set for the mentioned mean values. The span of variation of the arithmetic mean of arrival time to a construction objects, in minutes, per year, is calculated by means of the following model:

$$\bar{X} = \frac{X_1 + X_2 + \cdots + X_n}{n} = \frac{\sum X}{n}$$

Rv_1 = Xmax - Xmin

where:

Rv_1 - span of variation of the arithmetic mean of arrival time to a construction object, in minutes, per year,

Xmax – the longest average time of arrival to the intervention, in minutes, per year,

Xmin – the shortest average time of arrival to the intervention, in minutes, per year.

The following can be concluded from the above mentioned:

Rv_1 = 8.78 minutes – 6.54 minutes

Rv_1 = 2.24 minutes.

Having in mind that all (33,363) average times of arrival to the same interventions (at construction objects, in order to put out fire) are classified into 2.24 minute span of variation, it is not possible to make the analysis that would help determine the factors that brought about the variation of the analyzed time.

The arithmetic mean t_2 – duration of fire fighting time in a construction object, in minutes, per year, is:

X (t_2) = 35.26458 minutes (median M_e = 35.28 minutes),

with the average standard deviation

σ = 20.13154,

i.e. variance

σ^2 = 405.2789 (standard deviation square, i.e. σ^2).

The covariance has been also determined, in order to define the homogeneous/heterogeneous nature of elements of the statistical set per features of *arrival time of the fire brigade to the site of intervention (fire)*, in a construction object, in minutes.

$cV_2\% = \sigma / \bar{X}(t_2) \times 100 = 57\%$.

When comparing the values of cV1% and cV2%, the conclusion can be made whereby cV1% > cV2% (68%>57%), indicating the higher level of heterogeneous nature of data relating to t 1 when compared to t2, i.e. higher homogeneous nature of t2 in relation to t 1.

After that, dispersion measures in a form of variation and variance span have been determined for the mentioned mean values. The span of variation of the arithmetic mean of fire fighting time in a construction object, in minutes, per year, is:

Rv_2 = Xmax - Xmin

Where:

Rv_2 - variance span of the arithmetic mean of the time duration of fire fighting in minutes, in a construction object, per year,

Xmax – the longest average time of fire fighting in minutes, per year,

Xmin – the shortest average time of fire fighting in minutes, per year,

The following can be concluded from the abovementioned:

Rv_1 = 38.48 minutes – 33.23 minutes

Rv_1 = 5.25 minutes

Having in mind that all (33,363) average times of the same type of interventions (in a construction object, during fire fighting) are classified in a 5.25 minute variation span, as is the case with the average arrival time to the intervention, it is not possible to make an analysis that would help determine the factors which caused the variation of the analyzed time.

The variation span indicators show that the set relating to t_2 in comparison to t_1 is more homogeneous, i.e. that the set of values marked with t_1 in relation to t_2 is also more homogeneous, which is understandable given the several time higher values of the arithmetic mean values of the fire fighting duration in relation to the arithmetic mean values of the arrival time to the site of intervention (in a construction object), expressed in minutes, per year.

The main questions that should have been given reply to by this research relate to whether there is a correlation between t_1 – arithmetic mean value of arrival time in minutes, to the site of intervention (in a construction object), per year and t_2 – arithmetic mean value of fire fighting time in minutes, in a construction object, per year, and if there is any correlation – of which intensity and how reliable it can be. As the mentioned variables represent the features of the interventions of the Belgrade fire and rescue unit, the Pearson's correlation coefficient has been applied. The application of the Pearson's correlation coefficient is possible if there is a linear relation between the variables t_1 and t_2. The mentioned possibility will be presented in a part of this work titled *Results of the research and discussion*.

In addition, the mentioned features (t_1 and t_2) of fire fighting interventions of the Belgrade fire and rescue brigade should be discussed from the aspect of tendency of their development in the function of time, for which a suitable analysis is needed, derived on the basis of their linear trend. Such an approach has created the conditions for prediction of further deployment of fire and rescue units, both in Belgrade and other larger cities.

3. RESULTS OF THE RESEARCH AND DISCUSSION

By considering the circumstances to which the results of the research are applicable, the conditions have been provided in which the results are obtained, interpreted and analyzed. The following chart has been given as an illustration.

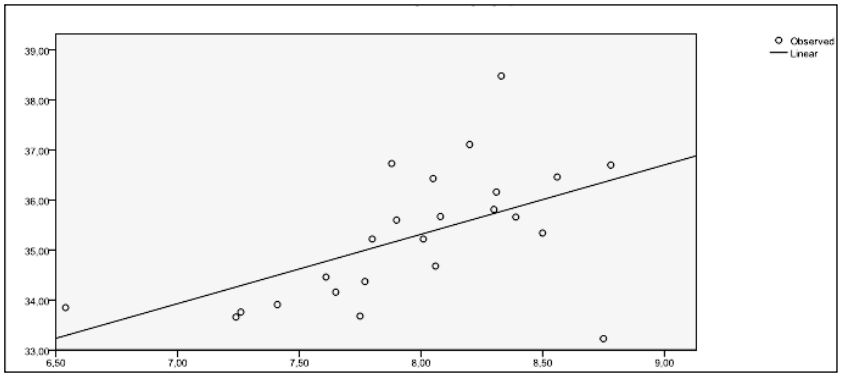


Figure 1: Linear interrelation of t_1 – arithmetic mean of the arrival time in minutes to a construction object, per year, and t_2 – arithmetic mean of the fire fighting time in minutes, in a construction object, per year (Source: Register of interventions, 1986)

The previous chart shows the linear relation of t_1 – arithmetic mean value of arrival time to a construction object, in minutes, per year, and t_2 – arithmetic mean value of fire fighting time in a construction object, in minutes, per year, where this relation is such that if the average arrival time to the fire fighting intervention in a construction object is increasing, then the average fire fighting time in minutes, in a construction object, is also increasing. This is one more proof that the application of the Pearson's correlation coefficient is possible (this will be done later in the paper). However, the intensity of the mentioned relation and reliability of its occurrence cannot be seen from the above chart. *Pearson's correlation coefficient* indicates the relationship of the mentioned occurrences by intensity

$r = 0.544$,

with the significance of

$p = 0.003$

indicating that the mentioned relation intensity of t_1 and t_2 can be accepted as reliable, as the confidence interval is:

$p \leq 0.05$ $(0.003 < 0.05)$.

Since the value of the correlation coefficient is

$r = 0.544$,

the discussed relation of t_1 and t_2 (actually, the influence of t_1 on t_2) is of significant intensity

$0.4 < r < 0.7$ (Petz, 2004).

In addition, the determination coefficient, as an indicator of share of t_1 and t_2 is

$R = r^2 = 0.296$,

which is significant for the field of social sciences.

Finally, the line diagrams of average arrival times to the site of intervention and fire fighting times have been derived, and so have their analysis in order to determine the trends of development of t_1 and t_2 during the observed period of 24 years, as well as the reliability of their approximation – by means of the R^2 linear function (the following chart).

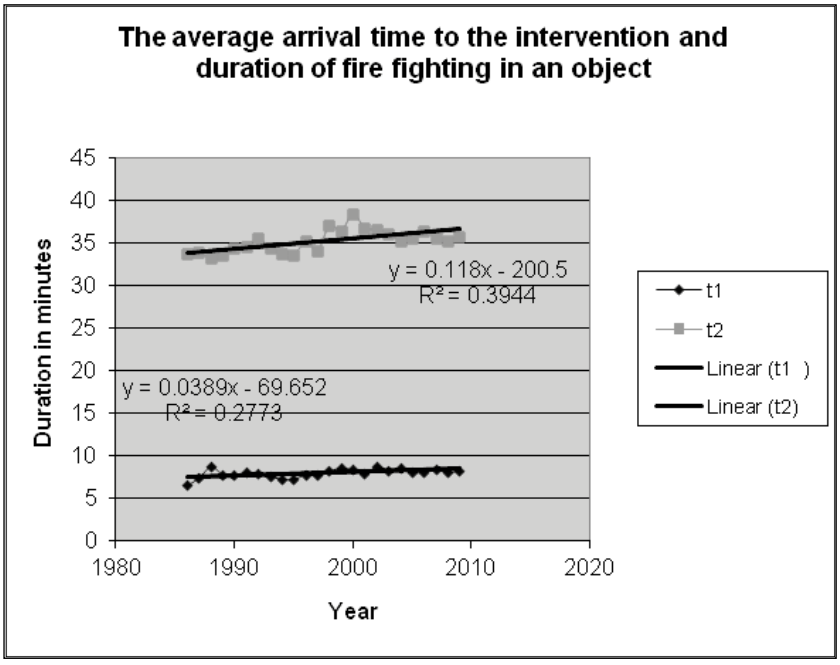


Figure 2: The average arrival time to the intervention and duration of fire fighting in a construction objects (Source: Register of interventions, 1986)

The previous chart has shown the growth of both t_1 – arithmetic mean value of arrival time to a construction object, in minutes, per year, and t_2 – arithmetic mean value of fire fighting time in a construction object, per year, also given in minutes. The growth is expressed by the linear trend and the positive values of both direction coefficients (coefficient in front of the variable x). In addition, the growth is more intensive in case of t_2 – arithmetic mean value of fire fighting time in a construction object, per year, given in minutes, in relation to t_1 – arithmetic mean value of arrival time to a construction object, in minutes, per year ($t_2 = 0{,}118 > t_1 = 0{,}0389$).

On the other hand, the linear approximation of real trends of both t_1 – arithmetic mean value of arrival time to a construction object, in minutes, per year, and t_2 – arithmetic mean value of fire fighting time in a construction object, per year, given in minutes, is valid since the determination coefficient is ($R^2 = 0.2773$) in case of t_1, and ($R^2 = 0.3944$) in case of t_2. The mentioned determination coefficients are important for social sciences having in

mind that they indicate significant levels of linear correlation coefficients (r = 0.526) of the real and linear trends in case of t_1, and (r = 0.628) of the real and linear trends in case of t_2.

3. CONCLUSION

The term of critical infrastructure in Serbia has not yet gone live, and is therefore presented by an approximated term of a construction object. Consequently, the paper took into consideration the protection of construction objects from fire in the area of the city of Belgrade. The Belgrade fire and rescue brigade is in charge of these tasks that are carried out in a form of interventions.

The study identified the linear relation of t1 – arithmetic mean value of arrival time to a construction object, in minutes, per year, and t2 – arithmetic mean value of fire fighting time in a construction object, per year, in minutes, in the area of the city of Belgrade, in the period 1986-2009. In addition, the mentioned relation is directly proportional, i.e. the following statement is applied: if the average time of arrival to the site of fire fighting intervention in a construction object is increasing, then the average time of the fire fighting intervention in a construction object, in minutes, is also rising. The Pearson's correlation coefficient indicated the relation of the mentioned occurrences (t1 and t2) by a significant intensity of r = 0.544, with the significance of p = 0.003, which implies the fact that the relation in question and its intensity can be accepted with confidence. When the mentioned conclusion is compared with the hypothesis statement, to the verification of which this study is eventually dedicated, we can conclude that this hypothesis has been confirmed.

Other conclusions also resulted from this paper:

- A permanent trend of growth in the arrival time to the fire fighting intervention is present (as a consequence of numerous factors, for example, the increase in the number of registered vehicles in Belgrade, the Republic of Serbia, etc.) and so is its duration in the observed space and time (as a consequence of confirmation of the verified hypothesis);
- Average fire fighting times in construction objects are more homogenous than the average times of arrival of the Belgrade fire and rescue unit to the fire fighting interventions, which indicates the fact that the issue of fire fighting is more standardized (in terms of construction, preventive, organizational, technical and natural matters) than the issue of predominantly traffic character, which is more significant for the average time of arrival to the fire fighting intervention and as such, it is prone to bigger changes (it is more heterogeneous/less homogeneous than the fire fighting issue);
- A small variation span of the average duration of fire fighting in construction objects and of the average arrival time of the Belgrade fire and rescue unit to the fire fighting intervention indicates that the development of that unit helped achieve many things: starting from the fire fighting prevention, regular schedule and dimensioning of its organizational units (battalions, squads, platoons, sections, fire fighting ships, etc.) where certain socio-economic factors should be taken into account, for example deindustrialization and other, as well as the method of research (forming a statistical set without extreme values);
- Also, a small variation span of the average fire fighting time in construction objects and of the average arrival time of the Belgrade fire and rescue brigade to the fire

fighting intervention enables a valid approximation of the real trend of discussed occurrences by using their linear trends;

- Longer average time of arrival to the site of intervention than the professional standard, which is 5-7 minutes world-wide, indicates that it is necessary to restructure the organizational units of the Belgrade fire and rescue brigade in the way that would take into account the existing organizational structure and unit schedule, but to introduce, according to the current estimates, four new fire fighting units, in the following parts of the city: Stari Grad – 1, Novi Beograd – 2 and Mirijevo – 1; and
- Certain reduction in the average arrival time to the site of fire fighting intervention will be effected as a consequence of the completion of the Belgrade road traffic system, by completing the accessing roads to the bridge over Ada, as well as by finishing the bridge Zemun-Borca, Belgrade ring-road, and several tunnels whose construction has already been planned.

4.SOURCES

1. *Evidencija događaja*: Program za unos i statistiku registrovanih događaja rađen za PC - računare, Autor: Brankica Popović, Uprava za analitku i informatiku MUP RS, Beograd, 1986/*Records of interventions*: A programme for entries and statistics of registered incidents made for PC computers, Author: Brankica Popovic, Department for analytics and informatics of the Ministry of Interior of the Republic of Serbia, Belgrade, 1986.
2. Grad Beograd – Stanovništvo. Preuzeto 29. juna 2013, sa *http://www.beograd.rs/cms/view.php?id=1201* / City of Belgrade – Population, downloaded on 29 June, 2013 from *http://www.beograd.rs/cms/view.php?id=1201.*
3. Petz, B. (2004). *Osnovne statističke metode za nematematičare*. Jastrebarsko: Naklada Slap/Petz, B. (2004) *Main statistical methods for non-mathematicians*. Jastrebarsko: Naklada Slap.
4. Uputstvo za popunjavanje obrazaca ID – 1 , ID – 2 i ID - 2a, MUP RS, Beograd, 1999/ Instructions for filling in the forms ID – 1 , ID – 2 and ID - 2a, Ministry of Interior of the Republic of Serbia, Belgrade, 1999.
5. *Zakon o kritičnim infrastrukturama*, „Narodne novine“, br. 56/13/ *The Law on Critical Infrastructures*, „Narodne novine“, No 56/13
6. *Zakon o planiranju i izgradnji*, „Sl. glasnik RS“, br. 72/2009, 81/2009 - ispr., 64/2010 – Odluka US, 24/2011 i 121/2012 / The Law on Planning and Construction, „Official Gazette of the Republic of Serbia“, No 72/2009, 81/2009 – erratum 64/2010 – decision US, 24/2011 i 121/2012

SECTION IV

TECHONOLOGIES RELATED TO CRITICAL INFRASTRUCTURE PROTECTION

UDC 726.9:75.041.5
ID 176374796

Bojan Zrnić, Veljko Petrović, Branko Medan
Ministry of Defence of Republic of Serbia, Defence Technology Department
bojan.zrnic@vs.rs
veljko.petrovic@mod.gov.rs
branko.medan@mod.gov.rs

ASPECTS OF CRITICAL INFRASTRUCTURE PROTECTION IN THE DEFENCE INDUSTRY[1]

Abstract: The defence industry is one of the pillars of economic and technological development and stability in many modern countries. Recognizing this fact, the infrastructure of the defence industry, primarily intended for the production and storage of arms and military equipment, is an important asset, meaning that protection of this infrastructure is among the prime interests of national security. Alignment with the highest standards and the establishment of control mechanisms in the sphere of critical infrastructure protection are basic prerequisites for protecting the defence, security and foreign policy interests of the country, including its international credibility. This paper considers some aspects of the security and protective measures to be taken in order to meet organizational and technical conditions for the safeguarding of classified information, to prevent the destruction or damage of critical infrastructure in the defence industry, to prevent jeopardizing the safety of human resources serving this infrastructure, and destruction or disclosure of classified information on the capacity of the critical defence industry infrastructure.
Keywords: *critical infrastructure, defence industry, risk, industrial security, protection.*

1. INTRODUCTION

Critical infrastructure, according to contemporary definitions and understandings, represents the assets, facilities, systems or their parts, which has necessary - essential role in provision of basic social functions, health, safety, security, economic or social well-being of people and whose destruction or disabling would have a significant impact on human society as a result of the inability to preserve these functions.[2] Depending on whose interest it is in, the Critical Infrastructure (CI) can be characterized as a corporate, national, regional or international. Within the areas - sectors that have incorporated the CI, the following areas are especially emphasized: energy (including generation, transmission, storage, transport and distribution of resources and energy), the communication and information technologies (including electronic communications, data transferring systems, information and media systems), traffic and transport (road, rail, air and water), health

1 The work was developed within the research project No. 47029 entitled "Cost-effective range of new technologies and concepts in defence of social change and the strategic orientation of Serbia in the 21 century". The Project is funded by the Ministry of Education and Science of the Republic of Serbia 2011-2014. The project leader is Professor Momcilo Milinović, PhD.

2 The EU Council (2008). Directive 2008/114/EC – on identification and designation of European critical infrastructure.

care (including health protection, manufacturing, trading and supervision of medicines), the provision of water and food (including the production, storage and quality control and supply of these items), finance (including banking and brokerage systems, investments and insurance and payment systems), production, transportation and storage of hazardous materials (chemical, biological and radiological), safety and security services (military, police, protection and rescue services, emergency services), as well as other sectors – areas.[3] The production of arms and military equipment or defence-industrial complex of a country or a region is recognized as especially important sector, which has some overlaps with the above mentioned areas, but due to its complexity, characteristics and elements that determine it, undoubtedly contains attributes that determine the CI.

This paper perceives the most important aspects of the system security and protective measures to be taken in order to meet organizational and technical conditions for the prevention of risks to which the CI may be exposed in the defence industry within the areas of physical and technical security, accidents resulted by disturbed pyrotechnic safety and industrial security.

2. CI IN THE DEFENCE INDUSTRY

The defence industry is one of the pillars of economic, technical and technological development and stability of modern countries. Recognizing this fact, the infrastructure of the defence industry is significant potential to which every organized society gives special attention, and the protection of this infrastructure, which has attributes of critical one, is ranked as a high priority interest of the national security system. Alignment with the highest standards and establishment of the control mechanisms in the sphere of CI, with particular emphasis on the defence-industrial complex, are the basic requirements for protecting the defence, security and foreign policy interests of the country, its international credibility and integrity.

What is specific for defence industry is that its industrial base consists of a very large, diverse, complex, and interdependent and hierarchically organized set of entities that are governed by different regulations and agreements and which include a wide range of different tiers of subcontractors and different ownership structure. In modern countries, which have developed defence industries and a strong technological base for realization of research, development, production, delivery and maintenance of armament systems and military equipment (AME), their sub-systems, components and parts, it is estimated that there are hundreds and thousands of stakeholders involved in the process, with the common purpose of meeting the demands of the armed forces through the preservation and improvement of the defence industry potentials. When viewed from this perspective, it is observed that unlike the other sectors, defence industry base is not primarily focused only on the products or services it provides, but rather on the users of these products - services and their requirements.[4] Recognizing this fact, the infrastructure that is critical for the defence industry may also belong to other sectors. In this paper, the term of defence industry will be cover the specialized companies that are directly involved in the production and storage of weapons and military equipment, which are

3 Zakon o kritičnim infrastrukturama Republike Hrvatske (Nar. Nov. 56/13 od 18.05.2013. godine).

4 U.S. Department of Defence (2007). Defence Industrial Base, Critical Infrastructure and Key Resources Sector Specific Plan

registered for this type of activities by the competent state authority, and in further consideration, the term CI is related to the critical infrastructure of these entities.

2.1. Identification of assets, facilities, systems and elements CI in the defence industry

In the process of CI protection, the starting point is its identification and assessment, and determination of entities and elements belonging to the chain of production, whether in the basic processes or in the logistics processes inside the defence industry infrastructure, where the negative impact on the subjects and elements would have caused far-reaching negative consequences and side effects on a broader level. Basic information that is collected in the process of identifying potential defence industry CI include the following parameters: basic information on the subject (company), data on the company focal point in charge of the areas of production and security, data on production capacities (facilities, equipment, capacity utilization and labour), information on products, production processes and production volumes, data on production programs, components and subsystems, data on cooperative companies (by tiers and products, with special reference on critical subcontractors), data on business indicators, data on financial indicators and data on critical technologies. In addition to these basic parameters, if the infrastructure is assessed as CI, additional information are collected including: information on all the objects which produce or store critical resources, data on the dependent enterprises within the defence industry sector and within other sectors which are necessary for its functioning, data on the continuity and redundancy of function (through identification of alternative sources of supply and backup production facilities), data on the impact in case of loss or damage, data on the activities undertaken to secure infrastructure and data intelligence threats exposure.[5]

Once identified as a CI in the sphere of defence industry, it is subjected to a continuous process of risk assessment and monitoring, checking and updating the relevant data in order to timely intervene and optimize the processes which ensure its protection and improvement.

3. CRITICAL INFRASTRUCTURE RISK EFFECTS CONSIDERING

In the process of identification and assessment of risks that defence industries CI may be exposed to, the main considered indicators refer to the effects that these risks would cause. In line with this, the risk consequences that exert influence are considered in practice through the four categories:[6]

- **The impact on people and the environment:** direct effects on human life and health and the environment;
- **Economic impact:** direct and indirect effects on the economy (in terms of costs for remediation, the cost due to loss of products and services supply, long-term costs due to threats to the environment, and others.)
- **Impact on the public:** The effect on the morale of the population and the confidence in the national economic and political institutions, and

5 U.S. Department of Defence (2007). Defence Industrial Base, Critical Infrastructure and Key Resources Sector Specific Plan

6 *Ibid*.

- **Impact on the ability of governmental agencies:** The effect on the ability of the government to maintain public order, to provide a minimum of public services, to ensure the health and safety of the population and implement the tasks of national significance.

In addition to these basic categories of consequences, an important factor in assessing the risks implications in the defence-industrial complex is an influence on the mission of the defence system and the armed forces as its specific part. This is considered through the technological base assessments, in terms of subjects which are the only source and the holders of unique technology or capacity whose loss would significantly affect the operational capability of the armed forces. Moreover, it is considered whether the subject is of special interest for the other areas/sectors CI and whether it can be redirected (pre-qualified) to the production of other products / services.

3.1. Impact on people and environment

As the defence industry encompasses a wide range of different areas of production (from textile and fabrics, over optoelectronic and telecommunications, technology and metallurgy, metals and aircraft industry to chemical industry) its impact on human health and the environment has a varying intensity (from low to very high). This influence, in normal circumstances is manifested in the production process, to the employees, production and technological capacities (with bigger intensity) and to the local population and the immediate surroundings (with smaller intensity). Nature and specificity of production and technologies used in different segments of the defence industry can be qualified as a dangerous and risky to people's life and health and to the environment. The risks that are identified in the production process are prevented by the strict application of regulations in the field of work safety and environmental protection, with constant monitoring and preventive response.

The impact on people and the environment is significantly increased in case of occurrence of emergencies in defence industry infrastructural capacities, particularly adverse events in the areas of chemical and technological and metallurgical production, irrespective of their cause. In those cases, the effect of the negative impact escalates on the broader population and region, causing, in most cases, huge consequences in terms of the number and severity of injuries and casualties, and contamination of the wider region. This is one of the key factors which the capacities of the defence industry aligns among the tempting targets for terrorists and other destructive activities and the risk of this type of activities is rated on the list of the potential dangers with the highest rank when the object of action is defence industry CI. For this reason, special attention is devoted to the analysis and monitoring of these types of risks in defence industry, as well as identifying its most exposed CI (buildings and equipment).

3.2. Economic impact

As defence industry in the developed countries is one of the key areas in terms of ensuring stability, technological progress, economic growth and engagement of significant capacities and contractors from different spheres, each disorder in its operation can cause a chain reaction and economic consequences on a larger scale. The main economic impact of the defence industry and its CI is through influence on the course of economic trends.

Namely, the disruptions of CI cause side effects by increasing direct and indirect costs, income reductions, loss of customers, subcontractors and markets, increased dependence on foreign technologies, and through the series of other relevant economic indicators. It should be noted that this impact is caused by different factors as a direct - physical and indirect - immaterial. Direct factors that may have a direct influence on costs increment are: the delay in production caused by organizational and technological process causes, accident situations, destructive or other actions and necessity for their short-term and long-term consequences remediation. Indirect factors that may affect the additional costs, thus reducing profits are: lack of products' competitiveness, reduced chances of product placement as a result of uniqueness of technology status loss, limited access to certain markets and the theft of intellectual property. Within the economic impacts of modern environment, special attention should be devoted to the analysis and reduction of risks caused by indirect factors, both in the mid-term, and a long-term basis.

3.3. Impact on the public

In contemporary geopolitical environment, as well as at the national level, public opinion is an important factor in the creation of public policy and relations in the state. Regarding this, the risks that threaten the defensive industry and its CI, with direct and indirect effects can influence to a large extent the state of morale and attitudes of the population, as the final result may have an impact on trust in governmental agencies and organizations, especially the institutions in the sphere of defence and the economy. In a word, the stable functioning of the defence industry, directly or indirectly provides safety and strong public support for state institutions. In this respect, the protection of defence industry CI, primarily on risks whose consequences would be immediately visible in public (accidents and enemy action) is an important aspect in the preservation of the moral and political stability of the key state segments.

3.4. Impact on the ability of government authorities

The ability of the government to maintain public order, to provide a minimum of public functions, to ensure the health and safety of people and carry out the tasks of national importance is the basic assumption for smooth operation of a regulated social system. The defence industry is one of the key factors necessary for the ability of the development of government authorities in the field of defence and public security, which is the national interest task. Every adverse impact on the capacities of the defence industry and its CI has a direct impact on reducing the ability of state authorities in this field, and indirectly, considering specificity and association of state governing institutions, on the capacity in other areas of national importance. Risks which present threats to defence industries CI can be direct (accidents and hostile action) and as such are with the short-term or mid-term character, or can be indirect (threat to industrial safety and the lag in technological development) with strong long-term impact on CI. Considering the above, there is a clear need to organize CI and defence industry protection within legislative and management framework as a continuous systematic process that requires constant and proactive work, identification and analysis of potential risks and their impacts, in order to ensure long-term provision and preservation of social system functioning ability.

4. IDENTIFICATION OF THE RISKS DEFENCE INDUSTRY IS EXPOSED TO

Considering the above-mentioned effects and consequences, and perceiving the potential risks that could be their cause in the field of defence industry, the most significant risks, which are further analyzed in the paper, are identified as:

- **The Hostile action** - in terms of terrorist, destructive or sabotage action on capacities of defence industry CI;
- **Accidents** - in terms of occurrence of accident caused by extraordinary events in the production process at critical capacity of defence industry, and
- **Violation of industrial security** - in terms of undesirable information leakage, whether in the field of official and business secrets or intellectual property domain.

4.1. The risk of hostile action

Hostile action (here is primary focus on terrorist and sabotage activities) on defence industry CI, in contemporary conditions, is a constant threat around the world, because of the nature of its character of asymmetrical warfare, where the relatively small actions achieve significant effects on a broader level. This mechanism of sabotage and terrorist activity on the capacities of defence industry CI represents a threat which directly results in immediate capacity disabling and production process suspension, and indirectly affects the induction of other impacts in terms of human health and the environment menace, the negative economic effects, public intimidation and political destabilization. In modern era, the modes of such an action are brought to light, in addition to direct physical attacks through the destruction and damage of CI assets and facilities, and by key personnel neutralization or information and processing systems hacking. Particularly vulnerable and attractive targets for this action are the parts of defence industry engaged in the production, transport and storage of components of chemical and NBC lethal means (powder, propellants, initiating devices, explosives, radioactive, chemical and biological agents, etc.), as well as those engaged in the production of explosive ordinance and pyrotechnic compositions.

4.2. The risk of accidents

The accidents here mean accidentally caused extraordinary events in the defence industry, which have arisen as a result of failures in performance, technical or technological errors as a result of "force majeure". Negative effects that are manifested in cases of accidents are similar to the effects caused by hostile action, with possibly different adverse impact on the public opinion, due to the nature of accidents, which are globally random and are less likely to repeat than hostile action. And this is the risk the defence industry CI is particularly exposed to in the field of production, transport and storage of ammunition, NBC equipment and chemicals for their production because of the physical and chemical characteristics of the materials used and the nature of the processes that take place, which are often unpredictable with a high degree of stochastic and instability.

In addition to the aforementioned finding, there is also the fact that in the critical infrastructure of the defence industry of the Republic of Serbia in the last two decades a number of accidents occurred, which had resulted in injuries, fatalities and accidents with material damage, among which the following should be emphasized:

- **December 2010** – In the Company Sloboda Cacak, whose product range includes mostly the production of medium and large calibre ammunition, there were a series of explosions of ammunition after a fire in one of the buildings with one worker injured;
- **January 2010** - In the Company Sloboda Cacak, two explosions occurred with one worker injured;
- **September 2009** - In the company Prvi Partizan Uzice, whose product range is based on the production of shooting, sporting and hunting ammunition, there was a series of explosions at the facility for gunpowder, killing seven workers and 14 were injured;
- **May 2006** - In the company Prva iskra – namenska proizvodnja, whose product range is the dominant production and processing of high explosives, an explosion occurred in which three people were killed and three of them wounded;
- **December 1997** - In the company Milan Blagojevic- namenska Lucani, whose product range includes the dominant production of powder and propellants, an explosion occurred in which three people were killed on the spot, five people were injured and subsequently died from their injuries;
- **June 1996 - I**n the company Prva iskra – namenska proizvodnja, an explosion occurred in which two workers died and suffered minor damage.

Analyzing the causes of the problem, the common attitude of most military analysts is that, in addition to the human factor, the most common causes of accidents are obsolete plants which produce flammable or explosive materials, which can easily cause a hazard in the most modern plants of its type in the world. We should not forget the labour-extensive character of production in the defence industry that is trying to catch up, in which it found itself after the bombing in 1999. Also, most analysts agree on the fact that the accident situations in the Serbian defence industry do not occur more frequently than elsewhere in the world.

Over the past 25 years there have been reports of more than 400 unplanned explosions at munitions sites in almost half the world's countries.[7] It is interesting to note some of the cases that have occurred in recent years:

- A blast in the Military Gunpowder and Explosive Factory in Villa Maria city, the Argentine province of Cordoba. The explosion occurred on September 5, 2013. There were several people injured and one factory worker was killed;[8]
- Three workers were injured on January 10, 2012, by an explosion at VMZ Sopot, Bulgaria's largest military factory, with the lives of all of them out of danger. The explosion was not occasioned by munitions, but rather occurred during a routine production process due to a malfunctioning of the equipment;[9]
- In an explosion at a military hardware factory, the Raytheon Systems factory in Glenrothes, two electricians have been injured on Decembar 5, 2011. The US company specialises in defence and aerospace systems. Its work is focused on weap-

7 Eric G. Berman and Pilar Reina (summer 2012). "Unplanned Explosions at Munitions Sites: Concerns and Consequences", Focus - The Journal of ERW and Mine Action

8 www.bernama.com

9 www.novinite.com/view_news.php

ons and military and commercial electronics, and is the world's largest producer of guided missiles;[10]

- A huge nitro-glycerine explosion has occurred at a factory in the Czech Republic on April 20, 2011, and four people were missing. The blast destroyed a building at the plant, which makes explosives for customers including the Czech military. The explosion occurred at the Explosia AS plant in Pardubice, 100 kilometres east of Prague, the capital;[11]
- A powerful blast at a factory making explosives and weapons in southern Yemen killed at least 78 people on Mart 28, 2011, after the facility was briefly taken over by Islamist militants and then looted by residents of the area;[12]
- Two people were killed and 16 injured on August 30, 2008, in an explosion at the Turkish Mechanical and Chemical Industry Corporation's (MKEK) gunpowder factory in the central Anatolia province of Kırıkkale. The MKEK factory in Kırıkkale was the site of another large explosion in 1997 in which three workers were killed. After the 1997 explosion the factories were rebuilt and the necessary safety measures were put in place. The MKEK factory, which also produces nitrocellulose, has ISO 9001 safety certification.[13]

It is an encouraging fact when it comes to upgrading the capacity of the Serbian defence industry that in recent times the great efforts are taken at the level of line ministries in order to enable the financing of investment projects of modernization of the plants of defence industry, which would mean their greater willingness to perform top production and create better security conditions.

4.3. The violation of industrial security risk

In contemporary societies, the real capital and value of the company is less expressed in tangible assets, but their real value is the ownership of knowledge and available technologies which provide them advantages over their competitors. This is particularly conspicuous in the field of defence industry, where the possession of more sophisticated technology and knowledge provides a significant advantage and the stability of a society by strengthening and maintaining its position in the international environment. From this point of view, violation of industrial safety through unwanted leakage of classified information and the theft of knowledge and technology can achieve significant adverse economic and other impacts on society in the medium and long run, primarily by the loss of technological preferences and imbalances in terms of competitive advantages in the common market, and also the weakening of overall state's developmental and industrial potential, which ultimately leads to the reduction of the state power.

5. DEFENCE INDUSTRY CI PROTECTION

Considering the risks to which the defence industry and its CI are exposed to, as well as the negative effects they might cause, it is noticeable that the problem of dealing with the risks is of wide coverage, and that the nature of the risk and the nature of CI are diverse,

10 www.dailyrecord.co.uk/news

11 www.godlikeproductions.com

12 www.theguardian.com

13 www.todayszaman.com/news

but the CI protection process is one indivisible whole, which requires an integrated approach to the risk analysis and the development of the required level of the organizational culture for the corporate action to prevent the undesirable consequences. Through this integrated action, three main aspects of protection of CI can be distinguished, which although assumed to a certain type of risk, in effect are also applied in the reduction of consequences of other types of risk. Compared to the identified risks defence industry CI is faced to, the aspects of its protection can be scrutinized.

5.1. Physical and technical protection of CI defence industry

Physical and technical security is a basic form of protection of human and material resources of CI in the defence industry, and this aspect of care is focused largely to a consideration of the risk of direct menace by external influences. This type of protection includes the implementation of measures and actions within the organization of physical and technical security and management in this area in order to prevent a threat to people and property, recovery and eventual discovery of the perpetrators.[14] The physical protection measures mean immediate protection of property, plants and space of companies, their immediate or wider surroundings and persons who reside there. This type of care includes manpower skilled for in the protection jobs, which perform monitoring and access control, deter threats, control and secure transport, inspection and shipment of material and others.[15] The subjects of physical security in the defence industry comprise the entire human potential, which performs jointly, in coordinated manner and proactively in order to eliminate potential risks, and reactively to eliminate eventual effects. The technical protection measures, in practice, mean protection and prevention of unauthorized access to CI facilities with the use of specialized technical resources and equipment. For this purpose, mechanical, optoelectronic, electronic and combined resources and systems are applied.[16] This form of protection is the complement of physical protection, and their combined application is implemented for effective CI protection. Compared to the risks discussed above, this type of protection has the biggest importance and the most effective use in monitoring and risk evaluation in the scope of the hostile action, in terms of prevention as well as in the removal of possible consequences.

5.2. Work safety and environmental protection within the defence industry CI

In the defence industry, as a conglomerate of producers of specific items, special attention is paid to the implementation of work safety, health and environmental protection in the process of production, transportation and storage of hazardous materials. This protection should be achieved by constant monitoring of conditions and processes with mandatory application of the highest standards, which need to be constantly improved and modernized in accordance with the development of new technologies. As already noted, of particular interest in the CI protection in the defence industry is the prevention of accidental situations caused by disturbed levels of pyrotechnic safety, as falling into the category of risks that may generate negative consequences of large-scale, especially to the people,

14 dr Milan Daničić, dr Ljubomir Stajić (2008). "Privatna bezbednost", Visoka škola unutrašnjih poslova, Banja Luka.

15 Goran D. Matić (2006). "Osnovi fizičko-tehničkog obezbeđenja", Privredna komora Srbije, Beograd

16 Milan Daničić, dr Ljubomir Stajić (2008). "Privatna bezbednost", Visoka škola unutrašnjih poslova, Banja Luka.

their working surrounding and the environment. Possible aspects of care in this area are reviewed by improving the internal work organization, technological processes and environmental conditions. The implementation of work safety and environmental protection comprises a set of measures and procedures based primarily on the regulation and organization of the process, with the use of certain physical and technical measures to control and monitor the process.

5.3. Defence industry CI Protection in the industrial security field

In the field of industrial security, where the main risk is unauthorized leakage of information, the protection of CI includes a number of mechanisms including primarily preventive and then reactive action in order to mitigate the consequences of this risk. These mechanisms are applied in layers, and include measures that involve a variety of ways to protect classified information. It can be said that the protection of defence industry CI in this domain, in fact is represented by the protection of its critical information. This process applies the same logic as the process of infrastructure protection, which begins with the identification of critical information through the consequences of their discovery and their classification with certain level of confidentiality. What are specific here are the types of classified information to be protected, and the way they exist. In regulatory terms, this field is regulated by industrial property rights and it, besides the materialized information protection (in the form of various instruments-documents, projects, prototypes, etc.) includes the safeguarding of the intangible values (such as "Know-how" that in practice includes knowledge and "Good will" which represents reputation).[17] Likewise, given the nature of the defence industry, in addition to regulations in the field of industrial property, the protection of the defence industry in the field of industrial safety is covered by the confidential data protection regulations and by the national security regulations. As already stated, the protection of critical information is implemented in different ways and in fact largely encompasses the described segments of physical and technical security and safety, with the extension of these measures in terms of legal protection of industrial property (through patenting, licensing, transfer of technology and know-how), and with, for this area, specific protection measures through political mechanisms (international agreements, treaties of alliances and other agreements, which protect the common interests in the defence industry).

It should be noted that in terms of industrial safety in the first half of this year a normative-legal act was adopted which gives in more detail the special protection of classified information relating to the manner and procedure for determining compliance with organizational and technical requirements for the storage of classified information provided by legal entities and individuals on the basis of the contractual relationship, the implementation of which will begin six months after its entry into force. This legal document is an additional incentive to the joint efforts of government bodies to complete reorganization of the confidentiality of the data, both in terms of the level of compliance with the EU legislation, and create the conditions for building strong and stable control mechanisms in the field of organization of the work process, to protect access to secret data, to provide protection against unauthorized use of classified information, certification entities, physi-

17 dr Vuk Raičević (2010). "Pravo industrijske svojine". Univerzitet Privredna akademija – Pravni fakultet za privredu. Novi Sad

cal and technical protection of the space in which the data are kept secret, fire protection, protection of confidential data during transmission and delivery outside the room where they are safeguarded, transportation of classified information, the provision and protection of information and telecommunications funds which are used for transmission and delivery of classified information and prescribed measures of cryptographic protection.

6. CONCLUSION

In the process of the defence industry CI protection, the risks that influence the human lives and health and the environment, national economy, public opinion and credibility of the government and governmental agencies have been presented as well as protection from those risks discussed through the aspects of physical and technical security, the environmental protection and the domain of the industrial security. The importance of these aspects is that each of them is focused on a particular type of risk, but also to a greater or lesser extent it extends to other types of risks, and in their evaluation it is necessary to provide a comprehensive analysis, which would include various perspectives of the impact on CI and the national interest. Although covered by different regulations, which require different specific procedures, all presented aspects of CI protection in the defence industry are in essence one inseparable whole, which requires an integrated approach to risk analysis and the development of the necessary level of organizational culture for corporate action in order to prevent undesirable consequences. What is characteristic of the risk analysis for CI in the defence industry is the lack of representation in domestic scientific and technical literature, as well as the legislation which has not been fully completed in this area. In the developed countries (the U.S. and the European Union), the practical realization in this area has special attention, with the constant improvement of the system of the national and corporate security and redefining of the normative-legal regulations. It is necessary to have continual improvement of practical implementation in real systems, which under the circumstances of under-developed regulations and the lack of trained personnel for implementation is a major problem of the national defence industry framework. In this regard, a need exists in the Republic of Serbia to systematically regulate these aspects through the normative-legal framework and through strengthening the monitoring mechanisms in this area because of the viability of the defence industry CI potentials, their further development and thus the development of national potential of the state.

REFERENCES

1. Bundesministerium für Wirtschaft un Technologie (German Federal Ministry of economics and Technology) (2004). Manual for industrial Security.
2. The EU Council (2008). Directive 2008/114/EC – on identification and designation of European critical infrastructure.
3. Eric G. Berman and Pilar Reina (summer 2012). "Unplanned Explosions at Munitions Sites: Concerns and Consequences", Focus-The Journal of ERW and Mine Action.
4. Goran D. Matić (2006). "Osnovi fizičko-tehničkog obezbeđenja", Privredna komora Srbije, Beograd.
5. dr Milan Daničić, dr Ljubomir Stajić (2008). "Privatna bezbednost", Visoka škola unutrašnjih poslova, Banja Luka.
6. U.S. Department of Defence (2007). Defence Industrial Base, Critical Infrastracture and Key Resources Sector Specific Plan.
7. U.S. Department of Defence (2006). National Industrial Security Program – operating manual.
8. dr Vuk Raičević (2010). "Pravo industrijske svojine". Univerzitet Privredna akademija – Pravni fakultet za privredu. Novi Sad.
9. Zakon o kritičnim infrastrukturama Republike Hrvatske NN56/13 od 18.05.2013. godine.

UDC 726.9:75.041.5
ID 176374796

Dragana Nikolić
University of Belgrade, Institute of Nuclear Sciences "Vinča"
anikol@vinca.rs

Ana Kovačević
University of Belgrade, Faculty of Security Studies
kana@rcub.bg.ac.rs

Srboljub Stanković
University of Belgrade, Institute of Nuclear Sciences "Vinča"
srbas@vinca.rs

THREAT ASSESSMENT FOR THE DESIGN OF THE EFFECTIVE PROTECTION SYSTEM OF NUCLEAR FACILITIES

Abstract: This paper is focused on nuclear security systems and arrangements for the protection of nuclear installations, nuclear and other radioactive material. In particular, a threat assessment process and methodology for the development, use and maintaining of the Design Basis Threat (DBT) are presented. The whole process is based upon a risk managed and threat-driven approach. DBT represents the largest reasonable threat that a facility should expect to defend against. It is an important tool used to determine well-specified threat levels, providing a representative set of attributes and characteristics of potential adversaries (internal and/or external). Since the DBT also provides detailed and precise technical foundations for the design and evaluation criteria for a physical protection system, the margins of achieving the adequate degree of assurance that the level of protection is sufficient are explored. Some common principles of nuclear safety and nuclear security are outlined in this paper and the importance of their correlation for efficient protection of nuclear facilities is discussed. The conclusion reached is that, in the context of the increased focus on defences against terrorists at nuclear facilities, the new, extended approach to analysis of the beyond DBT events is needed, to include more severe attacks as well as combination of the different types of threats. In addition, the application of more stringent requirements for physical protection and promoting of nuclear security culture at all levels of nuclear security regime is recommended.

Key words: *Critical nuclear infrastructure, design basis threat, physical protection, nuclear security regime, unauthorized removal, terrorist attack*

1. INTRODUCTION

Critical infrastructures (CI) are defined as those systems, assets, or part thereof which are essential for the maintenance of vital societal functions, security and economic security, and the disruption or destruction of which would have a significant impact on the state/nation as a result of the failure to maintain those functions (EC, 2008). The potential effects to CI of both human generated or natural catastrophic threats are huge and disruptive, and the resulting cost of damages can be enormous. Therefore, issues related to CI are becoming a progressively more important field, especially with increase in automation, posing a complex set of requirements upon security assessment (Rinaldi, et al, 2001).

The protection of CI should be based on an all-hazards approach. The variety of possible threats to CI is vast, ranging from natural disasters (earthquakes, tornadoes, flooding, etc.), accidents due to equipment failure, unintentional manmade accidents, to sabotage and terrorist attacks, which are considered as a priority in the CI protection process. The "severity" of the impact caused by the disruption or destruction of a particular infrastructure, is assessed with reference to multiple effects: environmental, political, psychological, public (number of members of the population affected); economic (significance of economic loss and/or degradation of products or services), as well as public health consequences. The significance of the impact shall also be assessed in terms of cross-cutting criteria, which includes the effects resulting from cross-sector dependencies and interdependencies, since the impact of disruption of one sector can propagate to other sectors.

CI protection approach should be developed and implemented taking into account specificities of the particular CI sector, and should be built on the existing CI sector-based measures.

Nuclear sector is identified as CI with the scope of sector definition that extensively varies: from including only "radioactive substances" as CI, to including all nuclear fuel cycle facilities and even radioactive waste facilities as CI. However, the majority of classifications, adopted by most of countries, consider nuclear power plants (NPPs) critical infrastructures.

In the *Proposal for a Directive of the Council on the identification and designation of European CI and the assessment of the need to improve their protection*, (EC, 2006) nuclear industry (production and storage/processing of nuclear substances) was identified as the CI sector. The *Council Directive* 2008/114/EC (EC, 2008), recognise that in terms of the energy sector, and in particular the methods of electricity generation and transmission, electricity transmission parts of NPPs may be included in electricity generation where deemed appropriate, but the specific nuclear elements covered by relevant nuclear legislation including treaties and Community law are excluded.

The US approach is more comprehensive and inclusive, and it has been particularly evolving since the attack of September 11, 2001. Executive Order 13228 established the Office of Homeland Security and assigned the duty to coordinate efforts to protect "facilities that produce, use, store, or dispose of nuclear material" (Executive Order 13228, 2001).

Homeland Security Act (HSA) of 2002 formally introduces the concept of "**key resources**" defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government". Without articulating exactly what they are, the act views key resources as distinct from CI, albeit worthy of the same protection. In addition, "key assets" as a subset of nationally important key resources was also introduced. Although key assets are individual targets that may not be vital to the continuity of critical services at the national level, their destruction could create local disaster or profoundly damage nation's morale.

The definitions of "CI" and "key resources" from the *HSA* are adopted, by reference, in Homeland Security Presidential Directive 7 (HSPD-7, 2003), which also adopts the CI and key asset categories. The requirements of HSPD-7 continue the policy of critical asset prioritization and protection "with an emphasis on CI and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction". Therefore, HSPD-7 designates Nuclear Sector as a key resource, specifically requiring protection of the following elements: commercial nuclear power and research reactors; nuclear material in medical, industrial and academic

settings, facilities that fabricate nuclear fuel; and transportation, storage and disposal of nuclear materials and radioactive waste. NPPs particularly are identified as one of 5 key asset categories.

Regardless the particular definitions of "CI", Nuclear Sector protection has always gained special attention, primarily due to the fact that potential accidents could cause significant loss of life and property in addition to long-term, adverse public health and safety consequences. Therefore, nuclear safety and security are founded on the high operational and organisational standards and well regulated, covered by relevant nuclear legislation including international and multilateral treaties. The development of effective national and global preparedness and response to nuclear and radiological incidents and emergencies is of major importance as well.

In the current global situation, there is a particular concern regarding the possibility that nuclear or other radioactive material could be used for malicious purposes. The nuclear community responded to this risk by engaging in a collective commitment to strengthen the protection and control of such material and to respond effectively to nuclear security events. It has agreed to strengthen the existing and has established new international legal instruments to enhance nuclear security worldwide. Nuclear security is fundamental in the management of nuclear technologies and in the applications where nuclear or other radioactive material is used or transported.

This paper is focused on the systems and arrangements that are necessary for the protection of nuclear installations, nuclear and other radioactive material. In particular, a threat assessment process and the methodology for development, use and maintaining of the design basis threat (DBT) are presented. DBT indicates the largest reasonable threat to a facility that should be expected to defend against.

1.1. Nuclear Facilities and Nuclear Material

In the context of CI identification, the Nuclear Sector consists of a wide variety of assets, systems and networks necessary for their secure and resilient operation. That comprises commercial nuclear reactors for generating electrical power, research, and other fuel cycle facilities; nuclear facilities in various stages of decommissioning; radioactive materials, industrial irradiation facilities, radioactive source production and distribution facilities; radioactive waste management facilities; transportation of nuclear and other radioactive material. However, some components of the above broadly defined Nuclear Sector are beyond the scope of this paper, such are radioactive sources and associated facilities, as well as nuclear weapon sites.

The nuclear facilities of interest are those civilian facilities (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of, and damage to or interference with such facility could lead to the release of significant amounts of radiation or radioactive material. This definition is specific to the revised Convention (CPPMN, 1980) and has been amended from the glossary definition (IAEA, 2007) for the purposes of the Convention. Essentially, this includes any facility for which an authorization or license is required, that is part of the nuclear fuel cycle.

Nuclear material refers to plutonium except that with isotopic concentration exceeding 80% in plutonlum-238; uranium-233; uranium enriched in the isotope 235 or 233; uranium containing the mixture of isotopes as occurring in nature other than in the form of

ore or ore-residue; any material containing one or more of the foregoing (CPPMN, 1980; Int. Convention, 2005).

In order to completely understand the scope and the character of the potential risks this infrastructure poses, it is helpful to be acquainted with the nuclear fuel cycle. The nuclear fuel cycle may be broadly defined as the set of processes and operations associated with the production of nuclear energy, including the manufacture of nuclear fuel, the operation of nuclear reactors, storage, reprocessing or the disposal of the irradiated fuel, all related waste management activities (including decommissioning), and any related research and development activities. Every stage in the nuclear fuel cycle merits the appropriate security measures, as well as the transportation of nuclear materials between each of the above operations/sites.

NPPs are the most complex components and therefore primary sector concern. Research, testing and training reactors (including sub-critical and critical assemblies) operate at major universities and research institutions, and since they are mostly located in highly populated areas, their protection is important and delicate. Reactors in various stages of decommissioning are also a part of the sector, and in cases when nuclear materials are still in storage at these sites, they may be targets that require protection. Other fuel cycle facility types comprise mining and milling of uranium/thorium ores, uranium conversion and enrichment, nuclear fuel fabrication, spent nuclear fuel reprocessing and recycling, and the storage and disposal of spent nuclear fuel. Because radioactive waste may pose a safety and/or security threat, the proper management of radioactive materials is also a key concern for Nuclear Sector.

Fuel cycle facilities are categorized based on the type of nuclear material that they store or produce. Special nuclear material (SNM) is given different designations depending on its level of enrichment and the amount of material a facility possesses. Spent reactor fuel is extremely radioactive and could be used for malicious purposes.

It is important to emphasise that, in addition to radiation risks, many fuel cycle facilities pose a chemical hazard. Chemical processing is used in most of these facilities: for example, uranium mill is a chemical plant where mined ore is leached to extract uranium; in reprocessing facility the spent fuel material is treated to recover the remaining portion of fissionable products for use in fresh fuel assemblies. Consequently, there is the principal potential hazard from chemical releases. An offsite release of these chemicals may have substantial consequences comparable to those associated with the release of radioactive material from a nuclear reactor.

The world inventory of nuclear CI facilities and materials that require protection and may be potential targets globally is extensive. For the purpose of illustration, total numbers of fuel cycle facilities by type and nuclear reactors in the world, in various stages of operation, are summarized in Tables 2 and 1, respectively. Global stocks of fissile materials comprise about

Table 1. Total number of nuclear power reactors (IAEA PRIS, 2012), research, training and test reactors (IAEA RRDB, 2012) in the world, in various stages of operation and decommissioning

Facility type	In operation	Temporary shutdown	Under construction	Shut down	In decommission
Research, training & test reactors	246	20	5	142	320
Power reactors	437	-	65	144	118
Total reactors	683	20	70	286	438

Table 2 Total number of fuel cycle facilities (IAEA-TECDOC-1613, 2009)

Facility type	In operation	Stand by	Under construction	Total by type
Uranium Conversion	23	1	3	27
Uranium Enrichment	18	1	2	21
Fuel Fabrication	52	2	0	54
Spent Fuel Storage	109	0	2	111
Spent Fuel Reprocessing & Recycling	20	4	2	26
Related industrial activities	33	1	1	35
Total fuel cycle facilities	255	9	10	274

1.370 t (metric) of HEU, not including 346t to be blended down, and 244.9t of separated plutonium in civilian stocks, about 255t in military stocks (while up to 100t is declared excess) (ISIS, 2003).

2. FRAMEWORK FOR THE PROTECTION OF NUCLEAR CRITICAL INFRASTRUCTURE

The protection of nuclear CIs from a variety of possible threats is a complex task that requires multifaceted approach. The Nuclear Sector sets a high standard for CI preparedness with its approach to the security of nuclear reactors, nuclear and other radioactive materials, and the extensive emergency planning and exercise programs around NPPs, as well as other nuclear and radiological facilities.

In the process of risk analysis relevant threat scenarios have to be considered in order to assess the vulnerability and the potential impact of disruption or destruction of CI. The defence against all possible threats is not achievable, but there is a rationale for developing all-hazards planning scenarios for use in national security preparedness activities.

Threats to nuclear infrastructure from major natural phenomena, operational failures (such as equipment breakage, loss of electric power supply) and inadvertent human errors are primarily considered in the safety evaluations, within the domain of nuclear safety. Malicious acts intended to cause damage or steal material circumventing protective measures are in the focus of nuclear security assessments. The aim of nuclear safety is to maintain stable operation of the facility, prevent accidents or mitigate accident consequences, and in that way achieves the ultimate goal of protecting workers, the public and

the environment from undue radiation hazards. Nuclear security is aimed at preventing the intentional acts that might damage the facility and/or associated activities, result in the theft of nuclear materials and its illegal transfer. An element of the security regime which is particularly focused to prevent the diversion of nuclear material for nuclear weapons purposes is Safeguards system. The concerns about diversions are particularly related to certain types of the fuel cycle facilities, i.e. enrichment and reprocessing facilities, as well as the facilities at which weapons usable materials are stored. NPPs, with the exception of those facilities that use fresh mixed oxide fuel, do not present the same opportunities for diversion (IAEA INFCIRC/153, corr, 1972).

The adequate protection of nuclear facilities and nuclear material is based on the "3S" approach, where synergy of Safety, Security and Safeguards is accomplished. During the years of nuclear facilities operation, sophisticated and comprehensive safety regime has been established, while the security regime is far less developed, although is receiving increased attention nowadays (IAEA, 2009). Even though the differences between the two domains in approach to the protection of nuclear infrastructure are evident, nuclear safety and nuclear security have a common, fundamental purpose — the protection of people, society and the environment. In addition, the presumption of the acceptable risk is the same regardless the initiating cause is a safety or a security event. It is necessary to ensure feasible interfaces between nuclear security and nuclear safety in a nuclear facility, as well as to design, implement and manage safety and security measures in a coherent and synergistic manner.

The operators of the nuclear facilities are responsible for the safety and security of their facilities in order to prevent unacceptable consequences. That comprises safety measures that are built in to prevent potential incidents and adequate arrangements to mitigate their consequences, as well as security measures to reduce the risk of internal or external malevolent actions and to counter internal or external action aimed at unauthorized removal of nuclear material.

Technical and organisational support for nuclear safety and nuclear security is provided by employing the fundamental protection systems, which includes physical protection, control, safety and emergency systems, and by implementing the prescribed safety and security measures.

The concept of physical protection initially emerged in response to the concerns about nuclear weapons security and the implementation of the strategic nuclear arms reduction treaties, and later was expanded to fissile materials and nuclear facilities, including those in the civilian sector. With the appearance of technical sophisticated non-state actors (militant extremists, criminals, etc.)[1] and terrorism the need has emerged to strengthen and improve physical protection measures.

In addition, cybersecurity has to be included in all hazards approach, following its increased importance for both nuclear safety and security in the recent years. Digital computer and communication systems and networks associated with safety, security and emergency preparedness functions at nuclear facilities, as well as instrumentation and control for support systems and equipment that might endanger these functions, need to be adequately protected against cyber attacks.

1 Definition from *United Nations Security Council Resolution 1540* (2004)

Each State has the responsibility to ensure the protection of nuclear material, other radioactive material, associated facilities and activities under its jurisdiction by creating an adequate nuclear security regime. However, nuclear security has become a matter of international concern and co-operation, especially when nuclear materials are transported across national borders.

2.1. Nuclear Security Regime

Protection of nuclear and other radioactive materials in use, storage, or transport, associated facilities and/or associated activities from criminal or intentional unauthorized acts, and other acts determined by the State to have an adverse impact, is the focus of nuclear security. The security activities comprise the prevention and detection of and response to theft, sabotage, unauthorized access, illicit trafficking or the inadvertent movement of nuclear and other radioactive material, as well as other malicious acts involving nuclear material and nuclear facilities (IAEA, 2007). Nuclear security system, as an integrated set of nuclear security measures and engineering safety measures for nuclear installations combined provide a comprehensive approach to nuclear security. For their effective implementation it is necessary to establish national nuclear security infrastructure that relies on the appropriate legal and regulatory framework, as well as supporting competent authorities which have defined the responsibilities and the interfaces between them. This task is the responsibility of the State. However, it has been recognised that regardless of the adequacy and effectiveness of nuclear security measures in one state, they might not be sufficient to detect and respond to the threats within state's territory, if not supported by the adequate measures taken by other States. This was the rationale for the increase in both regional and international cooperation, particularly during the nuclear material transport across national borders. The leading role in facilitating the regional and international efforts to enhance nuclear security, including measures to protect against nuclear terrorism, has belonged to the IAEA since the early 1970s.

The state accomplishes the goals of the nuclear security by creating the appropriate national nuclear security regime (IAEA, 2013). A set of recommendations endorsed by the IAEA (INFCIRC/225/rev 5, 2011) is a helpful guidance to States for the development or enhancement, implementation and maintaining a nuclear security regime for nuclear material and nuclear facilities.

2.1.1. Objectives and Principles of Physical Protection

The essential component of the nuclear security regime is the physical protection regime, the establishment of which is the full obligation of the State (Amendment to the CPPNM, 2005). The State's physical protection regime should be reviewed and updated regularly to reflect changes in the threat and advances made in PP approaches, systems & technology, and also the introduction of new types of nuclear material & facilities.

The objectives of the physical protection are to establish and maintain conditions to:

- Protect against deliberate malicious acts directed against a nuclear facility or nuclear material in use, storage or transport that could directly or indirectly endanger the health and safety of personnel, the public and the environment;
- Ensure the implementation of rapid and comprehensive measures by the State to locate and recover missing or stolen nuclear material;

- Mitigate or minimize the radiological consequences of a malicious act.

These objectives should be addressed in an integrated and synchronized approach taking into account the diverse risks included by nuclear security. There are 12 Fundamental Principles for physical protection that have to be applied as the basis for achieving the physical protection objectives (INFCIRC/225/revision 5, 2011). These principles encompass Responsibility of the State, *Responsibilities during International Transport, Legislative and Regulatory Framework, Competent Authority, Responsibility of the License Holders, Security Culture, Threat, Graded Approach, Defence in Depth, Quality Assurance, Contingency Plans and Confidentiality*.

Physical protection systems are realized through administrative and technical measures, including physical barriers. These measures are based on the state of the art in physical protection hardware and systems, and on the types of nuclear material and nuclear facilities. The protection of nuclear material from unauthorized removal and sabotage during transport is coupled with many challenges and is highly demanding; hence a specific approach is required, which is beyond the scope of this paper.

When designing the physical protection of nuclear material and facilities, the concepts of defence in depth and graded approach should be implemented for each of the essential physical protection functions - detection, delay and response.

The concept of defence in depth enhances the protection of targets by employing a combination of consecutive layers of physical protection systems and measures that have to be overcome or circumvented before physical protection is compromised. A graded approach is applied to provide physical protection measures proportional to the potential consequences of a malicious act, i.e. higher levels of protection against the threats that could result in higher consequences.

The level of risk which is acceptable and the corresponding level of protection against the particular threat that should be provided have to be determined by the State. In case of unauthorized removal, it is necessary to regulate the categorization of nuclear material and thus ensure an appropriate correlation between the nuclear material of concern and the physical protection measures.

The nuclear material itself (i.e., the different material types in terms of element, isotopic composition, physical and chemical form, quantity and irradiation history) is the most important feature for determination of the physical protection measures against any unauthorized removal. The categorization is performed considering the potential of nuclear material for use in the construction of a nuclear explosive device, which provides the basis for defining the levels of protection, and hence a graded approach for protection against the unauthorized removal. The categories of nuclear materials are presented in Table 3 (CPPNM, 1980). The protection is also obligatory for nuclear material that is not usable for weapons, but could be used for disposal (radiation-emitting device - RED), dispersal (radiological dispersal device - RDD or "dirty bomb") or other malicious acts causing significant consequences (Nikolic et al, 2012).

In case of sabotage, the State should define threshold(s) of unacceptable radiological consequences and thus determine the appropriate levels of physical protection, taking into account the existing nuclear safety and the radiation protection standards. The nuclear material categorization cannot be directly applied to protection against sabotage, although the requirements for the protection against unauthorized removal should also be taken

into account. Similar approach is applicable in reverse, so that the appropriate physical protection measures should be designed based on more stringent applicable requirements and implemented in an integrated manner for both unauthorized removal and sabotage.

Table 3. Categorization of nuclear material (Source: CPPMN, 1980)

Material	Form	Category I	Category II	Category III c
1. Plutonium a	Unirradiated b	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235	Unirradiated b uranium enriched to 20% 235U or more uranium enriched to 10% 235U but less than 20% 235U uranium enriched above natural, but less than 10% 235U	5 kg or more	Less than 5 kg but more than 1kg 10 kg or more	1 kg or less but more than 15g Less than 10kg but more than 1kg 10 kg or more
3. Uranium-233	Unirradiated b	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated Fuel f			Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content) d, e	

Note: This table is not to be used or interpreted independently of the text of the entire publication.

a. All Pu except that with isotopic concentration exceeding 80% in Pu-238.
b. Material not irradiatedr, or irradiated but with a radiation level ≤ 1 Gy/h at 1 m unshielded.
c. Quantities not falling in Category III & natural U, DU & Th should be protected at least in accordance with prudent management practice.
d. Recommended, but States may assign a different category of PP appropriate for the specific circumstances.
e. Other fuel classified as Category I or II before irradiation may be reduced 1 category level while the radiation level from the fuel exceeds 1 Gy/h at 1m unshielded.
f. Based on internat. *transport* considerations (State may assign a different category for domestic use, storage & transport)

2.1.2. Risk Management

Protecting all assets, systems, and networks against every possible or probable attack is not either feasible or practical. A risk-based approach driven by adequate threat evaluation (intelligence analysis and reporting) is crucial to an effective risk management strategy and efficient resource allocation. The risk acceptance criteria are described in terms of radiological consequences [CPPMN, 1980]. The nuclear threat is to be evaluated with

regard to the consequences defined by State, which are related to the safety of plant personnel and the public.

The main classes of malicious acts that are generally considered in regard to the protection of nuclear material and nuclear facilities, as recognised in the recommendations (INFCIRC/225/Revision 5, 2011) are:

- Unauthorized removal of nuclear material in use, storage and during transport, which includes a theft, robbery, an embezzlement or fraudulent obtaining of nuclear material, with the intent to: a) construct a nuclear explosive device; b) subsequently disperse material and causes or is likely to cause death, serious injury, substantial damage to property or the environment;
- Sabotage against a nuclear facility and of nuclear material in use, storage or during transport, which could directly or indirectly endanger the health and safety of personnel, the public and the environment.

Besides physical sabotage, the attempts of cyber sabotage to nuclear facilities have emerged as a major threat to facility operations and advanced Instrumentation and Control systems.

Malicious acts could also include gaining control of equipment or facilities for blackmail. Actions that are not committed directly at nuclear material and/or facilities, but could have an adverse impact on nuclear security are: a) Leakage of sensitive information in whatever form, including software, suitable for malicious use; b) Unauthorized acquisition, destruction, alteration, distortion of vital information in computer networks which could compromise nuclear security.

The major security concern is that terrorist attack on a nuclear facility might be attempted, and given the advancement of capabilities, tactics and increased militancy in the last decade, focus on defences against terrorists at nuclear facilities, as well as at other CIs, has been augmented. Subsequent to attacks in 2001, nuclear security was generally enhanced by improving physical protection with additional security devices, augmenting the forces guarding facilities, enhancing security procedures, tightening access control, increasing standoff distances for surface vehicles, reviewing and updating emergency preparedness.

Physical protection has to be designed in a manner that ensures that the anticipated risks, primarily those of unauthorized removal and sabotage, are established and maintained at acceptable levels. That is accomplished by assessing the threat and the potential consequences of malicious acts, by developing concepts, technologies and solutions to address the threats considered and by creating risk based physical protection systems and measures.

Risk can be managed by reducing the threat, improving the effectiveness of the PP system and/or reducing the potential consequences of malicious acts by modifying specific contributing factors.

3. THREAT EVALUATION METHOD

A fundamental principle of physical protection is that it should be based on current evaluation of a threat and associated capabilities, which is formalized through a threat assessment process. The State performs evaluation using various national and international credible information sources to define present and foreseeable threats to nuclear material, nuclear facilities and associated activities. Several organizations with different areas of ex-

pertise need to work closely together, such as intelligence and law enforcement agencies, military authority, regulatory authority, operators, research institutions and others.

The development of a threat basis for the design of physical protection consists of two main phases: 1) a **threat assessment,** and 2) an **evaluation and decision making** process carried out by the State that **results in a Design Basis Threat (DBT)** (IAEA, 2009).

A threat assessment is a formal process of gathering, systematizing and assessing information about the motivations, intentions and capabilities of existing or potential threats that could cause or lead to a malicious act. The result of this process is a Threat Assessment document (TAD), which is further utilised to derive a **design basis threat** - DBT, and in that manner facilitates the development of a security posture. The set of threats described in the TAD are modified to consider technical, economic and political issues, and the particular requirements of planning for the design of the physical protection system, thus creating a statement about the attributes and characteristics of potential adversaries (internal and/or external) – a DBT (IAEA, 2009).

The design basis threat is valuable tool commonly used to determine threat levels, and as a basis for the design, implementation and evaluation of the physical protection system. The State has overall responsibility, within its own policy and legislative framework, for the development, use and maintenance of a DBT, and for assigning the competent authority role to a single authority, or dividing it among several authorities. The competent authority should require from the operator to use a DBT and/or threat assessment for the development of a physical protection system for a nuclear facility, nuclear material and associated activities.

The process of threat assessment and the creation of TAD, DBT definition process and lifecycle are described and discussed, as well as issues and challenges related to the development and utilisation of these documents.

3.1. Threat Assessment

The threat assessment process basically consists of 3 stages: collecting the information, arranging and analysing them, and composing the output - TAD, as illustrated in Fig.2. A broad range of expertise from relevant disciplines is needed for assembling an appropriate team to carry out threat the assessment and the development of the DBT.

Therefore, various governmental agencies and organisations (intelligence, police, armed forces, border control and customs authorities), operators and researchers, are involved. They provide sources of information such as classified or unclassified material, official government reporting, incident reporting by operators and confirmed media reporting. State Intelligence Service may be the best source of information, although the efficient communication among all relevant agencies is essential, especially in case of real-time threat, when the real-time interaction is indispensable.

All reliable national and international sources of information should be considered, as well as relevant information regarding adversary characteristics for analogous hazardous industries with potential of high consequences. The credibility of the information has to be rigorously evaluated. The further utilisation of particular information depends on various source-related elements, such as whether or not the source has the first-hand access to the originator of the information, and whether or not the source is known to be reliable in transmitting information.

In that way a comprehensive compilation of information about all potential adversaries, their motivation, intentions and capabilities can be assembled. Additionally, various factors that can influence the potential adversaries should be taken into account and certain assumptions for use with the Threat Assessment have to be developed. For example, it may be assumed that there will be no advance warning for the attack, that it may occur in the peace or war time, and that potential threats may be both global and domestic. Also, it has to be pondered that potential adversary capabilities and behaviour may differ from those that have already been demonstrated.

Process of analysis

Collected information/data are analysed to identify, systematize and document the categories of threats (external and internal) and their characteristics (motives, intentions and capabilities) that have been evaluated as credible. The aim of the process is to provide a credible assessment of potential threats, not intended to define specific scenarios or the tactics that the adversary may use (IAEA, 2009). In that regard, it is crucial to identify what are the threat's motivations (political, ideological, personal, financial, psychological or other, e.g. coercion), what intentions the threat has (theft, sabotage, causing public panic and/or social disruption, mass injuries and casualties, environmental damage, disruption of the local/national economy), and what its capabilities are.

Potential threats that may be relevant to nuclear and other radioactive material, their associated facilities and transport should be analysed with particular attention. Furthermore, it may be required to gather an adequate intelligence related to a particular facility to ensure the completeness and relevance of the facility's threat matrix composition.

The scope, quality and comprehensiveness of the compiled data, influence not only the assessment of a current threat, but also a judgment regarding future behaviour of adversary groups or individuals. Many attributes and characteristics are necessary to precisely characterize a particular threat and enable the composition of a detailed **threat assessment matrix** for both external and internal threats. The most essential features that need to be considered for each threat in the assessment process, and a set of general threat types are presented in Tables 4 and 5.

The collection of information and data analysis are continuous activities, since the threat is dynamic in nature, and the analysis will often reveal the need for more information.

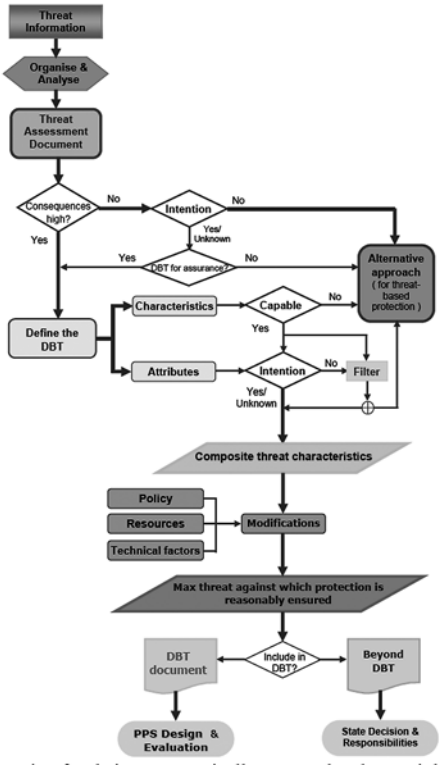


Figure 1 - The process of threat assessment and DBT development
(derived from IAEA, 2009)

The collection of information and data analysis are continuous activities, since the threat is dynamic in nature, and the analysis will often reveal the need for more information.

3.1.1. External threat

External threat categories generally comprise various kinds of protestors, criminals and terrorists. Resources, tools that are likely to be used and the motivations can substantially vary within each sub-category. The attributes and characteristics to be addressed for each general type of external threats to determine external threat assessment matrix are given in Table 4.

Protestors include demonstrators, activists or extremists, which are persons and organizations that protest for the same cause - against utilization of nuclear energy, but have different motives and intentions. Demonstrators are ideologically motivated and well-meaning individuals looking for media attention for their cause, typically unarmed and non-violent.

Activists have intention to gain political effect and attention of media, want government to abandon nuclear energy, and may be anarchists. They are educated, they make and use equipment skilfully, and they may attempt to enter controlled areas to demonstrate that the physical protection system of nuclear facility is ineffective.

Table 4 - External Threat Assessment Matrix

External Threat					
Features	**Protestors**			**Criminals**	**Terrorists**
	Demonstrators	**Activists**	**Extremists**		
Motivation (Ideological, political, financial, psychological)					
Intentions Theft / Sabotage / Vandalism					
Capabilities					
Tactics Force / stealth / deception					
Group size (number)					
Weapons					
Explosives (Type & amount)					
Tools (Power or hand tools)					
Transportation Ground, air, water					
Technical skills					
"Cyber" skills					
Funding					
Insider Collusion					
Support structure					
Other					

Extremists include different ideological/religious fanatics, right or left radicals, who are also intent on political effect and media attention, but their capabilities are more threatening. Organised in small groups, well educated and trained, they may be armed with conventional, commercially available firearms, and may attempt theft of material and cause sabotage.

Criminals conduct malicious acts solely for monetary gain, and therefore search for substance

that can be hastily exchanged for money. They might focus on a perceived value of fresh fuel or radioactive sources, and therefore attempt deceit, theft, fraud, coercion and extortion to obtain it. Criminals may cooperate with terrorists.

Terrorists, whether national or international, commit or threaten to commit violent acts to achieve political objectives and gain media attention. Usually they are highly trained and motivated, well equipped, willing to kill and/or die. Since international terrorists in particular have continually demonstrated flexibility, unpredictability and increased militancy, it is crucial to analyze their goals, objectives and developing capabilities, to obtain a wide view of the potential threat and postulated attack methods.

3.1.2. Internal threat

An insider is an individual with the authorized access to nuclear facilities, nuclear material or associated activities, or to sensitive information or its assets, who could commit unauthorized removal, sabotage, other criminal or intentional unauthorized acts or other acts determined by the State to have an adverse impact on nuclear security. An insider can also aid an external adversary to commit these acts. The advantages of having the authorized access, authority and knowledge to deceive and bypass security measures make the insider a severe threat to a nuclear facility. An insider may be any employee from the lowest level to the senior management, with violent or non-violent attitude. Motivation of the insider can be real or imagined ill-treatment, personality traits, mental illness, idealism, monetary gain, coercion by outsiders that lead to betrayal, revenge, etc. The attributes and characteristics to be addressed for each general type of insider to determine threat assessment matrix are presented in Table 5.

Table 5 - Internal Threat Assessment Matrix

Internal Threat					
Features	**Manager**	**Operator**	**Guard**	**Custodian**	**Maintenance worker**
Motivation					
Intentions (Theft / Sabotage)					
Capabilities					
Group size (number)					
Collusion with External threat / other Insider					
Passive / Active					
Violent / Non-violent					
Tools					
Weapons / Explosives					
“Cyber” skills					
Knowledge of sensitive information					
Access					
Authority / Control					
Knowledge of I & C systems					
Other					

However, a detailed analysis of insider threats has to be facility specific, which is plausible since there is a wide range of facility types to be protected (e.g. research reactors, NPPs and other nuclear fuel cycle facilities).

3.1.3. Threat Assessment Document (TAD)

The final stage of the threat assessment process results in a TAD which contains threat assessment matrices for all known credible threats that need to be taken into consideration

by the State, and the description of the overall threat environment. In addition, all available details about these threats and the credibility of the information should be provided. This document is further used as the basis for developing the DBT.

3.2. Development of a DBT

A DBT is a description of "the attributes and characteristics of potential insider and/or external adversaries who might attempt a malicious act, such as unauthorized removal of nuclear material or sabotage, against which a physical protection system for nuclear or other radioactive material or associated facilities is designed and evaluated" (definition in INFCIRC/225/Rev.4 (corr), 1999). Although derived from credible intelligence information, DBT is not intended to be a statement about the actual prevailing threats. The DBT represents the major reasonable threat that a facility should expect to be defended against, considering the current threat environment.

The DBT provides a rational basis for the design of physical protection system requirements for the operator and the State, for making and justifying potentially expensive decisions by the operators and the Competent Authority, and for evaluating the adequacy of an existing physical protection system. States use DBTs in their regulatory system to determine the appropriate allocation of resources to the protection of nuclear material and nuclear facilities from hostile actions (IAEA, 2011).

The basic factors considered in order to derive a DBT from TAD are:

1. **Potential adversaries (Insider/External adversary)** that may be any individual or group of individuals, estimated to have the intent/capabilities to commit a malicious act;
2. **Relationship between malicious acts** and **unacceptable consequences**;
3. The relevant **attributes** and **characteristics** of potential adversaries, which describe their motivation, intention and capability to commit a malicious act;
4. **Criteria for the design** and **evaluation of** an effective physical protection system;
5. A clear description of potential threats defines the conditions under which the physical protection system must perform and is therefore an essential prerequisite for the design of plausible and effective physical protection.

This document helps to ensure that the resulting DBT will be realistic and credible. The consequences deemed by the State to be unacceptable need to be understood by the CA developing the DBT.

3.2.1. DBT Definition Process

The DBT definition process is a process conducted by the competent authority that evaluates and analyses many factors to develop a DBT from the TAD, and makes necessary decisions that define what is included in the DBT and what is "beyond" the DBT. It is possible that some threats defined in the threat assessment will not be included in the DBT, but that protection against these threats will remain the responsibility of the State.

The evaluation for the DBT is based on several factors, including possible consequences of a potential malicious act, the type of the target, the likelihood of an attack, the resources for prevention and management of an event, as well as the resources needed for remediation. The State defines an unacceptable consequence, i.e. identifies a threshold of conse-

quence that is so severe as to justify that resources be expended to prevent its occurrence. The resources are expended by those organizations responsible for providing the protection (IAEA, 2009).

The analysis and decision making process for the DBT developments are schematically illustrated in Fig 1. This process encompasses 3 major phases:

1. Screening the TAD to identify those threats with motivation, intention, and/or capability to commit a malicious act.

The possible targets of potential malicious actions that could lead to unacceptable consequences are considered, and then these are compared to the attributes and characteristics of the postulated adversaries described in the TAD. The capabilities of the threat are firstly evaluated; if they are not sufficient to cause the unacceptable consequences, then the threat is removed from further consideration for the DBT. However, a conservative approach has to be exercised, and only the threats of the lowest capabilities could be excluded at this step of decision making. The remaining threats are screened further in the second step with regard to their motivation and intentions. If the threat, in addition to having sufficient capabilities, is also supposed to have sufficient motivation (or actual intention) to commit the malicious act, then this threat is stored for further consideration in Phase 2 of the process.

The output from this phase provides the range of credible threats that is capable and may be motivated or may have the intention to commit a malicious act leading to unacceptable consequences.

2. Conversion of the resulting screened list into a statement of representative attributes and characteristics of the postulated adversary.

The threats from previous phase should be re-examined with regard to their motivation, intentions and capabilities and the threat assessment matrices transformed into a set of representative adversary characteristics, which should not simply represent a combination of the worst characteristics of each threat. All the threat characteristics (i.e., motivation, intentions, and all the detailed capabilities including the number of adversaries) identified in the threat assessment process should be addressed.

3. Modifying the statement of the postulated representative threat on the basis of relevant policy factors.

Competent authority in conjunction with other State authorities defines relevant policy factors that have to be taken into account when reassessing the representative adversary characteristics from Phase 2. These factors include the degree of conservatism, cost–benefit optimisation and political factors. Consequently, the representative adversary characteristics from Phase 2 have to be adjusted in order to achieve more sustainable security levels and balance reliability of facilities operation against the costs of protection and the risks of the consequences of a potential malicious act.

The decision regarding what level of risk is acceptable and what level of threat it will protect against rests with the State, given the availability of protection resources, the benefit of the asset to society and other priorities. Risk, in this sense, is a combination of the severity of the consequences of a potential malicious act and the likelihood that the malicious act will be successfully committed. The competent authority should coordinate the con-

tent of the DBT with other relevant State authorities to gain consensus before finalization and introducing the DBT into the regulatory framework.

There are two outputs of the DBT definition process: the DBT document and a set of "Beyond the DBT" threats. The DBT document identifies the maximum threat capabilities against which protection will be reasonably ensured. This definition contains the capabilities for all potential threats against which the State has decided to develop specific protection measures.

The remaining threats are denoted as "Beyond the DBT", and identified as threats that are not appropriate for inclusion in a DBT but against which the State requires that protection should be reasonably ensured. The relationship between range of all threats defined in the threat assessment document and the DBT is illustrated in Fig 2.

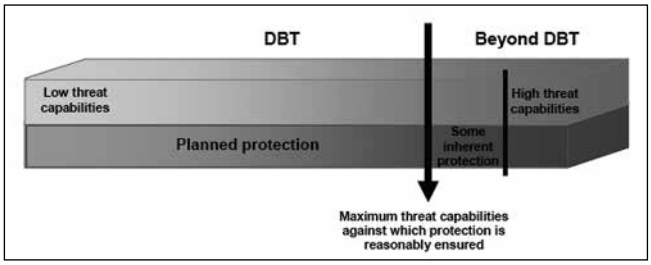


Figure 2 - The relationship between all threats defined in TAD and DBT

In the context of the increased focus on defences against terrorists at nuclear facilities, the new, extended approach to analysis of the beyond DBT events is needed, to include more severe attacks and evaluate physical and operational changes that may have to be made to nuclear facilities to mitigate their vulnerabilities. That comprises threats such are air attacks with a large commercial airliner, a smaller aircraft loaded with high explosives, land-based and/or water-borne attacks using high-explosive projectiles, and a moving suicide truck bomb.

In the past, airplane attacks were not regularly included in the DBTs even for NPPs, although some countries considered the impact of a small military aircraft crash for the NPP design. For example, NPPs in Germany which started operation in the 1970s were designed to withstand the crash of Starfighter (10t plane crashing at speed 180 m/sec), and those built after 1988 were designed against the "Phantom jet standard" (Hofer et al, 1998). The design here refers to the resistance of the containment building for the reactor and the primary cooling circuit, which is constructed of thick concrete heavily reinforced by steel, with a several centimetres thick steel lining. Nevertheless, the constructions of these NPPs will unlikely withstand the loads from the crash of a medium-sized passenger aircraft, let alone the loads from a large aircraft. The impact of a fully fuelled Boeing 767 flown into the NPP site is associated with the effects of flying debris and a jet fuel fire. However, the exact nature of the damage caused by such an attack would depend on the size of a plane, amount of fuel it carried, speed and angle of the impact.

In addition, cyber attacks have become increasingly threatening in the recent years, and therefore have to be included in a threat assessment and a DBT. Computer based systems used for physical protection, nuclear safety and nuclear material accountancy and control

systems should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the threat assessment or DBT.

A multimode threats, i.e. combination of different types of threat, such are attacks in which physical and cyber aspects are combined should be considered as well.

The DBT document should be maintained by establishing a formal review process, which could be triggered after a prescribed period of time, by occurrence of a significant event or a significant change in domestic or international regulation, policy, or guidance relevant to the DBT. Considering this, as well as the type and sensitivity of information provided in the DBT, the adequate structure of the document that meets these requirements is illustrated in Fig 3.

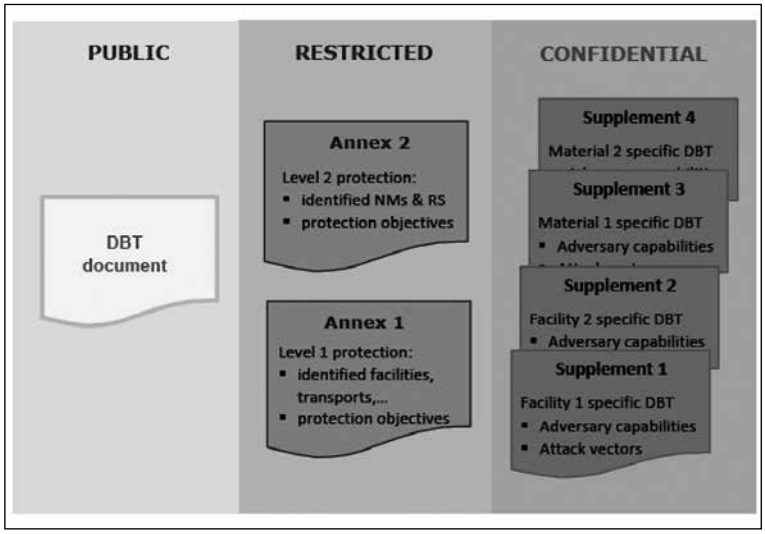


Figure 3 - Practical structure of the DBT document

4. CONCLUSION

Nuclear sector is identified as CI with the scope of sector definition that extensively varies, although nuclear power plants are considered as CIs in the majority of classifications, adopted by most of countries. Regardless of the particular definitions of "CI", Nuclear Sector protection has always gained special attention, primarily due to the fact that potential accidents could cause significant loss of life and property in addition to long-term, adverse environmental, public health and safety consequences. Therefore, nuclear safety and security are founded on the high operational and organisational standards and well regulated, covered by relevant nuclear legislation including international and multilateral treaties. The threats to nuclear infrastructure from major natural phenomena, operational failures and inadvertent human errors are primarily considered in the nuclear safety evaluations. Malicious acts intended to cause damage or steal material, circumventing protective measures, are in the focus of nuclear security assessments. The security activities comprise the prevention and detection of and response to theft, sabotage, unauthorized access, illicit trafficking or the inadvertent movement of nuclear and other radioactive material, as well as other malicious acts involving nuclear material and nuclear facilities.

Physical protection systems are realized through administrative and technical measures, including physical barriers, to protect against these malicious acts.

Focusing on security and preparedness from all-hazards approach enables the use of prevention, protection and response capabilities not only to reduce the threat of malicious acts toward nuclear facilities and material, but also to prevent or mitigate damage in the event of natural and/or unintentional manmade disasters.

In the current global situation, there is a particular concern regarding the possibility that nuclear or other radioactive material could be used for malicious purposes. This paper presents methods, systems and arrangements that are necessary for the protection of nuclear installations, nuclear material and associated activities. In particular, a threat assessment process and methodology for the development, use and maintaining of the design basis threat (DBT) are presented. A DBT is the State's description of a representative set of attributes and characteristics of adversaries, based upon (but not necessarily limited to) a threat assessment, which the State has decided to use as a basis for the design and evaluation of a physical protection system. DBT indicates the largest reasonable threat to a facility that should be expected to be defended against. The threats that are not appropriate for inclusion in a DBT are identified as the "Beyond the DBT", but against which the State requires that protection should be reasonably ensured.

In the context of the increased focus on defences against terrorists at nuclear facilities, the new, extended approach to analysis of the beyond DBT events is needed, in order to include more severe attacks. That comprises the threats from air attacks with a large commercial airliner, land-based and/or water-borne attacks using high-explosive projectiles, and a moving suicide truck bomb, as well as cyber attacks which have become increasingly threatening - for both nuclear safety and security in the recent years. Multimode threats, i.e. a combination of different types of threats, such are attacks in which physical and cyber aspects are combined, should be considered in the threat assessment process as well.

REFERENCES

1. Amendment to the CPPNM (2005). Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10–GC(49)INF/6, IAEA, Vienna
2. EC (2006) Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, COM (2006) 787 final
3. EC (2008). Council Directive 2008/114/EC of 8 Dec 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal L*, *345*(23), 12
4. Executive Order 13228 (2001) Establishing the Office of Homeland Security & the Homeland Security Council. Federal Register, Vol.66, No.196, 2001, pp51812-51817
5. Congress, U. S. (2002). Homeland Security Act of 2002, *Public Law* (107)
6. CPPMN (1980). "The *Convention on the Physical Protection of Nuclear Material* (CPPMN)", published as IAEA/INFCIRC/274/Rev.1
7. Hofer, P., Kromp, W., Seidelberger, E, Sholly, St.: Comments on the Safety of Khmelnitsky Unit 2 & Rivne Unit 4 in the Frame of the Public Participation Procedure of EBRD; Report to the Austrian Government, Vienna, 1998
8. HSPD-7: Homeland Security Presidential Directive 7 (2003). Critical Infrastructure Identification, Prioritization & Protection. US DHS, Washington DC, USA. http://www.dhs.gov/ xabout/laws/gc_1214597989952.shtm
9. IAEA INFCIRC/153 (corrected) (1972) The Structure and Content of Agreements Between the Agency and States Required in Connection with the treaty on the Non-Proliferation of Nuclear Weapons. International Atomic Energy Agency, Vienna
10. IAEA INFCIRC/225/Rev4 (corrected) (1999) IAEA, The Physical Protection of Nuclear Material & Nuclear Facilities, IAEA, Vienna
11. IAEA INFCIRC/225/Rev5 (2011) IAEA Nuclear Security Recommendations on Physical Protection of Nuclear Material & Nuclear Facilities, IAEA, Vienna
12. IAEA (2010). INSAG-24: The Interface Between Safety & Security at NPPs, A report by the International Nuclear Safety Group, IAEA, Vienna
13. IAEA (2009). NSS 10: Development, use & maintenance of the design basis threat, Implementing Guide, IAEA, Vienna
14. IAEA (2011). NSS 17: Computer Security at Nuclear Facilities, IAEA, Vienna
15. IAEA (2013). NSS 20: Objective & essential elements of a State's nuclear security regime: nuclear security fundamentals, IAEA, Vienna
16. IAEA PRIS (2012). Power Reactor Information System, http://www.iaea.org/pris
17. IAEA RRDB (2012). Research Reactor Database, http://www.iaea.org/worldatom/rrdb/
18. IAEA (2007). IAEA safety glossary: terminology used in nuclear safety and radiation protection: 2007 edition, IAEA, Vienna
19. IAEA-TECDOC-1613 (2009). *Nuclear Fuel Cycle, Information System, A Directory of Nuclear Fuel Cycle Facilities, 2009 Edition,* IAEA, Vienna

20. ISIS (2003). Global Stocks of Nuclear Explosive Materials, Institute for Science & International Security, Washington, DC, USA, http://www.isisonline.org/global_stocks/end2003/tableofcontents.html
21. National Strategy for Homeland Security (2002). Office of Homeland Security, Washington DC
22. National Strategy for the Physical Protection of Critical Infrastructures & Key Assets (2003).Washington DC
23. Nikolić,D., Kovačević,A., Stanković,S. (2012). "Comprehensive approach to tactical response in the case of terrorist acts involving WMD", book "Managing the consequences of terrorism attacks – Efficiency & Coordination Challenges", Institute for Corporative Security Studies, Ljubljana & Centre for Civil-Military Relations, Naval Postgraduate School Monterey, USA, pp 99–117
24. Rinaldi, S.M., Peerenboom, J.P, Kelly, T.K. (2001). Identifying, understanding & analyzing critical infrastructure interdependencies. *Control Systems IEEE*. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=969131

Acknowledgement

This work is supported by the Ministry of Education, Science and Technological Development, Republic of Serbia.

UDC 726.9:75.041.5
ID 176374796

Dejan Radović
University of Belgrade, Faculty of Biology
dejanr@bf.bg.ac.rs

Ivica Radović, Vladimir Jakovljević, Zoran Čvorović
University of Belgrade, Faculty of Security Studies
ivica.radovic@mpn.gov.rs
vladimir.jakovljevic@fb.bg.ac.rs
zoran.cvorovic@fb.bg.ac.rs

Boban Tomić
National Park Tara & University Singidunum, Belgrade
boban.tomic@nptara.rs

IMPLEMENTATION OF GIS TECHNOLOGIES IN THE MANAGEMENT OF NATURAL PROTECTED AREAS: CASE STUDY NP TARA (SERBIA)

Abstract: A GIS is a computer-based system used to input, store, manipulate, analyze and output spatially-referenced data. There is a huge range application with regard to GIS; they include topographic base mapping, socio-economic and environmental modelling, and global modelling to education. Applications generally set out to fulfil the five Ms of GIS: mapping, measurement, monitoring, modelling and management. The system of environment is highly complex and most of the problems with the environment are multifactor and require the analysis of a wide spectrum of information resources, questions and interests. For ecologists, GIS has opened many new possibilities for research and the application of gathered information. Management of natural protected areas represents some of the earliest application of GIS in environmental study. The global Nature-GIS program, i.e. European Thematic Network for Protected Areas - Preservation and Geographical Information, set up in 2002 by the EU Commission, aimed at the creation and application of new Guidelines to implement GIS in protected areas, is an excellent example of this.
Keywords: *GIS, natural protected areas, geodiversity, biodiversity, sustainable managing, landscape resources*

1. INTRODUCTION

In Serbia there are 463 protected natural areas, covering 527,152 ha, which is equivalent to 5.91% of the national territory. Five of the protected natural areas are National Parks: Mt. Fruška gora, Mt.Tara, Mt. Kopaonik Mt. Šara and the Djerdap gorge, covering 158,853 ha (Ministry of Energy, Development and Environmental protection of R. Serbia, 2012).

Mt. Tara is a unique example of preserved forests in Southeastern Europe with exceptional biodiversity including numerous endemic and relict species of flora and fauna. It is also characterized by specific geomorphologic, hydrological, geological, soil and climatic features. Mt. Tara is on the list of Important Bird Areas of Europe (IBA) (Puzović, Grubač, In: Heath, Evans, 2000) and Prime Butterfly Areas in Europe (PBA) (Jakšić, In: Swaay, Warren, 2003). There is an initiative to include Mt. Tara on the list of Important Plant Areas (IPA) in the Central and Eastern Europe (Stevanović, 2002). Mt. Tara recognized

and identified as Important Species Area (biodiversity hotspots) may play a key role in the development of the Pan-European Ecological Network.

During the Joint International Workshop on MAB Biosphere Reserves and Transboundary Cooperation in southeastern Europe Region (held in Belgrade in June, 2004, under the auspices of the UNESCO/ROSTE – IUCN) Mt. Tara NP was nominated for the MAB Reserve in Serbia as transboundary "Peace Park" between Serbia and Bosnia & Herzegovina (Radović, 2004b). The MAB status of NP is still under consideration.

The first attempt to declare Mt. Tara for a National Park was made in 1951, but Mt. Tara NP was not established until 1981 year. In order to manage it effectively, it is divided into five managing units containing 751 parcels and sub-parcels in all (Spatial Plan of Tara NP, 2010).

There is the question whether it is possible to optimally manage such a complex natural system using "traditional" data sources like paper maps and statistical books. The decision making processes in management and protection of complex natural systems require numerous data, cartographic as well as statistical, needed to produce necessary information in an efficient way. The response to the demands is searched in the functionalities of a geographic information system (GIS) as a computerized system that facilitates the phases of data entry, data analysis and interpretation and data presentation.

As nature conservation poses a complex problem, a key goal of this kind of study is to bring specialists from different disciplines together who will jointly help in applying GIS to this crucial field (Ashdown, M., Schaller, J. 1990; Wadsworth, R., Treweek, J. 1999; Convis, Ch. (Jr.) 2001; Dragut, G., Thompson, C. 2005; Longley *et al.* 2005). This type of research is fully in line with global Nature-GIS program, i.e. European Thematic Network for Protected Areas/Preservation and Geographical Information, set up in 2002 by the EU Commission, aimed at the creation and application of new Guidelines to implement GIS in the protected areas (www.gisig.it/nature-gis).

Therefore, the purpose of this study is to design the GIS consisting of reliable data for assessment of the natural resources and to provide the reasonable ground for sustainable managing landscape resources and to protect the area with high biological diversity. The first time GIS was implemented on nature protected area in Serbia in 2006 just in Tara NP within the project at the Faculty of Biology, University of Belgrade: "The application of GIS technology in the evaluation and protection of natural potential of NP Tara" financed by the Ministry of Science and Environmental protection of the Republic of Serbia (Radović, D., Radović, I, 2006). GIS tools have had the full use and as part of the project at the Faculty of Security Studies, University of Belgrade: "Protected areas of Serbia, security risks and control instruments of protection" financed by the Ministry of Science of the Republic of Serbia (Čvorović *et all.* 2011).

2. RESEARCH METHODS

2.1. Study Site

Mt. Tara NP is located in the south-western part of the Republic of Serbia, within the territory of the municipality of Bajina Bašta, 180 km from Belgrade between 43°52'30'' and 44°01' North and 19°14'30'' and 19°41'30''East. The Park covers an area of 19,175 ha, while the protected buffer zone surrounding it covers an area of 37,584 ha. The highest point of Mt. Tara is Kozji rid 1,591 m, while the lowest point is at 300 m. There are two characteristic spatially-functional areas within Mt. Tara NP: High Tara (11,562 ha) and Flat Tara (7,613 ha). The average altitude ranges from 1,000 – 1,200 m. Based on these characteristics Mt. Tara is classified as medium-high Mountain in Serbia.

2.2. Study Procedure

In order to create functional GIS for Mt. Tara NP, the accent was put to selection and creation of thematic data layers for analyzing natural values through consultations with experts from various fields. The relevant studies on the Park were reviewed and field surveys conducted to collect and check all necessary data on the landscape resources. The data, mostly in analogue form had to be transformed into digital form and then organized in the meaningful system of thematic data layers. The procedures also included database creation, adopting GIS guidelines in terms of resource data analysis and conclusion drawing.

2.3. Input Data

All data were geo-referenced in the Serbia National projection system. This is a geodetic datum-based system – Hermanskogel with prime meridian in Greenwich and ellipsoid Bessel (major axis – 6 377 397.155 m, semi major axis – 6 356 078.963 m). Projection is defined as Transverse Mercator (Gauss-Kruger) with the following parameters:

Latitude of origin	0°00′00.00″
Longitude of origin	21°00′00.00″
Scale factor at central meridian	0.9999
False easting	7 500 000.00 m
False northing	0 000 000.00 m

To create thematic data layers, relevant input data from a large number of data sources were used: the Vegetation map of Tara NP: 1:50,000; the Map of five managing units of Tara NP: 1:50,000; the Map of five managing units of Tara NP (with 751 parcels): 1:10,000; Managing units data, consisting of nine properties for each parcel (unit name, parcel and sub-parcel ID number, woodland type, vegetation communities, vegetation ecological affiliation according to the type of soil, percentage of vegetation communities, type and purpose of land use, level of protection - zoning), the data on the fauna and flora diversity, the Tourist map of Tara NP 1: 25,000; Corine Land Cover 2000 (CLC 2000) 1:100,000, Corine Land Cover Changes (1990 - 2000) 1:100,000.

2.4. Thematic data layers creation

We applied the procedures used in most GIS projects: scanning, geo-referencing, digitizing (manual and semiautomatic), database creation and data integration (Radović, 2004a).

The Mt. Tara NP GIS is divided (by type and format) into various data forms: raster data, vector data, digital elevation model and database. Raster data include all maps, aerial photographs and satellite images (cited in data sources) after having been geo-referenced. The following entities are represented in vector form: Geology (polygon), Soil (polygon), Hydrology (line/polygon),Vegetation communities (polygon), CLC 2000 (polygon), CLC Changes (1990-2000) (polygon), Locations of important species of flora and fauna (point), Border of Tara NP (polygon), Management units (polygon), Management units parcels (polygon), Settlements (polygon), Roads (line), Mountain paths (line) and Other structures: hotels, belvederes, waterfalls, caves, (point).

The GIS software used to organize these data are: Geographic Transformer (geo-referencing raster data), MicroStation (manual digitizing), Raster to Vector (semiautomatic digitizing), and ArcGIS 9.3 (digitizing, vector data and data base integration, creation of grid raster data; analyses).

3. RESULTS AND DISCUSSION

We used GIS to analyze natural values and resources that significantly contribute to the proclamation of Mt. Tara for a future UNESCO MAB Reserve. In order to understand the current status of the study site thematic data layers in our GIS were logically organized in three sets of data on the National Park:

- Physical data, i.e. topography (elevation, slope, aspect), geology, soil, hydrology, watersheds and climate;
- Biological diversity data, (vegetation community, flora and fauna) and distribution of endemic and relict species;
- Managing mechanisms data and identification of current human pressure that may lead to violation of natural habitats.

3.1. Topography/Geomorphologic characteristics

To achieve the maximum effect of visualization, 3D analyses were used throughout this GIS study. Analyses demand that certain phenomena be correlated with relief characteristics: elevation, aspect, and slope. To meet the set requirements, a digital elevation model (DEM - resolution 20 m pixels) was created. The DEM covered an area of about 1,200 km^2 providing for each pixel: coordinates (in meters), elevation (in meters), aspect (in degrees), and slope (in degrees and percentages) (Fig. 1).

The elevation value in all Figures and 3D models is authentic (Z factor is 1.00 and H=100 %), so relief images are absolutely realistic and appear as in nature. The 3D model lies on a rectangle, which represents the sea level (altitude is zero meters) (Fig. 2).

Relief and hydrology maps were included as input data for DEM development. The Managing procedure included scanning maps and geo-referencing, as well as semiautomatic digitizing of isolines. After that, each isoline was given a unique identification (ID) and then converted to points (retaining ID), which were finally interpolated to grid (DEM) by spline method. Topography is a dominant factor affecting processes occurring on the

Earth's surface. It interferes with spatial climate distribution, and consequently with the distribution and productivity of biological systems (Manojlović, Dragićević, 2002).

The GIS analyses of the National Park's topographic characteristics included: elevation zones, relief aspect and slope. Thus, it was established that most of the Park area is situated at altitudes ranging from 800-1,200 m (12,571 ha or 65.56%) (Fig. 2), north (2,853 ha; 14.9%), northeast (3,604 ha; 18.8%) and northwest (2,199 ha; 11.5%) aspects cover most of the Park. The slope between 0-9.1% covers 4,964.2 ha (25.9%), between 9.2-18.3% covers 5,363.4 ha (28%), between 18.4-27.4% covers 3,895.4 ha (20.32%) and slope between 27.5-36.5% covers 2,768.2 ha (14.44%) of the Park area. It is possible to correlate and analyze the distribution of biotic elements to topography data as well as all other themes.

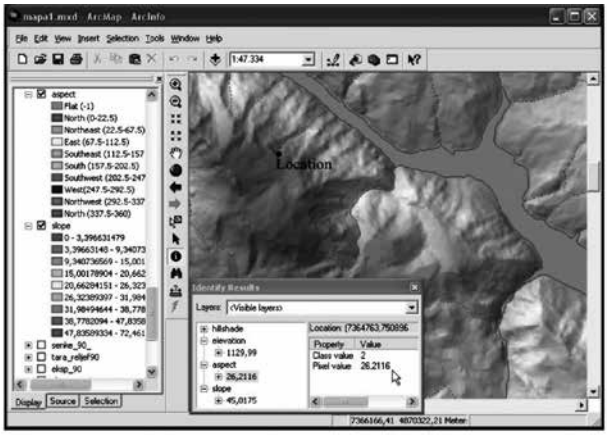


Figure 1 - Coordinates, elevation, aspect and slope for chosen location -2D (Radović, 2004a)

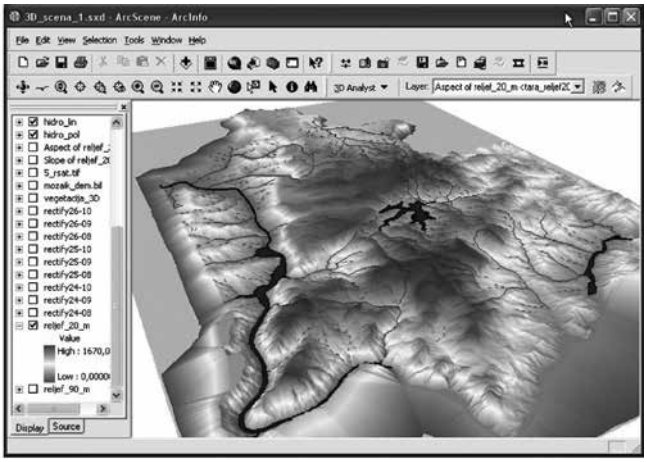


Figure 2 - Digital elevation model -3D (Radović,D, Radović, I., 2006)

Aerial photograph. The material used to process aerial photographs included a series of 19 photos of Tara NP (scale, 1:30,000; Wild RC-5 camera, year of production 1959). By using photographs that are almost 50 years old, we were able to observe changes in vegetation, some of which were caused by human impact. The processing of these photographs included scanning (resolution 750 dpi greyscale), geo-referencing, and their combining with other data (vector and DEM) (Fig.3).

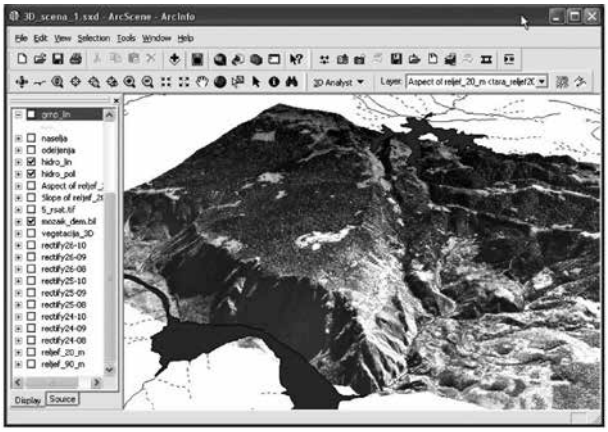


Figure 3 - Aerial photo from 1959: geo-referenced, combined with DEM and actual hydrology -3D (Radović, 2004a)

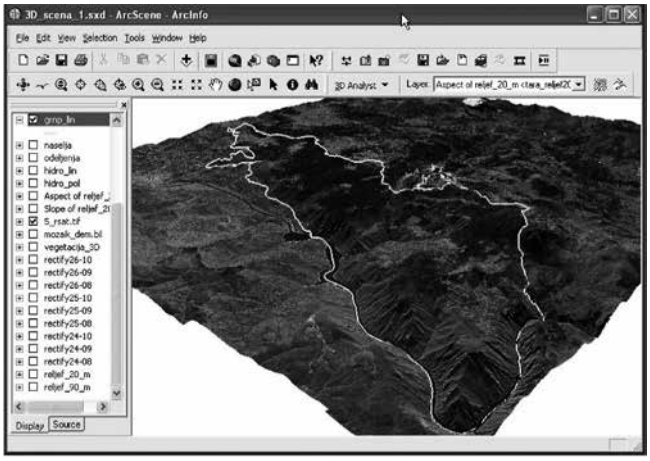


Figure 4 - Satellite image combined with DEM and Park border -3D (Radović,D., Radović, I., 2006)

Satellite images. For this study several types of satellite images were used: Landsat 7 ETM+ Multispectral, SPOT 5 multispectral, pan sharpened. After satellite images were combined with other data (raster, vector, data base and DEM), the authentic visualization of the area (satellite images and aerial photos were joined to the DEM in 3D analyst) was

obtained (Fig.4). Simultaneously the vector data were integrated with the database to represent qualitatively and quantitatively abiotic, biotic and human content.

3.2. Geologic characteristics

The complex of Mt. Tara is characterized by high geological diversity with respect to age, origin and composition. There are rocks from the Carboniferous, Triassic, Jurassic, Cretaceous, Tertiary and Quaternary.

The GIS analyses of geology covered a total area of 34,351 ha. Authentic content was classified into 35 types of geologic cover. In order to make adequate correlations, primarily with the vegetation, a generalization into six basic and six combined types was performed (Tab. 1). Inside the Park, limestone constitutes 77% of the rock.

Table 1: Distribution of geology (absolute and proportional) (Radović, 2004a)

Geology	Area (ha)	Area (%)
Limestone	14,778.13	77.07
Mostly clastites	1,381.11	7.20
Clastites	328.66	1.71
Mostly clastites with carbonates	95.53	0.50
Serpentinites- ofiolites (peridotites)	736.50	3.84
Ofiolites	700.82	3.65
Metamorphite	941.49	4.91
Free fluvial	130.58	0.68
Serpentinites- ofiolites	6.24	0.03
Mostly clastites (meta sediments)	24.90	0.13
Decomposed substrate	43.77	0.23
Mostly metamorphite	6.83	0.04
total	19,174.56	100.00

3.3. Soil characteristics

The soil cover of the area of 55,024 ha was digitized. The following ten types of cover are present: skeletal-rocky ground, chernozem on serpentines (humus silicate soil), alluvial deposit, deluvium, brown reddish soil on limestone, calcareous-skeletal soil on firm limestone, brown skeletoid soil on schist, parapodsol-gleized soil, eroded smonitza (shallow), and skeleton soil on serpentines. There are five types of soil cover inside the park.

3.4. Hydrologic characteristics

The most conspicuous hydrological characteristic of the park is the Drina River (total length 346 km; 22.7 km running around the park) and its canyon. The Drina forms a can-

yon over 1,000 m high on the park's boundary line. There are three reservoirs in the region of Tara NP: Perućac, Zaovinsko Lake (altitude is 600 m above Perućac) and Kruščica. The Perućac Reservoir (50 km long, area 12.4 km^2, max. depth 85 m) was created when a dam (93 m high and 461 m long) was built in 1962 to provide hydroelectric power for Bajina Bašta. Zaovinsko Lake belongs to the artificial reversible type used to preserve water for the hydroelectric power during dry season. Kruščica is used only for the supply of drinking water for the whole region.

The GIS theme Hydrology includes all hydro elements present in Mt. Tara: streams, rivers, and lakes. It is possible to get information about the length of every watercourse or its stretches. The data provides information about the ichtyofauna present.

3.5. Analyses of vegetation and floristic diversity

The complexity of the topography, geology, soil, hydrology and climate of Mt. Tara is readily evident from the distribution of vegetation. Within its spacious area at the altitude from 900–1,200 m, almost all species of European boreal dendroflora and their communities occur. All communities of mixed deciduous-coniferous forests and coniferous forests are spread like a mosaic, dependent on the aspect and slope of the relief.

The vegetation map (Mišić, 1988) for the area of 28,244.5 ha was digitized, being differentiated into 35 vegetation communities consisting of 354 polygons. The attribute data are Serbian and Latin names. Inquiries, arising from the database, allow obtaining the data on the size of every polygon and all other statistical indices regarding the distribution of vegetation communities (Fig. 5). Vegetation parameters can be readily correlated to all other themes, e.g. how the vegetation distribution corresponds to the type of geology, soil, elevation zones as well as to relief slope and aspect.

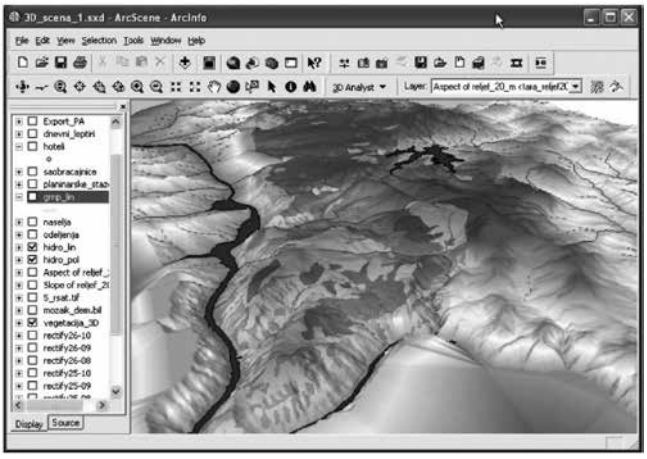


Figure 5 - Vegetation combined with DEM and hydrology - 3D
(Radović, 2004a)

Until now, 1,013 plant species have been recorded in Mt. Tara which accounts for almost 1/3 of the entire flora of Serbia (Stevanović, 2002). With large number of relict and endemic species, Mt. Tara is one of the centres of floristic and vegetation diversity not only in

Serbia but also in this part of the Balkan Peninsula. In this floristic diversity of Mt. Tara of greatest interest is certainly the Serbian (Pančić's) spruce, *Picea omorika*, a unique paleo–endemic species and a living fossil of the European dendroflora with a range confined to the middle course of the Drina River in Western Serbia and Eastern Bosnia and Herzegovina (Gajić *et al.* 1994). Locations of important endemic and relict plant species were mapped with GPS (*Picea omorika, Micromeria croatica, Centaurea derventana, Euphorbia glabriflora, Acer heldreichii, Spirea cana, Daphne malyana, Leontopodium alpinum, and Aquilegia grata nikolicii*).

Owing to this high floristic diversity, the initiative taken for including Mt. Tara in the International Plant Areas (IPA) list is absolutely justifiable (Stevanović, 2002).

3.6. Analyses of fauna diversity

In addition to floristic and vegetation diversity, one of the most important characteristics of the natural resources of Mt. Tara is the high diversity of its fauna (Radović, 2004a) (Tab. 2). The special value to the fauna of Mt. Tara is lent by the presence of the grasshopper *Pyrgomorphulla serbica*, an endemorelict from the Pliocene. Among other insect species, the occurrence of three butterfly species (*Euphydryas maturna, Maculinea arion,* and *Parnassius apollo*) is very important. They qualify Mt. Tara as one of the Prime Butterfly Areas (PBA) in Europe. Thus, since 2003, Mt. Tara is on European PBA list (YU-14) and a priority site for conservation (Jakšić, 2003).

Table 2: Numerical synopsis of fauna diversity in the region of Mt. Tara and Serbia (Radović,D., Radović, I., 2006)

Region / Taxa	Mt. Tara	Serbia	Mt. Tara/ Serbia (%)
Butterflies	115	192	59.9
Freshwater fishes	27	91	29.7
Amphibians	12	23	52.2
Reptiles	12	26	46.1
Birds	170	350	48.6
Mammals	51	107	47.7

There are three important fish species in Mt. Tara: Danubian salmon *(Hucho hucho*), brown trout *(Salmo trutta*), and grayling *(Thymallus thymallus*) (Simonović, 2001). Some of the important amphibian and reptile species are: *Salamandra salamandra, Rana graeca, Zootoca (Lacerta) vivipara, Vipera ammodytes*.

At the proposal of Serbian ornithologists (Puzović and Grubač, 2000), this area was nominated as one of the Important Bird Areas (IBA) of Europe. The nomination was accepted (as IBA 019) for the following six bird species: *Aquila chrysaetos, Falco peregrinus, Otus scops, Picus canus, Picus viridis, and Phoenicurus phoenicurus*, the population of which in Mt. Tara is larger than 1% of the total world populations. Among other important bird species of Tara NP are *Picoides tridactylus* and *Tetrao urogallus*.

The mammal fauna of Mt. Tara is characterized by the presence of the following large species: *Ursus arctos, Canis lupus, Rupicapra rupicapra, Sus scrofa, Felis sylvestris, Capreolus capreolus, Martes martes, Martes foina, Meles meles,* and (recently) *Lynx lynx*. The bear, *Ursus arctos*, is the symbol of Mt. Tara and is a characteristic resident of the western part of the mountain. Based on intensive monitoring of the bear population, the estimated number today is about 30 individuals. The chamois, *Rupicapra rupicapra*, is the second protected species of large mammals. It is present on steep limestone peaks, cliffs, and hillsides. Today it numbers about 100 individuals (Savić *et al.* 1995). The presence of the great vole (*Microtus multiplex*) is very important. Its habitat in Mt. Tara is the only one in Serbia, and at the same time the easternmost point of its range in Europe. The distribution of all the mentioned fauna species in Tara NP is mapped with GIS.

As a PBA, an IBA and an IPA, Mt. Tara has all the characteristics required for joining the Pan-European Ecological Network (PEEN), which is a tool of the Pan European Biological and Landscape Diversity Strategy (PEBLDS), and can be seen as one of the priority issues for nature conservation in Europe (Council of Europe, UNEP & ECNC 1996).

3.7. GIS and Management in NP Tara

In order to manage Mt. Tara NP effectively, it is divided into five managing units which are composed of 751 parcels and sub-parcels. By now the managing of almost all natural potentials of Tara NP was mainly based on principles of forestry technology. In this GIS study all 751 parcels of five managing units were digitized. For each parcel, the following eight characteristics were put together in the relational database: unit name, parcel and sub-parcel ID number, woodland type, vegetation communities, vegetation ecological affiliation according to the type of soil, percentage of vegetation communities, type and purpose of land use, and level of protection - zoning. Database consists of eight tables with 2,978 rows. Queries about combination of forest species distribution for every parcel in percentages are enabled. When we identify the present distribution of endangered endemic species we can easily calculate other areas in NP that fulfil similar combination of forest species and other biotic (vegetation, CLC) and abiotic (relief, hydrology, geology and soil) conditions present in those parcels and then try to spread that species (Fig. 7; Fig. 8).

The GIS of Tara NP also includes information about the nature reserves, settlements, roads and transportation, tourist facilities and line of visibility.

Nature reserves. There are ten nature reserves within Tara NP. The data model enables obtaining information about area, zoning, and the presence of specific plant and animal species.

Levels of protection. In accordance with the spatial plan of NP Tara land use zoning of the area is caused by the first, second and third levels of protection. The first protection zone coverage 2,959.25 ha or 15.43% of territory, the second 7,721.89 (40.27%) and the third 8,439.86 (44.30%) while the wider area of the NP with buffer zone covers 37,584 ha (Fig. 6, Fig. 7).

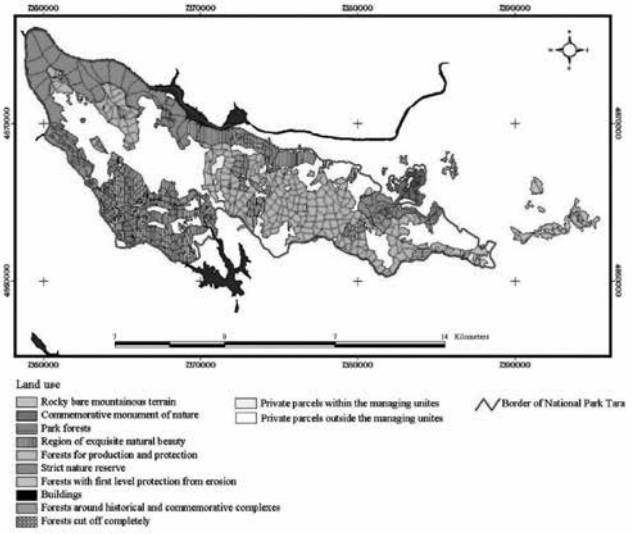


Figure 6 - Type of land use -2D (Radović, 2004b)

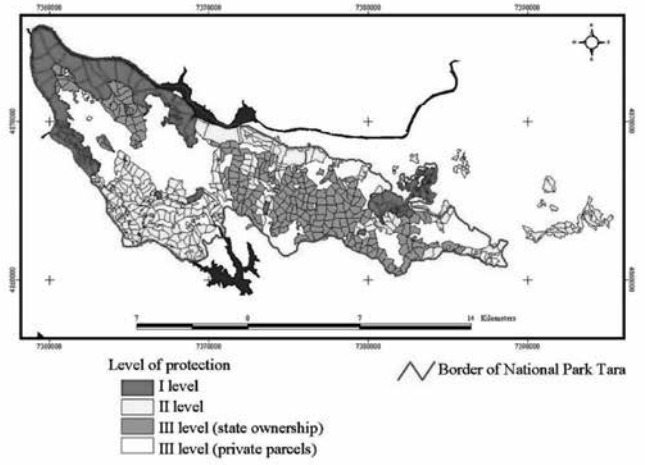


Figure 7 - Level of protection - zoning - 2D (Radović, 2004b)

Settlements. The settlements theme was digitized on the basis of topographic map (in digital raster form). All urban and rural settlements within the National Park are included. The biggest settlement is Bajina Basta, the administrative centre of the municipality.

Roads and transportation. The roads theme was digitized from a topographic map on a scale of 1:50.000 (in a digital raster form) representing all types of roads. The roads were divided into three categories: asphalt, macadam, and dirt roads. All digitalization rules have been followed, so that queries enabled getting of precise information about the length of every section and the shortest road distance between any of two points or crossroads in Mt. Tara.

Tourist contents. A tourist map of Tara NP was the basis for digitizing hotels, mountain paths, scenic sights, administrative buildings and cultural monuments.

Line of visibility. This GIS allows presenting the line of visibility from any point on the DEM, giving information about visibility, relief profile, starting and end points of the elevation, and the distance between these two points. This is of particular interest from the stand point of tourism, mountaineering, telecommunications, and defence.

3.8. GIS and CLC 2000 Serbia

For the interpretation of habitats diversity in NP Tara, we used a seamless vector database (CLC 2000 Serbia & Montenegro, 2006) which follows standard methodology of CLC 2000 (**C**orine **L**and **C**over) as a part of the European Commission Programme to **CO-RINE CO**o**R**dinate **IN**formation on the **E**nvironment Habitats Codes by EEA (European Environmental Agency, 2006) aiming to provide information about land cover resources, environmental monitoring and national/regional spatial planning strategies. The I&CLC 2000 project in Serbia and Montenegro aims to provide a satellite "snap shot" of Serbia and Montenegro (IMAGE 2000) (Nestorov, Protić, 2006).

The CLC nomenclature described in CORINE Land Cover Technical Guide is a physical and physiognomic land cover nomenclature relevant for the environment, nature and landscape protection. It distinguishes land cover classes grouped in a 3-level hierarchy. The classes of the first level are: (1) artificial surface, (2) agricultural areas, (3) forests and semi-natural areas, (4) wetlands and (5) water bodies. In a second level there are 15 land cover classes and in third there are 44.

Land Cover in Serbia is characterized by 29 out of 44 classes of the third level of CORINE Land Cover Nomenclature. On the territory of the NP Tara (19,150 ha) we have distinguished even 11 CLC third level classes (Tab. 3; Fig. 8), a convincing fact about high habitat diversity.

Table 3: CORINE Land Cover Classes for the year 2000 (Acording: CLC 2000 Serbia, (Nestorov, Protić, 2006)

	Code	CLC Class	Polygons	Area (ha)	Area (%)
1	231	Pastures	8	352.14	1.84
2	242	Complex cultivation patterns	6	54.34	0.28
3	243	Land principally occupied by agriculture, with significant areas of natural vegetation	32	1,041.34	5.44
4	311	Broad-leaved forest	21	5,190.05	27.1
5	312	Coniferous forest	14	990.73	5.17
6	313	Mixed forest	6	8,639.93	45.13
7	321	Natural grassland	6	194.17	1.01
8	324	Transitional woodland/shrub	23	2,490.46	13.00

9	331	Beaches, dunes, sands	1	5.53	0.03
10	511	Water courses	3	86.82	0.45
11	512	Water bodies	2	104.95	0.55
To-tal			122	19150	100

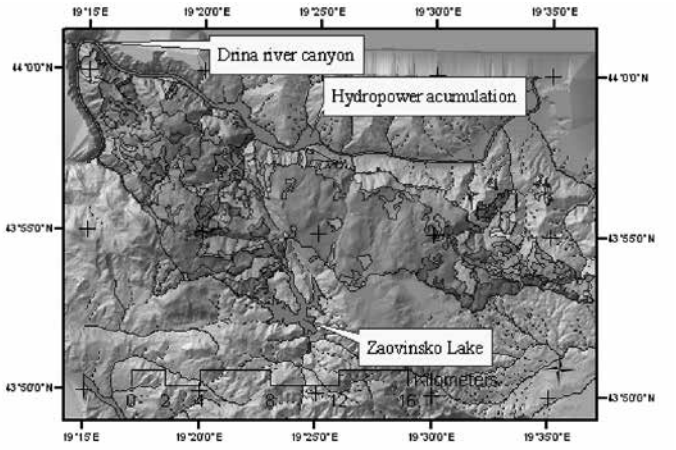


Figure 8 - CLC 2000 classes in Mt. Tara NP (Radović, D., Radović, I, 2006)

4. CONCLUSIONS

Mt. Tara NP represents an area incorporating natural values of global importance, most of which have retained the character of autochthonous environment.

The present work is a contribution to the GIS application in the areas of conservation geography, biogeography, environmental ecology, biodiversity protection, physical geography and spatial planning. This will be helpful to a wide circle of users in the areas of natural, biotechnical, technical, economic, and social sciences, as well as in tourism, sports, and recreation.

The advantages of the Mt. Tara NP GIS are: highly sophisticated computer solutions (hardware and software); production process standardization (data input and storage); data standardization (they may be used with any other GIS software currently and in the future); system openness (the system is open to input of new themes and modification of existing ones); clear visualization; analyses thoroughness (interactive, with more systematic, thematic, and topographic parameters); and system decision support.

All of these elements allow the efficient managing and provide the basis for good decision making for the protection and conservation of natural resources.

It also provides a basis for adequate preparation of documentation supporting the nomination of Mt. Tara for MAB “Biosphere Reserve” status within the global network of the UNESCO MAB Biosphere Reserve Program.

Acknowledgement: The present work was supported by the Ministry of Education, Science and Technological development of Serbia (No. III 46002).

5. REFERENCES

1. Ashdown, M., Schaller, J. (1990). Geographic information systems and their application in MAB-projects, ecosystem research and environmental monitoring. *MAB – Mitteilungen,* **34**, pp. 1–250.
2. Convis, Ch. (Jr.) (2001). *Conservation Geography; Case Studies in GIS, Computer Mapping and Activism.* Redlands, California: ESRI Press.
3. Čvorović, Z., I. Radović, D. Radović (2011). Potencijalne pretnje i rizici
4. po zaštićena prirodna dobra Srbije. Zbornik referata, rezimea referata i poster prezentacija, Knjiga br. 2: 932. Žabljak 20-23 Septembar 2011. Zavod za zaštitu prirode Crne Gore, Ministarstvo održivog razvoja i turizma Crne Gore.
5. Dragut, G., Thompson, C. (2005). Incorporating GIS Capabilities into National Park Service's Databases Using MapObjects. *ESRI User World Conference. Proceedings*, pp. 1-30.
6. Gajić, M., Vilotić, D., Karadzić, D., Mihajlović, Lj., Isajev, V. (1994). *Omorika – Picea omorika (Pancic) Purkyne na području Nacionalnog parka Tara* (monografska studija). Bajina Bašta: Nacionalni park Tara, Beograd: Šumarski fakultet.
7. Jakšić, P. (2003). Yugoslavia, In: *Prime Butterfly Areas in Europe; Priority sites for conservation* (Eds. c. van Swaay & M. Warren), 655-684. De Vlinderstichting, Butterfly conservation, Insect Life International, Landbouw natuurbeheer, Ministry of Agriculture, Nature Management and Fisheries, The Netherlands.
8. Longley, P., Goodchild, M., Maguire, D., Rhind, D. (2005). *Geographic Information Systems and Science,* New York: John Wiley & Sons, Ltd..
9. Manojlović, P.A. i Dragićević, S. (2002). *Praktikum iz geomorfologije.* Beograd: Geografski fakultet.
10. Ministarstvo energetike, razvoja i zaštite životne sredine Republike Srbije, Izvešraj o stanju životne sredine u Republici Srbiji za 2011. Agencija za zaštitu životne sredine Srbije. Beograd, 2012.
11. Mišić, V. (1988). *Vegetacijska karta NP Tara*: Prostorni plan područja Nacionalnog parka Tara. Službeni glasnik SRS, Br. 29/88. Beograd.
12. Nestorov, Protić, (2006). CORINE Land Cover, CLC 2000 Serbia & Montenegro Belgrad: EvroGeomatika d.o.o; Podgorica: Geological Survey of Montenegro.
13. Prostorni plan područja posebne namene NP Tara (2010) (Nacrt plana). Ministarstvo zaštite životne sredine i prostornog planiranja, Republička agencija za prostorno planiranje, Jugoslovenski institut za urbanizam i stanovanje JUGINUS AD, Beograd.
14. Puzović, S., Grubač, B. (2000). Federal Republic of Yugoslavia. In: *Important Bird Areas in Europe: Priority sites for conservation. 2: Southern Europe,* (Eds. M.F. Heath and M.I. Evans), 725-745. Cambridge, UK: Bird Life,
15. Radović, D. (2004a). *Vrednovanje i zaštita prirodnih potencijala Nacionalnog parka Tara primenom GIS tehnologija.* Beograd: Biološki fakultet, Univerzitet u Beogradu. Magistarski rad.
16. Radović, D. (2004b). Presentation of the working methodology and the Tara National Park case. *UNESCO/ROSTE – IUCN, Joint International Workshop on "MAB Biosphere*

Reserves and Transboundary Cooperation in the SEE Region. Belgrade and Tara National Park 13-17 June, 2004 (Plenary session III).

17. Radović, D., Radović, I. (2006). Implementation GIS technology in valorization and protection of natural values of NP Tara. Final Report of Project, Faculty of Biology, University of Belgrade, Ministry of Science and Environmental protection of the Republic Serbia.
18. Savić, I., Paunović, M., Milenković, M., Stamenković, S. (1995). Diverzitet faune sisara (Mammalia) Jugoslavije, sa pregledom vrsta od medjunarodnog znacaja. U: *Biodiverzitet Jugoslavije sa pregledom vrsta od medjunarodnog znacaja* (Eds. Stevanović, V., Vasić, V.), 517-554. Beograd: Biološki fakultet Beograd: Ecolibri,.
19. Simonović, P. (2001). *Fishes of Serbia*. Belgrade: NNK International, Belgrade: Institute for Nature Conservation of Serbia.
20. Stevanović, V. (2002). Fitogeografski položaj i opšti prikaz flore i vegetacije planine Tare, Bajina Basta: *Zbornik radova XXV Savetovanja o lekovitim i aromaticnim biljkama*, 4-7.
21. Wadsworth, R., Treweek, J. (1999). *Geographical Information Systems for Ecology: An Introduction*, London: Longman.
22. http://www.gisig.it/nature-gis

UDC 726.9:75.041.5
ID 176374796

Dejana Jovanović-Popović, Zoran Keković
University of Belgrade, Faculty of Securities Studies
dejana_kastor@yahoo.com
zorankekovic@yahoo.com

Miroljub Milinčić, Dejan Šabić
University of Belgrade, Faculty of Geography

NANOTECHNOLOGY AND FOOD SAFETY: APPLICATIONS AND EMERGING OPPORTUNITIES

Abstract: Rapid advancements in nanosciences and nanotechnologies in recent years have opened up new prospects for numerous potential applications to the food critical infrastructures. In this review, we intended to summarize food system vulnerability as well as the applications of nanotechnology relevant to food packaging and pathogen detection together with the outstanding challenges the applications of nanotechnologies might have on food safety and quality. However, despite a great deal of interest in the possible use of nanotechnologies in food safety area, rapid developments in nanotechnologies have also raised a number of health and safety and regulatory issues.

Key words: *nanotechnology, food safety, nanoscience*

1. INTRODUCTION

Nanotechnology has become the center of attention of a substantial amount of scientific and financial interest and is widely cited to be one of most important technologies for the 21st century. Lux Research (2008) estimates that nanotechnology material manufacturing industry was $147 billion worth of products in 2007 – a figure likely to grow to $3.1 trillion in manufactured nano-goods in 2015. Nanotechnology has taken hold in many industries, as corporate, government, and venture capital funding have driven spending on nanotechnology R&D to $13.5 billion (Lux Research 2008). According to the European Commission report (2009), the global expenditure on nanotechnology research, both public and private, in the two-year period 2007-2008, reached EUR 24.6 billion. Japan has the leading role to the global nanotechnology research funding (28.8%), followed by the USA (27.2%). Europe accounted for about one quarter of the worldwide total (25.6%).

Nanotechnology applications to the agriculture and food sector are relatively recent compared with their use in drug delivery and pharmaceuticals. However, nanotechnology as an emerging technology could potentially provide significant benefits in various sectors, including food, water and agriculture. Nanotechnology products are expected to bring a range of benefits to the food sector, including healthier foods (lower fat) with desirable sensory properties, new tastes, and textures, the potential for removal of certain additives without loss of stability, enhanced absorption of nutrients, improved packaging, traceability and security of food products (Groves, 2008; Kuzma & VerHage, 2006; Mor-

ris, 2008; Chaudry et al., 2010; Frewer et al., 2011; Huang, 2012). New applications such as purification of water, rapid pathogen and chemical pollutant detection systems, waste treatment, energy conservation, and new information and communication technologies applied along the food chain may be the new tools to deal with food safety and food security (Chaudhry et al. 2008). Whilst the market for nanotechnology in foods is just a small segment of total market, it is rapidly growing and predicted to rise to $20 billion USD in 2015 (Helmut Kaiser Consultancy, 2004).

The US government published the document entitled "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" (U.S. Department of Homeland Security, 2003). This document identifies a clear set of national goals and objectives and outlines the guiding principles to secure the infrastructures, systems and assets that are essential for the society, economy and national defense. Agriculture & Food has been identified by The National Strategy for Homeland Security along with other 14 areas or infrastructures that required protection from threats. In this article, potential applications to the food critical infrastructure have been addressed.

2. VULNERABILITY OF FOOD PRODUCTS AND AGRICULTURAL COMMODITIES

Food and Drug Administration (FDA) published the report entitled "Vulnerability Assessments of Food Systems" and stated that food products fell into three subgroups based on the nature of the industry: farm, manufacturing, and retail/distribution (FDA, 2012, p. 8).

Due to the geographically spread out, and open nature of farms, most areas in the farm subsector exhibited a high degree of accessibility. Moreover, the level of human observation in many farm activities may be low and an attacker may have opportunity to contaminate a product with little chance of being discovered. For these reasons, accessibility is generally high for this subgroup. However, vulnerability is generally low and the successful contamination of a farm process is unlikely.

Usual attributes of critical points include manufacturing steps where ingredients are mixed or added to a mixture are frequently identified as high risk. Similarly, the nodes where liquid ingredients are handled or stored are also commonly identified as high risk. The potential to add an agent (chemical or biological) to these types of processing steps and have that agent homogeneously mixed within the food product caused high levels of concern.

Products grouped in the retail/distribution subgroup typically involved the transportation, preparation, and sale of consumer food items. In retail food service environments, critical nodes focus on the preparation of ready to eat food. The workers in these nodes had open and complete access to unpackaged food and could introduce a threat agent. For assessments involving transportation and distribution of products, critical nodes typically focused on the long periods of time where a truck driver would have the opportunity to contaminate the product being transported.

The interdependencies and supply chain complexities of the food and agriculture industry make the impact of an attack on a single item or commodity difficult to determine (FDA, 2012:15). There is a need for detection methods and rapid sampling of biological and chemical contaminants in order to improve the safety and quality of food products.

3 CURRENT STATUS OF THE USE OF NANOTECHNOLOGY AND NANOMATERIALS IN FOOD AND AGRICULTURE

Manufactured nanomaterials can be added to food or food can be produced, processed or packaged with nanotechnology. The list of current and projected nanotechnology applications in the food and agriculture sectors is published in Appendix 4 of the report from the FAO/WHO expert meeting. The list includes: nanotechnology food ingredients, nanodelivery systems for nutrients and supplements, organic nanosized additives for food, health food supplements, and animal feed applications, inorganic nanosized additives for food, health food supplements, and feed applications, food packaging applications, nanocoatings on food contact surfaces, surface functionalized nanomaterials, nanofiltration, nanosized agrochemicals, nanosensors for food labelling, water decontamination, and animal feed (FAO/WHO, 2010, pp. 99-102).

Patent data emphasize the interdisciplinary, science-based and market-driven, nature of nanotechnology. Patents are, in fact, one of the direct and best measurable outputs of research and development (Igami and Okazaki, 2007). According to the Royal Commission on Environmental Pollution (RCEP) (2008) the number of patents registered from 1990-2006 for nanoparticles, nanorod, nanowire, nanocrystal, nanotube or carbon nanotubes has more than doubled every 2 years. The following search string in nanopatents review is applied to the Web of Knowledge database in the period 2009-2011: "nano" AND "food" (FAO/WHO, 2013). Out of 183 patents, 47 are related to packaging or coating applications, 19 patents are relating to nano-additives. Moreover, 10 patents covered nanotechnology applications for the detection of compounds in food.

The Project of Emerging Nanotechnologies (PEN) at the Woodrow Wilson International Center for Scholars maintains an inventory of consumer products that claim to utilize nanomaterials. The products fall into a number of different product categories such as health and fitness (738 products), home and garden (209 products), automotive (126 products), food and beverages (105 products), cross cutting (82 products), electronics and computers (59 products) and goods for children (30 products)(PEN 2012). Associated with food and beverages category are a number of appropriate sub-categories including cooking, food, storage and supplements. The Woodrow Wilson Center's Project of Emerging Nanotechnologies database lists mostly supplements, plus several applications in food packaging (such as in McDonald's burger containers or plastic beer bottles) and a few uses in cookware.

Recently, the European Consumers' Organization (BEUC) and the European Consumer Voice in Standardization (ANEC) have published on their website an inventory of different products claimed to contain nanomaterials applying the similar product categories and subcategories used in the Woodrow Wilson International Center for Scholars database (ANEC/BEUC 2009, 2010). The ANEC/BEUC's initial research was carried out between 31 October 2008 and 23 April 2009 through search on the Internet and in shops. The inventory only contains products that are actually being promoted as containing nanomaterials. In 2009, the group identified 151 products which are available to consumers in the EU. In October 2010, the ANEC/BEUC inventory listed 475 products, among them food supplements that claim to contain nanomaterials (total 27 products).

4 NANOTECHNOLOGIES FOR IMPROVING DETECTION OF PATHOGENS, AND PACKAGING AND PRODUCT INFORMATION

Nanomaterials may offer tremendous benefits around food products such as: detecting microorganisms, and improving packaging and product information.

4.1. Microorganism detection and identification

The rapid detection and identification of microorganisms is a pressing issue in the fields ranging from monitoring of food-borne pathogens to diction of biological warfare agents. Since conventional methods for detection and identification of pathogens often require long time (Baeumner, 2003), there is a need for development of fast, efficient and reliable methods for detection and identification of pathogens (Nugen & Baeumner, 2008). Nanotechnology is enabling rapid sampling of biological and chemical contaminants and more precise diagnosis (Mairhofer et al., 2009). The food industry is seeking a small, handheld device that only requires tiny quantities of sample sometimes called a 'lab-on-a-chip'. Food samples can be processed and analysed by a 'lab-on-a-chip' so rapidly that the results can be read out in a matter of minutes compared to the conventional methods which are too time-consuming and labour-intensive.

4.2. Smart food packaging and information

While most applications of nanotechnology in the food and agriculture sectors are currently at R&D or near-market stages, the applications for food packaging are rapidly becoming a commercial reality (FAO/WHO, 2010). The main products and materials in food packaging include silver, nanoclay, titanium dioxide and zinc oxide. Applications in smart food packaging are considered highly promising in the near-future because they can improve the safety and quality of food products. This includes intelligent (smart) packaging, which is reactive to the environment and active packaging, which is able to interact with the food product (Sozer & Kokini, 2009; Chaudhry et al., 2010).

Active packaging includes plastic polymers incorporating nanomaterials with antimicrobial properties. The commercially important nanomaterials in this respect include nanosilver and nanozinc oxide for antimicrobial action (FAO/WHO 2010).

Smart packaging incorporates nanosensors to monitor condition of the food and therefore responds to environmental conditions and alerts a consumer to contamination and/or the presence of pathogens. Sensors can warn consumers before the food is no longer safe to eat or can inform us the exact nutritional status contained in the contents. Examples include indicators that provide visual indication to the consumer when a packaged foodstuff starts to deteriorate (Smolander et al., 2004; Park et al., 2007). In fact, nanotechnology has the potential to change the fabrication of the entire packaging industry.

5. SOCIETAL DIMENSIONS OF NANOTECHNOLOGY

Any assessment of strategies for developing nanotechnology around the globe needs to take into account wider considerations and debates about the potential impacts of nanotechnology. Although nanotechnology is anticipated to lead to advances in many technological fields, multiple risks and societal concerns have also been identified, including health and environmental risks as well as needs for improved regulation (Hansen 2010; Maynard 2006; Oberdörster et al.2007; Stone et al. 2010). Cobb and Macoubrie (2004)

point to uncertainty about not only the scale but also the distribution of nanotechnology's potential social, economic, health, and environmental risks and effects.

The safety measures and risk assessment of manufactured nanomaterials have become the focal point of increasing consideration. In recent years, scientists, international organizations and regulatory agencies are still left with many questions as to whether nanomaterials pose a risk to human health or the environment, but have been actively working towards developing risk assessment for nanomaterials (European Commission 2003; EPA 2008; OECD 2009; SCENIHR 2009). Currently, there is a general consensus among regulators, scientists, policy experts and civil society organizations that there are some significant weaknesses in the application of the existing regulation to nanotechnology.

Recently, the European Union adopted new legislation that regulates food information and also addresses the presence of engineered nanomaterials in foods (EU, 2011). The Article 18 of Regulation No. 1169/2011 states that "All ingredients present in the form of engineered nanomaterials shall be clearly indicated in the list of ingredients. The names of such ingredients shall be followed by the word 'nano' in brackets" (EU, 2011). This regulation is going to apply from 13 December 2014 (FAO/WHO, 2013). It also provides, for food, a legal definition of an "engineered nanomaterial", which "...means any intentionally produced material that has one or more dimensions of the order of 100 nm or less or that is composed of discrete functional parts, either internally or at the surface, many of which have one or more dimensions of the order of 100 nm or less, including structures, agglomerates or aggregates, which may have a size above the order of 100 nm but retain properties that are characteristic of the nanoscale."

The application of the precautionary approach suggests taking action before scientific evidence has completely emerged, in order to protect human health and the environment (Dimitrijevic, 2011). However, the 'wait and see' approach is increasingly becoming a dangerous way to overcome the present vacuum in the regulatory field.

CONCLUSIONS

The current level of applications in the European food market is at an elementary stage. However, it is widely expected that more and more products will be available in the EU over the coming years. Applications in smart food packaging and pathogen detection are considered highly promising in the near-future. They can improve the safety and quality of food products and, therefore, play a great role in the protection of food critical infrastructure.

The toxicological nature of hazard and risk to consumers from nanotechnology-derived food/food packaging are largely unknown. A number of uncertainties and gaps in relevant regulatory frameworks have also been identified. In terms of comparison with other technologies in the food area, several consumer studies have reported that there is generally much greater acceptance of the benefits of nanotechnology than over genetically modified foods.

An improved understanding of the benefits of the technology, based on sound scientific data, will help gain the acceptance of nanotechnology by the food industry. A key finding of the 2009 FAO/WHO expert meeting was that public confidence in engineered nanomaterials can be supported through institutional efforts to provide an overview of applications of nanotechnology in food and packaging that are transparent and allow public involvement (FAO/WHO, 2013).

REFERENCES

1. ANEC/BEUC (2009). Nanotechnology—Small is beautiful but is it safe? Brussels: The European Consumer Voice in Standardisation (ANEC) and European Consumers' Organisation (BEUC) (http://www.anec.org/attachments/ANEC-PT-2009-Nano-002final.pdf. Accessed 30 August 2013.
2. ANEC/BEUC (2010). *Nano – ANEC-BEUC inventory of products claiming to contain nanoparticles available on the EU market.* www.**anec**.org/attachments/**ANEC**-PT-2010-**Nano**-017.xls. Accessed on 30 August 2013.
3. Baeumner, A.J. (2003). Biosensors for environmental pollutants and food contaminats. *Analytical and Bioanalytical Chemistry*, 377:423-445
4. Chaudhry, Q., Scotter, M., Blackburn, J., Ross, B., Boxall, A., Castle, L., Aitken, R.& Watkins, R. (2008). Applications and implications of nanotechnologies for the food sector. *Food Additives & Contaminants.*25(3):241–258.
5. Chaudhry, Q., Castle, L. & Watkins, R. (Eds.) (2010). Nanotechnologies in Food. London: Royal Society of Chemistry Publishers.
6. Cobb, M. D. & Macoubrie, J. (2004). Public perceptions about nanotechnology: risks, benefits and trust. *Journal of Nanoparticle Research*, 6(4), 395–405.
7. Dimitrijević, D. (2011). *Nanotechnology: The Need for the Implementation of the Precautionary Approach beyond the EU*. In G. Meško, D. Dimitrijević & C. B. Fields (Eds.), Understanding and Managing Threats to the Environment in South Eastern Europe (pp. 205-224). Dordrecht: Springer.
8. EPA (2008). *Nanomaterial research strategy*. Environmental Protection Agency, Washington, DC. http://www.epa.gov/nanoscience/files/nanotech_research_strategy_final.pdf. Accessed on 23 May 2013.
9. European Commission (2003). *Technical Guidance Document on Risk Assessment in support of Commission Directive 93/67/EEC on Risk Assessment for new notified substances, Commission Regulation (EC) No 1488/94 on Risk Assessment for existing substances and Directive 98/8/EC of the European Parliament and of the Council concerning the placing of biocidal products on the market*. European Chemical Bureau, Italy. Resource document. European Commission.
10. http://ecb.jrc.it/Documents/TECHNICAL_GUIDANCE_DOCUMENT/EDITION_2/tgdpart1_2ed.pdf. Accessed on 23 May 2013.
11. European Commission (2009). *Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee: Nanosciences and Nanotechnologies: An action plan for Europe 2005-2009*. Second Implementation Report 2007-2009, {COM(2009)607 final}.
12. EU (European Union) (2011). Regulation (EU) No 1169/2011 of the European Parliament and of the Council of 25 October 2011 on the provision of food information to consumers, amending Regulations (EC) No 1924/2006 and (EC) No 1925/2006 of the European Parliament and of the Council, and repealing Commission Directive 87/250/EEC, Council Directive 90/496/EEC, Commission Directive 1999/10/EC, Directive 2000/13/EC of the European Parliament and of the Council, Commis-

sion Directives 2002/67/EC and 2008/5/EC and Commission Regulation (EC) No 608/2004. *Official Journal of the European Union*, L 304: 18–63.

13. http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0018:0063:EN:PDF, accessed 6 December 2011. Accessed on 30 August 2013.
14. FAO/WHO (2010). *FAO/WHO expert meeting on the application of nanotechnologies in the food and agriculture sectors.* Potential food safety implications. Meeting report. Rome: FAO and WHO. http://whqlibdoc.who.int/publications/2010/9789241563932_eng.pdf. Accessed on 30 August 2013.
15. FAO/WHO (2012). *Joint FAO/WHO Seminar on Nanotechnologies in Food and Agriculture*, 27 March 2012. Rome: FAO.
16. http://www.fao.org/fileadmin/user_upload/agns/news_events/Nano_Seminar_Agenda_FINAL.pdf. Accessed on 30 August 2013.
17. FAO/WHO (2013). *State of the art on the initiatives and activities relevant to risk assessment and risk management of nanotechnologies in the food and agriculture sectors.*
18. http://www.fao.org/fileadmin/templates/agns/pdf/topics/FAO_WHO_Nano_Paper_Public_Review_20120608.pdf. Accessed on 30 August 2013.
19. FDA (2012). *Vulnerability Assessments of Food Systems*. Final Summary Report June 2009 – February 2012. http://www.fda.gov/downloads/Food/FoodDefense/UCM317547.pdf. Accessed on 30 August 2013.
20. Frewer, L., Norde, N., Fischer, A. & Kampers, F. (Eds.) (2011). *Nanotechnology in the Agri-Food Sector*: Implications for the Future.Wiley-VCH Verlag.
21. Gelman, D.L. & Wolf, D. G. (2009) Applications of Nanotechnology to the Food & Water Infrastructure. *Journal of Homeland Security and Emergency Management*, 6(1):1547-7355, DOI: 10.2202/1547-7355.1522
22. Groves K. (2008). Potential benefits of micro and nano technology for the food industry: does size matter? *New Food Mag*azine, 4:49–52.
23. Hansen, S. F. (2010). A global view of regulations affecting nanomaterials. *Nanomedicine and Nanobiotechnology*, doi:10.1002/wnan.99.
24. Helmut Kaiser Consultancy (2004). Study: nanotechnology in food and food processing industry worldwide 2003–2006–2010–2015.Available at: www.hkc22.com/Nanofood.html
25. Huang, Q. (Ed.) (2012). Nanotechnology in the Food, Beverage and Nutraceutical Industries Cambridge, UK: Woodhead Publishing Ltd.
26. Igami, M., & Okazaki, T. (2007). *Capturing nanotechnology's current state of development via analysis of patents*. STI Working Paper 2007/4, OECD Directorate for Science, Technology and Industry. Paris: OECD. http://www.oecd.org/dataoecd/6/9/38780655.pdf. Accessed 25 April 2011.
27. Kuzma J, & VerHage P. (2006). *Nanotechnology in agriculture and food production: anticipated applications.* Project on Emerging Nanotechnologies. Washington DC, Woodrow Wilson International Center for Scholars, September 2006. Available from: www.nanotechproject.org/filedownload/94 (Accessed February 26, 2010).

28. Lux Research (2008). *Nanomaterials State of the Market Q3 2008: Stealth Success, Broad Impact*. State of the Market Report Lux Research Inc, New York.
29. Mairhofer, J., Roppert, K. & Ertl, P. (2009) Microfluidic Systems for Pathogen Sensing: A Review. *Sensors*, 9:4804-4823.
30. Maynard, A. D., Aitken, R. J.,, Butz, T., Colvin, V., Donaldson, K., Oberdorster, G., Philbert, M. A., Ryan, J., Seaton, A., Stone, V., Tinkle, S. S., Tran, L., Walker, N. J., & Warheit, D. B. (2006). Safe handling of nanotechnology. *Nature*, 444, 267–269.
31. McClements, D.J. & Jiajia, R. (2011). Food-grade nano-emulsions: formulation, fabrication, properties, performance, biological fate, and potential toxicity. *Critical Reviews in Food Science and Nutrition* , 51(4):285–330.
32. Morris, V.J. (2008). Nanotechnology in the food industry. *New Food Magazine*.4:53–55.
33. Nugen, S. R. & Baeumner, A. J. (2008). Trends and opportunities in food pathogen detection. Analytical and Bioanalytical Chemistry. Springer
34. Oberdörster, G., Stone, V., & Donaldson, K. (2007). Toxicology of nanoparticles: a historical perspective. *Nanotoxicology* 1:2–25.
35. OECD (2009). *Safety of manufactured nanomaterials.* Organisation for Economic Cooperation and Development.
36. http://www.oecd.org/department/0,3355,en_2649_37015404_1_1_1_1_1,00.html. Accessed on 30 August 2013.
37. Park, B. K., Kim, D., Jeong, S., Moon, J. & Kim, J. S. (2007). Direct writing of copper conductive patterns by ink-jet printing. *Thin solid films*, 515(19):7706–7711.
38. PEN (2012). A *Nanotechnology consumer Product Inventory*. Woodrow Wilson International Center for Scholars. Washington DC. http://www.nanotechproject.org/inventories/consumer/. Accessed 10 March 2012.
39. Royal Commission on Environmental Pollution (RCEP) (2008). *Novel materials in the environment: the case of nanotechnology*. Royal Commission on Environmental Pollution, November 2008. http://www.officialdocuments.gov.uk/document/cm74/7468/7468.pdf. Accessed 24 May 2011.
40. SCENIHR (2009). *Risk assessment of products of nanotechnologies*. European Commission: Scientific Committee on Emerging and Newly Identified Health Risks, January 19. http://ec.europa.eu/health/ph_risk/committees/04_scenihr/docs/scenihr_o_023.pdf.
41. Accessed on 30 August 2013.
42. Smolander, M., Hurme, E., Koivisto, M. & Kivinen, S. (2004). *PCT International Patent Application* WO 2004/102185 A1, 2004.
43. Sozer, N. & Kokini, J. L. (2009). Nanotechnology and its applications in the food sector. *Trends in Biotechnology*, 27(2):82-9. doi: 10.1016/j.tibtech.2008.10.010
44. Stone, V., Hankin, S., Aitken, R., Aschberger, K., Baun, A., Christensen, F., et al (2010). *Engineered nanoparticles: review of health and environmental safety* (ENRHES) 2010. Resource document. ENRHES. http://nmi.jrc.ec.europa.eu/project/ENRHES.htm. Accessed 20 June 2010.

45. U.S. Department of Homeland Secuity (2003) The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.
46. http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf. Accessed on 30 August 2013.
47. U.S. Department of Homeland Secuity (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*
48. http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

UDC 726.9:75.041.5
ID 176374796

Mitar Kovač, Nenad Dimitrijević, Brankica Potkonjak-Lukić
Ministry of Defence of the Republic of Serbia
mitar.kovac@mod.gov.rs
nenad.dimitrijevic@mod.gov.rs
brankica.lukic-potkonjak@mod.gov.rs

SECURITY ASPECTS OF THE "SOUTH STREAM" AS A CRITICAL INFRASTRUCTURE ELEMENT OF THE REPUBLIC OF SERBIA*

Abstract: The objective of this paper is to analyze the security aspects of the transnational pipeline "South Stream", the project that should, according to the expectations, significantly contribute to improving of the energy security on the European continent, including Southeast Europe region and the Republic of Serbia. This territory is the crossroads of the important international communication routes and geopolitical interests of many international subjects, as well, which tend to achieve the dominant position for the realization of their own interests. It is more and more evident that survival and progress of every society depends on how easy it can provide the energy, in other words, on how much energy is accessible. High level of social, economic and political importance, exhaustibility, non-renewability and unequal distribution in different parts of the world are the main characteristics of the natural gas, as energy resource that represents an important element of national wealth and productive forces of every state. Continuous energy resources supply influences economic stability of the country, shapes the structure of its economy and secures the planned dynamics of economic growth, and that, essentially, reflects on its defence capability. With growing global demands for energy resources, including natural gas, it could be expected that the great powers will tend to strengthen their strategic positions and attempt to restrain the influence of their rivals. In that context, in this paper, the possibility is pointed out that the competitions for energy resources and markets all around the world could lead to political tensions and increased potential for confrontations. Available information and forecasts indicate an increasing significance of energy security which includes availability of energy supplies, in sufficient quantity and by acceptable prices, stability of deliveries, as well as physical security of the infrastructure for energy supplies. Considering that, the interests of great powers, first of all the Russian Federation and US have been analyzed, but also the interests of the European developed countries, as well as the positions of the international organizations on the construction of the South Stream pipeline. It is estimated that the continuation of strategic connecting with the Russian Federation in the area of energetic will have a positive influence on overall economic development of the Republic of Serbia. Considering that the part of the pipeline is planned to pass through the Republic of Serbia, and also that this project has a national significance, it is evident that this pipeline will be an extremely significant critical infrastructure element on the national territory. Therefore, from the aspect of this pipeline infrastructure protection, the issues having importance for establishing an efficient system for its protection are

* The paper has been made within the project 47029 titled "Cost Effective Selection of New Technologies and Concepts of Defence through Social Reforms and Strategic Orientations of Serbia in the 21st century". The project is financed by the Ministry of Education and Science of the Republic of Serbia in the period 2011–2014. The project manager is Professor Momčilo Milinović, PhD.

discussed. In that context, the possible implications on the security of the Republic of Serbia are analyzed and, in function of the protection of the national interests in the area of security, the challenges, risks and threats have been identified for which it has been assessed that have or, in some circumstances, may have influence, directly or indirectly, on the security of citizens, the state, material resources or the environment.

Keywords: *security, critical infrastructure, pipeline "South Stream", Republic of Serbia.*

1. INTRODUCTION

The term "critical infrastructure" is relatively new,[2] although the importance of the concept has been continuously recognized throughout the history of human society. The existence of infrastructural facilities whose importance can be qualified as remarkable or even vital[3] for the functioning and in some cases for the very survival of the community, can be observed in almost all societies. Since they were largely dependent on proper and continuous functioning of this category of infrastructure, and fully aware of the fact that their partial or complete incapacitation or destruction would cause severe consequences, the communities, and above all those who manage them, paid a special attention to providing adequate protection against threats to their security, whether they come from natural disasters or intentional or unintentional destructive human activities.

In contemporary age, the issue of critical infrastructure protection is for many reasons especially topical, first of all regarding the energy infrastructure. Available information and forecasts indicate an increasing importance of energy security which implies the availability of sufficient energy supplies at affordable prices, the stability of deliveries, as well as physical security of energy supply infrastructure, taking also into account an environmental dimension.[4]

It is more and more evident that the survival and progress of any society largely depends, inter alia, on the quantity of available energy and how it can be provided. Energy dependence makes modern societies extremely sensitive to any disturbance, including a short or prolonged disruption in energy supply for the production capacities and population,

---

2 The term has been used for the first time in the document Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection (1997), and afterwards in a series of other documents of the United States and a number of other countries, as well as international organizations (NATO, EU, OSCE and others).
There are many definitions of critical infrastructure, although their formulation in terms of content and scope largely overlap. Since the Republic of Serbia is a candidate for the membership in the EU, the most relevant definition is the following: "Critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." See: Council Directive (2008, December 8). See also: Gospić, N., Murić, G., Bogojević, D. (2012).
The definition of national critical infrastructure contained in Article 3 of the Law on Critical Infrastructures (2013), which the Republic of Croatia was in obligation, according to the Directive, to adopt before accession to the EU, and which has been in force since 18 May 2013, is the following: "National Critical Infrastructure are the systems, networks and facilities having national importance whose disruption of operation or interruption of goods or services providing may have a serious impact on national security, health and life of the people, property and environment, security and economic stability and continuous functioning of the government."

3 Typical examples of critical infrastructure are the aqueducts in the ancient Rome. For the experiences related to their protection and the analogy with modern infrastructure, see: Assante, M. J. (2009).

4 The discussions on energy security were actualized after oil embargo in 1973, as a consequence of Arab-Israeli war. There is no universally accepted definition of energy security. See more in: Yergin, D. (2006).

which may be caused by functional disabling, physical damage or destruction of a part or the entire energy infrastructure on the territory.

With further reduction of natural energy reserves in the world, the actuality of critical energy infrastructure security will continue to grow at the global, regional, and national level. To meet the growing energy demands, especially those of the most technologically developed countries, but also of the others, the efforts to provide the required amount of energy from different alternative sources will continue to increase.

Continuous energy supply affects a country's economic stability and its planned economic growth rate, which consequently, influences its defence capability. Under the conditions of natural energy reserves reduction and their uneven distribution, it can be expected that, as global demands for energy resources, including the natural gas, continue to grow, the great powers will keep strengthening their strategic positions in trying to stop the influence of their competitors. The competition for energy resources and markets around the world will very likely lead to political tensions and conflicts. The main suppliers of energy - the exporting countries will try to exploit energy resources for achieving their strategic and political objectives and it is expected that they will be in a position to do it. The main energy consumers recognize that an increasing dependence on imported energy enhances their strategic vulnerability and limits their ability to achieve a wide range of foreign policy and national security objectives. In such a situation, the diversification of supply and resources will remain a fundamental principle of energy security, regarding both oil and natural gas.

Enormous socio-economic and political importance, exhaustibility, non-renewability and uneven distribution in different parts of the world are the main characteristics of the natural gas. Ensuring the security of a pipeline as a critical infrastructure element should be the primary responsibility of each state over whose territory a transnational gas pipeline runs. Taking into account the current security environment, the character of contemporary threats and risks, as well as the fact that critical infrastructure includes an increasing number of objects whose protection is not an exclusive responsibility of state authorities, considering that some of them are owned by the private sector, continuing constructive cooperation based on common standards, mutual trust, information sharing and coordinated preventive action of the parties involved, should be the key factors in reducing the risk of endangering the security of pipeline infrastructure to a minimum.

2. THE "SOUTH STREAM" PROJECT

The "South Stream" project aims at improving European energy security and it is a key project within the strategy of diversifying gas supplies routes to the EU. By connecting the suppliers directly to the consumers of gas, the "South Stream" will significantly increase the security of gas supplies for the entire European continent.

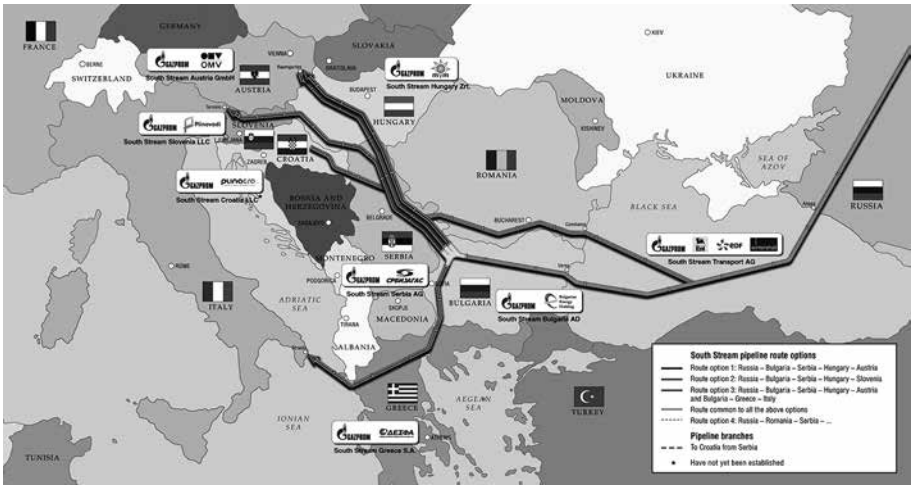


Figure 1: The "South Stream" map
(Source: www.south-stream.info/en/maps/)

The "South Stream" pipeline will run from Russia through the Black Sea in a distance of 925 km, Bulgaria 536 km, Serbia 422.4 km, Hungary 229 km, Slovenia 266 km, and Italy 11 km. Pipeline branch to the Republic of Srpska will be 105.8 km, and to the Republic of Croatia 52.8 km long. Estimated cost of the project is 16 billion Euros, out of which 10 billion Euros is intended for financing its construction through the Black Sea and 6 billion for the land part.

The maritime part of the "South Stream" project is realized by the Russian Gazprom, which owns a 50% stake, the Italian ENI with 20%, French EDF and German Wintershall with 15% of shares. The land part of the "South Stream" is being implemented with the countries through which it passes, by forming joint companies, where the ratio of shares is 50% - 50%, except in Serbia, where the Russian-Serbian company "South Stream Serbia" was established, in which Gazprom holds 51% and Srbijagas 49% of total capital.

The material intended for installation weights 377.08 thousand tons, and the annual capacity is about 41 billion m^3 of gas. The investment value of works through Serbia is 1.7 billion Euros (Srbijagas, 2013). It is expected that the gas will start to flow through the "South Stream" pipeline in 2016, and the total capacity of the pipeline will be achieved in 2017.

The international system of very high pressure gas pipelines consists of pipelines with integrated devices, installations and facilities that are used for transportation of hydrocarbons.

The international gas pipeline system "South Stream" includes (Spatial Plan, 2012):

Line gas pipeline:

- Approximately 411 km long 1,400 mm pipe diameter pipeline with working pressure of 9.8 MPa,
- Branch pipeline to the Republic of Croatia 52.7 km long with 500 mm pipe diameter and 9,8 MPa working pressure,
- Branch pipeline to the Republic of Srpska 105.8 km long with 300 mm pipe diameter and 9.8 MPa working pressure, and



Figure 2: The "South Stream" map through the Republic of Serbia
with branch pipelines and compressor stations
(Source: www.south-stream.info/en/maps/)

- Block valve stations - cut-off valves for the gas flow (every 30 km).

Gas facilities:

- Two compressor stations: in central Serbia CS "Velika Plana" and in northern part of Serbia CS "Bačko Dobro polje",
- Two measuring stations: on the border with Bulgaria MS "Vrška Čuka" and on the border with Hungary MS "Bački Breg", and
- Regulation-measuring stations: RMS "Paraćin" and RMS "Gospođinci".

All pipeline facilities shall be fenced to prevent uncontrolled access to them. Along the entire length of the gas pipeline corridor an optical cable will be deployed for monitoring and management of gas transportation as well as an electric power cable for supplying the installations located on the line gas pipeline. The international high pressure gas pipeline has a transit character, runs through uninhabited areas and it is planned to be buried. The pipeline will be built according to the highest Russian and European standards.

It was announced that Serbia will officially award to its section of the pipeline the status of the project of national importance. The status of the project of national importance is required, inter alia, for the recognition of the "South Stream" in the EU as a cross-border project. This would enable Serbia that the pipeline running through its territory could not

be used by a third party.[5] By now, Bulgaria, Hungary and the Republic of Srpska have already granted the status of the project of national importance to their sections of the pipeline.

If all the countries through whose territory the pipeline passes, grant their sections the status of the project of national importance, in that case the "South Stream" will become a cross-border pipeline and the European Union's Third Energy Package, or the possibility that third parties use about 50% of its capacity, wouldn't apply.

Until now, for the construction of the "South Stream" through Serbia the following documents have been finalized: Feasibility study, Spatial plan of the Special Purpose Areas - transnational gas pipeline "South Stream", Strategic Environmental Impact Assessment Report of the Spatial Plan of the Special Purpose Areas - transnational gas pipeline "South Stream" and the Law was adopted on determining the public interest and the special procedure for expropriation and obtaining documentation required for the realization of the construction of the natural gas transportation system "South Stream".

3. ATTITUDES OF GREAT POWERS AND INTERNATIONAL ORGANIZATIONS TO THE "SOUTH STREAM"

Uneven distribution of the world's oil and gas resources leads to the natural division on the exporting and importing countries. The majority of oil reserves is located in the Middle East, where the political situation is unstable and unpredictable. In Russia, Iran and Qatar 56% of the world's gas reserves are located. The European Union, which is one of the major importing countries, has 2% of the world's gas reserves and less than 4% of the world's oil reserves. The EU energy security depends significantly on the energy policy of Russia and other countries that export their energy resources to Europe (Qatar, Algeria, Libya, Nigeria, Azerbaijan).

The situation in global energy sector is unstable and it is not easy to predict it. That is why both the exporting and importing countries consider reducing their energy risks, as a priority task of their energy policies in which the important place is given to the issues related to providing energy security.

The EU countries import energy resources and for now they depend on energy exporters. Since the EU cannot influence significantly the resolution of the problem, it ensures its energy security through political dialogue with exporters and transit countries. Therefore, the policy direction that would ensure energy security is crucial for the EU and its member countries.

It is estimated that the energy cooperation between the EU and Russia will further strengthen in the near future. Partner relations with Europe have a number of advantages for Russia. It recognizes that the need for gas on the market of 500 million users, will be at a stable level in the future.

The European Union imported 58% of gas in 2005, and according to the forecasts regarding the increse in demand for gas in Europe, it is expected to import 81% in 2025.

---

5 According to the European Union's Third Energy Package, the owners of gas pipelines should allocate about 50% of the capacity to third parties. If the country through which the pipeline runs awards to its section of the pipeline the status of the project of national importance, this package does not apply.

In 2005, the EU consumed 543 billion m^3 of gas, out of which 42% from its own domestic production. It is estimated that in 2025 the EU will consume 629 billion m^3 of gas, and provide 19% of gas for the market from its own production.

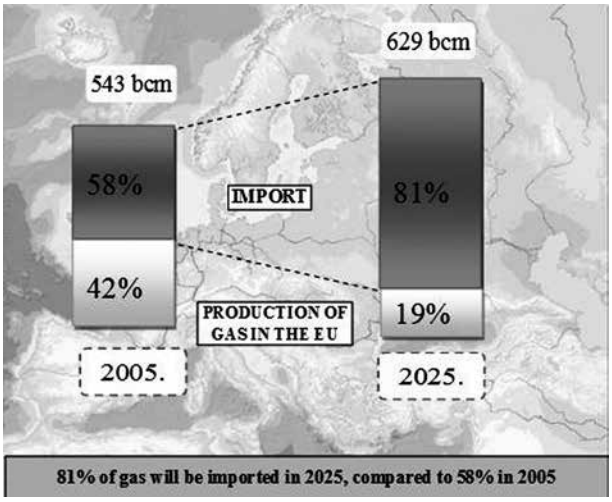


Figure 3: The increase in demand for gas in Europe 2005-2025
(Source: European Commission (2007))

In that context, the "South Stream" could be the answer to the challenges of today and the necessity of moving to the safest sources of energy, and it is a gas. Once completed, the pipeline will diversify European energy supplies and ensure a steady supply of gas.

With the construction of the South and Nord Stream (capacity of Nord Stream is 55 billion m^3 of gas per year), Russia wants to reduce its dependence on Ukraine and other transit countries where the problem occurred with the price of gas transfer, which in January 2009 led to a complete breakdown of gas supplies to Europe.

Russia owns about 6% of the world's oil reserves and 23% of gas, while the dependence of the EU on Russian gas and oil increased after the former Eastern Bloc countries joined the EU (in 2004 and 2007), and the construction of the Nord Stream pipeline.

Out of total exports of these energy resources, Russia exports 32% of oil and 50% of its gas to the EU market. In Norway, which is one of the major energy suppliers of Europe, the resources are slowly decreasing.6 On the other hand, the situation in the Middle East is unstable and the future of Iraq and Iran is uncertain. Africa provides 20% of energy supplies to the EU. However, the European companies are there faced with tremendous competition when they buy from American, as well as Chinese and Indian companies. Therefore, geographic proximity makes Russia its natural partner, and what is even more important is that, because of political reasons, the quantities of the Russian exports to the United States and China are not in the extent that could jeopardize the safe supplying of Europe. In addi-

6 The most serious threat for the region is the process of national disintegration as a consequence of the civil war in Syria. What makes the civil war in Syria so dangerous is the fact that the actors on the scene are no longer its driving force. Instead, the war became the competition for the dominance in the region. As a result, the Middle East could easily dissolve into chaos.

tion, the accession of Russia to the World Trade Organization (WTO) opens the possibility for foreign investments in oil and gas sectors, which could also include the exploration of new oil and gas fields.

The EU contributes to the development of an industrial partnership with Russia in order to establish a mutual dependence and thus ensure its energy supply. By its accession to the WTO, the market of Russia will become open, and the Russian customer will buy goods produced in the EU with the revenue realized from the gas sale. Russia is a reliable European energy supplier, and this supply has never been conditioned upon, even during the Cold War period. The EU strategy is to provide a secure energy supply in the future.

The question is to what extent the Russian assessment that the demand for its gas in Europe will continue to increase is realistic. In fact, according to the current state of affairs, the situation is a lot different now, and these expectations seem to be too optimistic for Russia. However, this can be explained, among other things, by market conditions, which are worsened due to a difficult financial situation in Europe and the reduced demands for gas. It is very uncertain whether Russia can count on the increase of the EU demand after the crisis, considering the Europe's tendency to reduce its dependence on "Gazprom", and therefore trying to find an alternative energy supply.

One of the most promising alternatives is a shale gas. Thanks to shale gas, the U.S. has fully covered its needs for gas. But for now, the quantity of shale gas reserves in Europe is not completely known, and there is also a strong resistance of ecologists whose positions are very influential in most of countries. However, the fact is that the exploitation of gas and oil from shale is toxic and pollutes soil and subterranean waters. Therefore, France banned new explorations of shale gas resources by the law. Also in Poland, where there are considered to be located the largest shale gas resources in Europe, the explorations were ceased because they were not profitable.

Another alternative is seen in the development of technology for the production of liquefied natural gas (LNG)[7] and the method for its delivery. Liquefied natural gas is an alternative to the gas from pipelines, and in case there is an appropriate infrastructure, it is possible to deliver it from any location in the world and thus significantly increase the competition in the world market. The supplier of the liquefied gas could be Qatar, but for now, Europe does not have a sufficient number of built warehouses for the storage of liquefied natural gas, nor special tankers for its transportation. The liquefied natural gas price in Europe ranges between 210 and 310 U.S. dollars per 1,000 m^3, while during winter 2012/2013 the price of Russian gas was between 353 and 392 U.S. dollars per 1,000 m^3.

The third possibility is an alternative pipeline. The Russian competitors are the North African countries (Libya, Algeria, Egypt), but it is unlikely that Europe can rely on them due to political instability in these countries.

The "Nabucco" pipeline was designed to supply Europe through the South Caucasus and Turkey with the gas from the Caspian region. Initially, this pipeline was planned to transport 30 billion m^3 of gas from Turkmenistan, Iran and Azerbaijan. However, Iran was given up due to the international sanctions and Turkmenistan because of unregulated legal issues concerning the Caspian Sea (for laying gas pipelines). Also, the role of a very strong opposi-

7 Liquefied natural gas (LNG) is a clear, colourless, non-toxic liquid that forms when natural gas is cooled to -162ºC (-260ºF). This shrinks the volume of the gas 600 times, making it easier to store and ship overseas.

tion in Russia was very important, and that consequently made connecting to the "Nabucco" impossible. Meanwhile, Turkmenistan has shifted to the Asian market and supplies China through the pipeline with capacity of 30 billion m^3, and there is also a plan to build a gas pipeline to India via Afghanistan and Pakistan. Azerbaijan for now has no independent capacity to supply it. Azerbaijan is in a process of developing two new projects. The first one is the AGRI gas pipeline (Azerbaijan - Georgia - Romania Interconnector). Regarding this project, the gas would be delivered through pipeline from Azerbaijan to the Black Sea coast in Georgia, where a factory for the production of liquefied natural gas is planned to be build. Produced liquefied gas would be transported by ships to Romania, where it would be returned to the gaseous state and delivered through the gas pipeline to Europe.

The second project as an alternative to "Nabucco" is the "Transanatolian" gas pipeline (TANAP), through which the gas would be transported from Azerbaijan via Georgia, Turkey, and Bulgaria to Europe. Turkey and Azerbaijan have agreed on its construction to begin in 2014. The capacity of this gas pipeline will be 16 billion m^3 per year.

In 2012 Azerbaijan produced 43 billion tons of oil and 26.9 billion m^3 of natural gas. Currently, the second phase of the exploration of gas resources at the Shah Deniz site is ongoing as well as some other perspective projects, which could significantly increase the production of gas in the future period.

4. THE "SOUTH STREAM" INFRASTRUCTURE PROTECTION

The protection of pipelines from accidents and damages is a serious problem worldwide. Environmental damage and economic losses from disasters, theft, vandalism and other emergencies require serious questions to be raised because of their essential importance for the establishment of an efficient system for pipelines protection.

The main threats to security of gas pipelines are the following:

- Leakage of the gas due to age, wear and corrosion of pipes,
- Gas pipeline damage due to technological disasters, earthquakes and land subsidence,
- Gas pipeline damage due to theft of gas,
- Terrorist attacks, hacker attacks, sabotage and other criminal activities.

Due to its properties methane explodes at a low gas concentration, while at higher concentrations it burns. In case of methane explosion the affected area may cover up to 300 meters on both sides of the damaged gas pipeline. An additional problem may be caused by a leak, as this gas has no odour or colour (not visible with the naked eye) when a pipeline is buried in the ground. On the one hand, the buried pipeline is better secured from theft and intentional damage (for example, by terrorists), but, at the same time, this makes it more complicated in a situation when it is necessary to repair damage, because it is difficult to approach it.

Pipeline security is a serious issue, since the pipeline and areas around it fall into the high risk zone. According to the media information published in the territory of the Community of Independent States, there are many examples of the pipelines protection in the world.

The *Sakhalin–Khabarovsk–Vladivostok pipeline* is under construction and due to the lack of experience in that region regarding the protection of gas pipelines, those who have a lot of experience from other regions have been invited to come and provide assistance. In

particular, the private companies are engaged with their mobile teams who are trained to react in case of a terrorist attack on the pipeline or in case of an explosion and gas leakage.

The Tashkent-Bishkek-Almaty pipeline which connects Uzbekistan, Kyrgyzstan and Kazakhstan is protected by the police because it is not affordable to provide the private security protection.

In the Persian Gulf and the Israel the concepts have been developed which, along with the responsibility of companies themselves, provide the cooperation with the government in the interest of security. Generally, for the protection of gas pipelines, the police and the armed forces can be engaged. Where the military and the police, from whatever reason, cannot take care of the gas pipelines security, private companies could be engaged. Companies-owners of gas pipelines are responsible to their partners, customers and investors. The tasks of private security companies are to carry out strategic consultations, assess the existing risks and to safeguard the facilities and employees.

The security of energy supplies has a strategic importance for Europe, and because of that all available means should be employed to provide it. In that context, the armed forces also play a role, and so operation "Atalanta" in the region of the Horn of Africa provides the protection of the sea route which is very important in terms of energy supplies.

The Baku-Tbilisi-Ceyhan oil pipeline security system may serve as an excellent example of a modern approach to pipelines security. The oil pipeline will be in the entire length buried in the ground; only terminals and compressor stations will be on the surface. Besides, the additional security measures will be provided to protect the installation from theft and damage. The oil pipeline will be fully covered by the security services personnel, even the cavalry will be used, and also the modern techniques and technology will be applied.

According to the information of the Ministry for Emergency Situations of the Russian Federation, published in the Russian media on 11 January 2013, for ten months during 2012 twelve emergencies on the main pipelines (gas and oil pipelines) were registered in Russia. Compared to 2011, it is an increase six times. One third of them occurred in the Ural Federal District. The main causes of the emergencies were mechanical damages of underground cables, corrosion and excessive pressure in gas stations. It must always be taken into consideration that places where pipelines intersect with roads and railroads are potentially extremely dangerous.

Regarding the "South Stream" pipeline, which is an international high pressure gas pipeline having a transit character and running through uninhabited areas, it will be buried and built according to the highest Russian and European standards.

It is estimated that the objects having the highest risk for terrorists attack are the compressor stations. An attack on them could cause the most serious negative consequences such as loss of life and significant property damage. In Serbia two locations are planned for the compressor stations: Velika Plana and Bačko dobro polje.

The compressor stations are potentially very dangerous production facilities, which consist of installations for taking the gas for compression and discharging of compressed gas, for gas purification from mechanical impurities and liquids, gas compression and cooling the gas after compression. In the compressor stations, there will be also technical-service facilities, the staff accommodation facilities, the auxiliary facilities for water purification,

the transport surfaces, the storages (tanks) for methanol, oil (flammable and explosive materials), etc.

According to the "Gazprom" standards, the compressor stations will be fenced with two meters high metal grid on the top of which there will be three barbed wires on both sides. The total height of the fence will be two meters and fifty centimetres. For the protection and preventing from unlawful interference with the functioning of the compressor stations as components of a linear (line) pipeline management, the security service must be established. Detachments, groups and commands of the security service will provide the security of the compressor stations and linear (line) parts of the gas pipeline. The personnel of the security service must be specially trained, licensed to be engaged in providing security, and they must have adequate equipment and weapons. The security of the compressor stations must be provided round the clock by armed personnel deployed on guard posts, and also the appropriate equipment for signalization (alarms, cameras, etc.) must be set up.

In addition to Gazprom's standards and their requirements, the security of gas pipelines could be provided also by the Sector for Emergency Situations of the Ministry of Interior of the Republic of Serbia, Centre for Emergency Situations in Niš and the Serbian Armed Forces.[8]

5. REFLECTIONS OF THE "SOUTH STREAM" ON THE SECURITY OF THE REPUBLIC OF SERBIA

The question of European energy security has brought attention to the strategic significance of South-eastern Europe as a transport hub of natural gas and a key region for European energy security. By constructing and operating the "South Stream" gas pipeline on its territory, Serbia will gain a good position in the region as well as in the relations with the EU. Generally, the situation when other countries become dependent provides great opportunities. The Russian president, Vladimir Putin explained such a situation in a very picturesque way to the Slovenian Prime Minister.9 The fact is that neither Russia nor the EU will allow Serbia to be unstable, since nobody has the interest to cause conflicts and create instability in this area and to jeopardize a huge investment and stop the transportation of gas. Furthermore, it is expected that the project will contribute to the stability of the whole region, and for Serbia, although it is the only country along the route of the pipeline which is not a member of any defensive alliance or the EU, it brings safety and provides the national security.10 Having in mind the estimations that the world's reserves

8 In case of emergency situation on the gas pipeline (gas leaks, explosions, fires, evacuation of population, etc.) the Armed Forces will provide support to civil authorities (Defence Strategy, Chapter 5.1).

9 Putin said in Slovenia (22.03.2011.): "When the South Stream passes through Slovenia, the Italian Prime minister will call you in the morning and in the evening to ask how you are and to wish you good morning and good night" (2011 Izjave.net), during the signing of the agreement on the establishment of a joint venture for constructing the Slovenian section of the "South Stream".

10 It is not the number of soldiers and army hardware this is important, but the position of the countries in the energy strategy. Today, the crucial regional project is the construction of the South Stream pipeline, which favours Serbia, Hungary and some NATO countries. This gas pipeline has the potential to influence the relative strategic power of the Balkan countries in correlation with the EU as the gas end-consumer, which is transported through the region, but also to the economic situation in the region (Fatić, A., 2012, 12.03.).

of gas will last for another 65 years, the future period for Serbia should be secure, with no risk of recurrence of 1999 (NATO bombing) and any armed conflict in the Balkans.

As a country through which the gas will be transported, it is expected that Serbia will have a safe and regular supply with this kind of fuel, it will no longer depend on other countries (Hungary, Ukraine), it will not pay high fees for gas transportation and therefore it will have cheaper gas available. Serbia imports more than 90% of gas annually, but after completing the construction of the "South Stream" gas pipeline, Serbia will become one of the countries which earns from this energy resource, and the estimated income, only from transit fees, will be approximately 200 million Euros, although according to other estimations, it could be as many as 500 to 600 million Euros.

Today, it is becoming more and more evident that the availability of energy resources and their utilization determine the level and dynamics of socio-economic development of a country. It is estimated that for the construction of this gas pipeline about 2,000 workers will be hired, and for its maintenance 500 to 1,000 people. It is expected that the Serbian construction industry and the related services sector, engineering and other industries will be maximally engaged. The value of the "South Stream" gas pipeline through Serbia will be around 1.7 billion Euros.

In that context, the estimated value of the related projects that will be implemented within the realization of the "South Stream" will be additional 1.2 billion Euros. These projects refer to the underground storage, the interaction with Bulgaria and the construction of gas power plants and those of cogeneration type.11 In addition to Russia, as the largest investor in the region, the EU will also be interested to invest more, not only in Serbia as a stable and safe state, but also because Serbia can provide "duty-free exports"12 of the EU goods to the huge Russian market.

Serbia is becoming an important regional factor in supplying the surrounding markets with gas. The underground gas storage Banatski Dvor where 450 million m3 of gas will be stored will serve as reserve storage for supplying Serbia, Croatia, Bosnia and Herzegovina and Hungary.

The Agreement on connecting Macedonia to the "South Stream" gas pipeline is expected to be concluded soon. The gas would be supplied from Serbia and it would be transported alongside the highway from Niš to the south. The plan for the southern branch of the gas pipeline is in development phase, and this branch will be directed to Macedonia and Kosovo.13 The gas pipeline enters our country near Zaječar and exits near Subotica.

The environmental aspects of the "South Stream" project are also very significant, because gasification is expected throughout the country, which means that the industry and the population will mostly use this kind of fuel which, compared to other fuels, is the least pollutant.

---

11 Referring to the study of EPS (Electric Power industry), the construction of the cogeneration plant type (production of electricity and thermal energy) would be possible in Belgrade, Novi Sad, Zrenjanin, Kragujevac, Nis, Subotica, Sremska Mitrovica. When the electricity is produced from coal utilization is about 25%, while when it is produced in thermal power plants with steam-gas cycle, utilization is 80%, and then the production of electricity from gas is profitable. This is exactly what led Germany to build the Nord Stream and produce electricity from gas.

12 The trade agreement between Serbia and Russia on duty-free import of goods

13 Internet portal, Energetics, 14.03.2013.

By implementing the "South Stream" project Serbia gains essentially important communication which connects it more closely, from one side with Russia, and from other side to Europe, and also the status of an important partner in the project at the regional and even global level, and thus increasing the importance of Serbia.

6. CONCLUSIONS

The situation in the global energy sector is unstable and it is not easy to predict it. That is why both the exporting and importing countries consider reducing their energy risks, as a priority task of their energy policies where they give an important place to the issues related to providing energy security.

The aim of the "South Stream" project is to improve the energy security of Europe. It is a key project in the strategy on gas supplies to the EU from different directions. Connecting the suppliers directly to the consumers of gas, the "South Stream" will significantly increase the security of energy supply of the entire European continent.

The question is to what extent the Russian assessment that the demand for its gas in Europe will continue to increase is realistic. In fact, according to the current state of affairs, the situation is a lot different now, and these expectations seem to be too optimistic for Russia. However, this can be explained, among other things, by market conditions, which are worsened due to a difficult financial situation in Europe and the reduced demands for gas. It is very uncertain whether Russia can count on the increase of the EU demand after the crisis, considering the Europe's tendency to reduce its dependence on "Gazprom", and therefore trying to find an alternative energy supply.

The relations between the Russian Federation and the United States are characterized by the struggle for supremacy in Europe. The United States are trying to prevent Russia to be the only or the biggest supplier of Europe with gas. The United States, in addition to producing the gas from shale and having the available technology for the production and transportation of liquefied gas, announced that in 2015 they will be ready to offer their gas to Europe in sufficient quantities and much cheaper than Russia.

Russian-American rivalry in Central Asia, so called "new Great game", is largely associated with the struggle for the control over the production and transport of energy resources (Iran, Iraq, Syria, Azerbaijan, Turkmenistan), from where America intends to supply Central Europe and Romania, and thus reduce their dependence on the import from Russia.

The Republic of Serbia as the only country that is not a member of NATO or the EU continues to be the territory in which Russia, Germany, Turkey and the United States are vitally interested, due to their strategic and geopolitical reasons.

Russia is interested in strengthening its position, primarily in the energy sector, in the Balkans over Serbia as a regional centre for the gas supply and production. Germany, as a co-investor of the "South Stream" project (15% of the shares for the construction on the bottom of the Black Sea) and the largest current and future[14] European consumer of gas,

14 Germany will close all its nuclear plants by 2022 and shift to gas. In addition, Germany imported 92.82 billion m3 of gas in 2010. Its production is 10.6 billion m3, which is a decline in production compared to 2000 when the production was 16.9 billion m3. The production of electricity in nuclear power plants in Germany is approximately the same as the electricity production from 35 billion m3 of gas. When Germany closes all its nuclear power plants it should provide that amount of gas.

is interested for running that gas pipeline through our country uninterrupted and safely, inter alia, because Serbia can be a barrier to the uncontrolled migration from Turkey and the Middle East through the Balkans to Western Europe. Turkey, through whose territory land lines of alternative Nabucco and "Trans-Anatolian" gas pipeline (TANAP) run, leads more and more independent and ambitious policy, seeking to restore its influence in the countries that once belonged to its empire, and to confirm itself as a macro-regional power. The United States are aimed at counteracting the Russian influence in the Balkans, and, through the Balkan members of the NATO and Kosovo, they have mechanisms to influence the situation in the region.

In the future, an increase of the importance of energy security is to be expected, both globally and regionally. Also, we will be faced with the increased competition for influencing both the suppliers and transit countries, but also for the control over the energy resources, delivery routes (pipelines) and technologies.

REFERENCES

1. Assante, M. J. (2009). Infrastructure Protection in the Ancient World. *Proceedings of the 42nd Hawaii International Conference on System Sciences – 2009*, http://www.hicss.hawaii.edu/HICSS_42/BestPapers42/ElectricalPower/ReliabilityAndCyberSecurity.pdf. Accessed 3. August 2013.
2. Council Directive (2008, 8 December). *Official Journal of the European Union L*, 345-375, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF. Accessed 8. August 2013.
3. *Critical Foundations: Protecting America's Infrastructures: The Report of the President`s Commission on Critical Infrastructure Protection* (1997). Washington D.C.: The Commission.
4. Gospić, N., Murić, G., Bogojević, D. (2012). Definition of Critical Telecommunication Infrastructure in the Republic of Serbia. *Memoirs from XXX Symposium of new technologies in postal and telecommunication traffic – PosTel 2012, Belgrade, 04 and 05 December 2012,* (str. 367-376.) Belgrade.
5. Yergin, D. (2006). Ensuring Energy Security. *Foreign Affairs* 85 (2), March-April, 69-82. http://www.un.org/ga/61/second/daniel_yergin_energysecurity.pdf. Accessed 8. August 2013.
6. Law on critical infrastructure (2013). *Peoples Papers* 56/13, The Republic of Croatia, http://www.zakon.hr/z/591/Zakon-o-kriticnim-infrastrukturama. Retrieved 2. August 2013.
7. Srbijagas (2013). South Steam, www.srbijagas.com/projekti/južni-tok.51.html. Retrieved 24. July 2013.
8. Spatial plan of the special purpose transnational gas pipeline, South Stream, "December 2012th, The Ministry of Natural Resources, Mining and Spatial Planning of the Republic of Serbia.
9. Fatić, A.(2012, 12.03) Region needs joint defence strategy, *SEETimes*, http://setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/features/2012/12/03/feature-01
10. Fisher, J. (2013, 03 19). The Balkanization of the Middle East, *Today*, www.danas.rs.danasrs/dijalog/balkanizacija_bliskog_istoka.46.html?news-id=257660. Accessed 24. July 2013.
11. Defence Strategy of the Republic of Serbia, Section 5.1.
12. The trade agreement between Serbia and Russia on the duty-free import of goods,
13. Internet portal, Energetics, 14.03.2013. http://www.naturalgaseurope.com/pdfs/GDSS1SERB-Dusan%20Bajatovic%20Presentation%20South%20Stream%20Serbia%20-%20DB.pdf

UDC 726.9:75.041.5
ID 176374796

Kristina Radojević, Zoran Dragišić
University of Belgrade, Faculty of Security Studies
kristinaradojevic@gmail.com
zoran.dragisic@yahoo.com

A MODEL OF SECURITY MANAGEMENT SYSTEM FOR TRANSPORTATION SYSTEMS

Abstract: The Transportation Systems Sector, a sector that comprises all modes of transportation (aviation, maritime, mass transit, highway, freight rail, and pipeline), is a vast, open, interdependent networked system that moves millions of passengers and millions of tons of goods. The transportation network is critical to the way of life and economic vitality. Ensuring its security is the mission charged to all sector partners, including governments (national, regional, local) and private industry stakeholders. The transportation systems represent very important part of critical infrastructure. The security and safety of transportation influence all other social and industrial processes. The disruption of this system causes disruptions in all other segments of social life. The specific characteristics of this system which influence its security are: easy accessibility, interconnection and vastness. Hence, the tolerance of this system to malfunctions and security and safety risks is very low. In order to achieve security and safety, along with reliability, efficiency and punctuality of these systems, we need to consider applying integrated approach to security and safety management systems. Like many other critical infrastructure sectors, the Transportation Systems Sector faces a dynamic landscape of potential natural disasters, accidents, and terrorist attacks. The terrorist threat poses special challenges. Taken together, the risk from terrorism and other hazards demands a coordinated approach involving all sector stakeholders. Stakeholders throughout the sector have been and continue to be actively developing methods to improve their operational security and overall resilience. However, since the Transportation Systems Sector is segmented by individual modes, an increased emphasis is needed on a risk-based approach across the entire transportation spectrum. Security management systems by integrating security awareness throughout the organization and verifying compliance through quality assurance can be a significant force in achieving the highest possible level of regulatory compliance. Specific security practices, training and audit functions within a security management system should all be built so as to ensure compliance with applicable national transportation security programs. As an attempt to deal with all those problems, this paper presents an integrated approach to safety and security and a model of safety and security management system for transportation organizations.
Key words: *security, safety, management, transportation, safety and security management system*

1. INTRODUCTION

The transportation sector is a vast, open, interdependent networked system that moves millions of passengers and millions of tons of goods. Safety and security have always been essential conditions for this sector. These issues in travel and tourism came to the front by the evolution of the mass tourism from the beginning of the 1950s. But it is an undeniable fact that safety and security issues gained a much bigger importance in the last two decades in transport and travel industry. Changes in the World during the last two decades

were enormous. Due to terrorist acts, local wars, natural disasters, epidemics and pandemics, that we were witnesses to, security has significantly decreased. The transport and travel industry could not avoid the negative impacts and consequences of these events.

By the US Executive Order 13010 (EO 13010, 1996), transportation is a part of critical infrastructure, and it represents: "physical distribution systems critical to supporting the national security and economic well-being of this nation, including the national airspace systems, airlines, and aircraft, and airports; roads and highways, trucking and personal vehicles; ports and waterways and the vessels operating thereon; mass transit, both rail and bus; pipelines, including natural gas, petroleum, and other hazardous materials; freight and long haul passenger rail; and delivery services" (U.S. Congressional Research Service [USCRS], 2003). In 2006 the European Commission adopted a package of measures for critical infrastructure protection, which included measures for transport infrastructure (European Commission [EC], 2006).

The transportation systems represent very important part of critical infrastructure. Safety and security are of primary concern for any transport system. They are at the forefront of everyone's mind when they travel (EC, 2006). The security and safety of transportation influence all other social and industrial processes. The disruption of this system causes disruptions in all other segments of social life. The specific characteristics of this system which influence its security are: easy accessibility, interconnection and vastness. Hence, the tolerance of this system to malfunctions and security and safety risks is very low. In order to achieve security and safety, along with reliability, efficiency and punctuality of these systems, we need to consider applying an integrated approach to security and safety management systems.

To eliminate or prevent identified failure in this complex system, the safety program has to go beyond the available local information and make causal inferences stretching much further back in time and up into the higher system levels to understand why some events happened. The analyst is able to do so for causal factors closely related in time and space to the event by applying individual knowledge and expertise. But it is extremely difficult to systematically identify latent failures in management activities and monitor management interventions to control risk. Without a systematic model to see the broad picture and show the relative safety priorities, the effectiveness of management remedial action is difficult to monitor (Lin, 2011).

2. TRANSPORT SYSTEM SAFETY

Creating the environment for safe transport is essential for the European citizens (EC, 2006). In fact, this is true for any country in the world. Whether a transport organization is privately or publicly owned, safety is crucial for passengers as well as for employees.

The European Commission strives to provide the highest standards of safety worldwide. In the European Union (EU) there are safety agencies dealing with the different transport modes – EASA, ERA and EMSA, responsible for the aviation, rail and maritime sectors respectively – and all contribute to the advances in safety (EC, 2006).

Aviation is one of the safest and fastest growing forms of transport. The EU air safety policy ensures a high level of safety for passengers, promoting rules that are cost efficient and facilitate the free movement of products, services and persons involved in civil aviation. Given the unprecedented growth in air traffic and large number of carriers resulting from

the successful implementation of the single aviation market, the EU has prioritised work on effective aviation safety standards. These are the basis for a list of airlines banned from EU skies which is constantly updated. Road transport is the most widely used means of travel and a primary cause of accidents. The EC has been very active in promoting rules, technical standards, and awareness campaigns to decrease the number of fatalities caused by road accidents. It is mainly done by establishing road safety policy, raising awareness through different types of projects, public consultations, development of manuals and best practices in road safety, raising the safety culture, etc. In maritime transport passenger ship safety is of paramount importance. The European Commission has progressively developed safety policies in response to several major shipping accidents since the 1990s. Europe's railways are among the safest in the world. The policies of the European Union aim to maintain high standards and align safety requirements EU-wide. This is essential if they strive to achieve a Single European Railway Area (EC, 2006).

The major airlines have started to employ safety management activities such as accident prevention and flight safety programs, wishing to improve their safety records. Such activities are often overseen by a safety office which monitors the overall operating experience and provides independent advice to company management on the action needed to eliminate or avoid identified hazards, or to reduce the associated risks to an acceptable level. The failures and accidents rarely occur from random failures of hardware. They usually arise from a complex combination of factors both in the operational level (for example pilot, crew, ATC, dispatcher) and in the supporting processes of maintenance, airline management policy, aircraft design, etc. (Lin, 2011). The safety management systems (SMS) which are being applied within airline companies provide good basis for safety incident prevention and reduction. This model should not be used only for airlines, but for any organization which deals with critical infrastructure, and for all transport organizations, whatever mode of transport they use.

3. TRANSPORT SYSTEMS SECURITY

The transport industry remains a legitimate target in the eyes of terrorists. The focus of terrorist attacks has changed since 2001 as now casualties are a central part of terrorist operations rather than simply be collateral damage. Since 2001, every organization involved in transportation has re-assessed and is still re-assessing their security measures (International Air Transport Association [IATA], 2011).

Transport security is a sensitive issue that affects us all across the world. In transport, it often refers to terrorist attacks. As rare as such an event might be, the risk remains, and exposes the vulnerabilities of the entire transport supply chain. Other forms of security threats to transport are more common: crimes committed on the premises of transport operators (like a break-in), a robbery of a valuable cargo in transit, or armed piracy on the high seas. These have a massive economic cost which can be measured in terms ranging from the cash value of cargo thefts to insurance losses, business interruption and damage to property. In order to maintain proper security levels cooperation with third countries is paramount. The European Commission consolidates and strengthens security by working together with major international partners, exchanging experiences and best practices (EC, 2006).

The security management systems (SeMS), by integrating security awareness throughout the transport organizations and verifying compliance through quality assurance, can be a significant force in achieving the highest possible level of regulatory compliance. Specific security practices, training and audit functions within a security management system should all be built so as to ensure compliance with applicable national aviation security programs (IATA, 2011). New technologies can really assist in developing smooth high-security systems for the future but without making the security checks too long and intense.

4. SAFETY AND SECURITY MANAGEMENT SYSTEM FOR TRANSPORT ORGANIZATIONS

A Security Management System (SeMS) is an element of the corporate management responsibility which sets out a company's security policies and its intent to manage security as an integral part of its overall business. However, it is important to keep in mind that each organization must implement the system that works best in their specific situation – there is no 'one-size-fits-all' system. A SeMS is a businesslike approach to security. As with any business plan, the goals are set, the levels of authority are established and so on. Ultimately, SeMS becomes woven into the fabric of the organization and becomes part of its culture (IATA, 2011).

According to process engineering approach all the processes which have same or similar purpose could be managed from the same centre. Here we are adopting this approach. Having reviewed the research evidence on security and safety management models which are being used in transport organizations across the globe (Hong Kong, Taiwan, Australia, USA and EU), we concluded that both of these models have same structure and similar elements. Since the ultimate objective of any safety and security management system is to prevent injury and hazards in the workplace, we are convinced that security (SeMS) and safety (SMS) management systems could be integrated in one management system.

There are numerous elements of safety and security management system in transportation. The main elements could be classified as follows:

1. A safety and security policy which states the commitment of the organization responsible for transport to safety and security;
2. A structure to assure implementation of the commitment to safety and security;
3. Training to equip personnel with knowledge to work safely and without security risks to passengers and personnel;
4. In-house safety and security rules to provide instruction for achieving safety and security management objectives;
5. A program of inspection to identify hazardous conditions and for the rectification of any such conditions at regular intervals or as appropriate;
6. A program to identify hazardous exposure or the risk of such exposure to the workers and passengers and to provide suitable personal protective equipment as a last resort where engineering control methods are not feasible;
7. Investigation of accidents or incidents to find out the cause of any accident or incident and to develop prompt arrangements to prevent recurrence;
8. Emergency preparedness to develop, communicate and execute plans prescribing the effective management of emergency situations;

9. Evaluation, selection and control of sub-contractors to ensure that sub-contractors are fully aware of their safety obligations and are in fact meeting them;
10. Safety committees;
11. Evaluation of transport related hazards or potential hazards and development of safety and security procedures;
12. Promotion, development and maintenance of safety and security awareness;
13. A program for accident control and elimination of hazards before exposing personnel and passengers to any risk;
14. A program to protect workers from occupational health hazards (Hong Kong Labour Department [HKLD], 2002).

These elements were examined by a group of authors in order to determine which are of the most importance in airline industries. The model resulted from the research is given in Figure 1 below. It is hereby assumed that there are no significant differences in managerial sense between air and other modes of transportation considering security and safety. So it is absolutely appropriate to use this model as a guide for any organization in transportation sector.

General safety and security rules include clear instructions to personnel. In any organization, especially in transportation organizations, there should be a system for the identification and establishment of specialized in-house safety rules, specialized work rules, specialized work permits and procedures.

Measuring the safety and security performance against the predetermined plans and standards exposes the need for remedial action. Monitoring activities signalize management commitment to safety and security objectives in general. They are an essential part of developing a positive safety and security culture. There are two types of monitoring systems (HKLD, 2002):

(a) Active systems which monitor the achievement of objectives and the extent of compliance with the pre-set standards, and

(b) Reactive systems which monitor accidents, incidents and other evidence of deficient safety and security performance.

Inspection is an active monitoring program.

The element of the safety and security management system regarding risk management is a pro-active one which seeks to promote continuous improvement of the working environment and ensure that hazards are identified timely so that risks can be assessed and controlled before anyone (or anything) is adversely affected. In order to identify hazards and assess their associated risks, the organization should prepare items, such as premises, people and procedures, and gather information about them. After the identification of the hazardous exposure or the risk of such exposure to the workers and passengers, the organization should find out whether the planned or existing safety precautions (if any) are sufficient to keep the risk under control and meet the legal requirements.

The investigation of accidents or incidents forms part of a reactive monitoring system which is triggered after an event and includes identifying and reporting (HKLD, 2002):

(a) Injuries and cases of ill health;

(b) Other losses, such as damage to property;

(c) Incidents, including those with the potential to cause injury, ill health or loss;

(d) Hazards, and

(e) Weaknesses or omissions in performance standards.

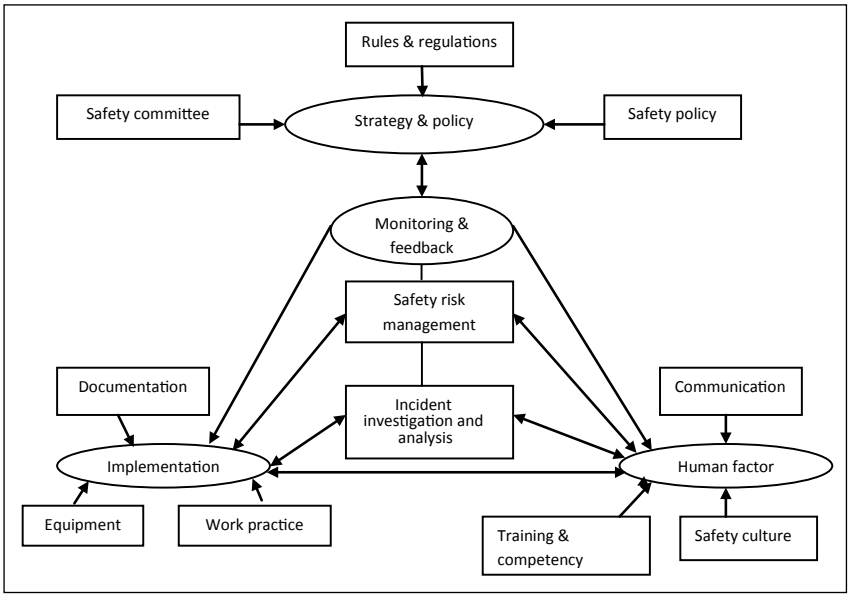


Figure 1 - Impact Relation Map (IRM) for an effective Safety Management System (SMS) (Source: Liou, J. J. H., et al., 2008)

Each of the above provides opportunities for a transportation organization to check safety and security performance, learn from mistakes, and improve the safety and security management system and risk control. The information gathered from investigations is useful in reinforcing key safety and security messages.

Training helps people acquire the skills, knowledge and attitudes to make them competent in the safety and security aspects of their work. It includes formal off-the-job training, instruction to individuals and groups, and on-the-job coaching and counselling. It is helpful to integrate the safety and security requirements of each job into the individual job specifications. Each transportation organization should devise and refine or adjust its training policy systematically.

The objective of safety and security promotion is to develop and maintain awareness among all personnel of (a) the organization's commitment to safety and security; and (b) individual person's responsibility to support that commitment. In the proposed model, this promotion is represented by the elements of communication and development of safety and security culture. The concept of communication refers to the transfer of information to employees about the possible risks in the workplace and the correct way to combat those risks (Fernández-Muñiz et al., 2007).

4.1. Safety and security policy

The term 'policy', refers to the general intentions, approach and objectives of an organization together with the criteria and principles on which actions and responses are based. The effective safety and security policy sets a clear direction for the organisation to follow. It contributes to all aspects of business performance as part of a demonstrable commitment to continuous improvement. The objective of defining the safety and security policy is to set down in clear and unambiguous terms its management's approach and commitment to safety and security. The organisation's most senior management should define, document and endorse its safety and security policy.

The transport organization should ensure that the policy includes a commitment to (HKLD, 2002):

(a) Recognize safety and security as an integral parts of its business performance;

(b) Achieve a high level of safety and security performance, in compliance with legal requirements as the minimum;

(c) Provide adequate and appropriate resources to implement the policy;

(d) Make the management of safety and security one of the prime responsibilities of managers at all levels, from the most senior executives down to the front line supervisory staff;

e) Ensure its understanding, implementation and maintenance at all levels in the organization;

(f) Consult and involve employees so as to secure their commitment to the policy and its implementation;

(g) Keep the policy and the management system under periodic review and audit/ review compliance with policy; and

(h) Ensure that employees at all levels have received appropriate training and are competent to carry out their duties and responsibilities.

The safety and security policy should be written, specific and relevant to the transportation mode and the organization itself. An effective safety and security management system should have a self-regulating and self-improving mechanism built in. This is affected by reviewing the safety policy from time to time by way of (a) performance measurement, and (b) safety and security audits or reviews.

4.2. Safety and security committee

A safety and security committee should carry out the following functions for the purposes of identifying, recommending and keeping under review measures to improve the safety and security of personnel in transport organization (HKLD, 2002):

(a) Monitoring of the safety and security policy — determining whether it is adequate and how well it is being implemented;

(b) On-going evaluation of hazards and arrangements to implement safety and security measures;

(c) Establishment of arrangements to deal promptly and effectively with dangerous working conditions, including those coming to light in disputes arising from workers refusing to work on the grounds of imminent danger;

(d) Discussion and establishment of a mechanism to resolve disputes when workers refuse work on the grounds of imminent danger;

(e) Assistance in the development of safe working procedures and safe and secure systems of work;

(f) Vetting of accident/incident/ill-health statistics to identify trends and monitor safety performance, and submission of reports on its findings to the top management with recommendations;

(g) Examination of safety and security audit reports and submission of reports on its observations to the top management with recommendations;

(h) Scrutiny of safety and security performance reports submitted by the safety office and giving of direction on appropriate actions;

(i) Monitoring of the adequacy and effectiveness of safety and security training;

(j) Monitoring of the adequacy of safety and security communications and publicity in the workplace;

(k) Organization of safety promotion activities such as safety competitions, exhibitions, safety incentive schemes, and safety suggestion schemes, and

(l) Provision of links with external sources regarding safety and security.

The safety and security committee should organize regular site visits for its members to enable them to experience the actual situations on the ground so that they can add a practical touch to their working strategies. Their regular presence on site also serves to good public relations and promotional purposes.

The safety and security committees are most likely to prove effective when their work is related to a single establishment rather than a collection of workplaces at different locations.

Therefore, if the proprietor or contractor is running a business consisting of two or more establishments in separate places, he should have two or more safety and security committees. An example is a large transportation organization with branches in different districts. In this case, there should be a safety and security committee per location at the workplace level, as well as a central safety and security committee at the enterprise level.

4.3. Safety and security culture

The phrase 'safety culture' was first used by the International Nuclear Safety Advisory Group (INSAG) in a report following the 1986 disaster at the Chernobyl Nuclear Power Plant. Amongst other causal factors, it was reported that the lack of safety culture, both within the Chernobyl plant and at a national level, contributed to the incident (INSAG-1, 1986).

Several meanings have been attributed to the term safety culture, giving rise to numerous definitions. Despite this, it is possible to identify various common aspects allowing us to propose the following definition of a positive safety culture: "A set of values, perceptions, attitudes and patterns of behaviour with regard to safety shared by members of the organi-

zation; as well as a set of policies, practices and procedures relating to the reduction of employees' exposure to occupational risks, implemented at every level of the organization, and reflecting a high level of concern and commitment to the prevention of accidents and illnesses" (Fernández-Muñiz et al., 2007).

Despite the lack of consensus in definitions and models of safety culture, there is some agreement that a strong safety culture is an organisational culture that places a high priority on safety-related beliefs, values and attitudes. Whilst the literature often presents safety culture as a specific issue, it can be argued that it is a result of the overarching organisational culture, and is perhaps better viewed as a sub-component or effect of organisational culture, and not a culture in itself (Edwards, et al., 2013).

A culture of safety and security that governs the attitudes and behaviour of individuals should be integrated in the management system. Safety culture and security culture are based on similar principles. Safety culture is defined as "the assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance" (International Atomic Energy Agency [IAEA], 2010).

Security culture has the same definition except for a focus on security issues. Nonetheless, there are some elements that are unique to each culture. For example, one difference between the two cultures relates to the way information is handled. In the security field, the sharing of information should typically be restricted to a small and select group of individuals in order to prevent sensitive information related to protective measures or facility weaknesses from falling into the hands of adversaries. Further, it is also important to take measures to ensure that the knowledge of malicious acts does not encourage similar events. The general rule in the safety area, by contrast, is to pursue transparency. The management should also seek the promotion of both safety and security culture. These cultures often involve individuals of diverse backgrounds and experiences. That is, security personnel, unlike safety personnel, often have military or police backgrounds. Since culture is an attribute of both organizations and individuals, it is important to provide both safety and security staff with an appreciation of the importance of each area, while emphasizing the importance of cooperation and balance to achieve optimized protection. The recognition of the difference in backgrounds should be taken into consideration in these efforts (IAEA, 2010).

Managers should be strongly committed to safety and security and should be extremely sensitive to the consequences of accidents and serious injuries and their effects on the victims. This commitment should be reflected in managers' awareness of the problems, in their concern for safety and security, in their conviction that high levels of safety and security can be attained, in their ability to demonstrate a continuous positive attitude to safety and security, in their ability to promote safety and security actively at all levels of the organization, in their low tolerance of failure to comply with safety and security norms. But attitudes and positive words contained in a formal declaration of principles are insufficient to modify employee behaviour and reduce accident rates. Good intentions have to be translated into daily experience, and management decisions should reflect an interest in investing, not only for further profit, but also for people (Fernández-Muñiz et al., 2007).

5 CONCLUSION

The development of a safety and security management system involves planning and developing.

Planning is the process of determining in advance what should be accomplished. The planning stage answers the questions: "Where are we now?" and "Where do we want to be?" Developing is the process of determining how the safety and security objectives should be realized. The developing stage needs to answer the question: "How do we get there?"

The implementation of a safety and security management system involves organizing and implementing. Organizing is the process of prescribing formal relationships between people and resources in the organization to accomplish objectives, and implementing is the process of carrying out or putting into practice the plans to achieve the desired objectives, with the appropriate and adequate control to ensure proper performance in accordance with the plans.

The maintenance of a safety and security management system involves measuring and auditing or reviewing, through which an organization knows whether the safety and security management system of its relevant industrial undertaking is working well or needs improvement, thereby maintaining the system in an efficient and effective condition.

Measuring is the process of checking performance against the agreed standards to find out when and where the improvement is needed, and a means of monitoring the extent to which policies and objectives are being met.

Auditing or reviewing is carried out to assess performance in addition to routine monitoring of safety and security performances. Auditing or reviewing constitutes the 'feedback loop' to the planning stage which enables the relevant industrial undertaking to reinforce, maintain and develop its ability to reduce risks to the fullest extent and to ensure the continued efficiency, effectiveness and reliability of the safety management system. In addition, there should be information flowing between the development, implementation and maintenance stages and the auditing/reviewing stage so as to ensure the correct operation of the safety and security management system.

Safety and security audits or reviews should assess whether or not the processes as described in the management model have been successfully and effectively followed in order to develop, implement and maintain a safety and security management system.

The implementation of safety and security management system in transportation system is a complex task and involves a number of entities within and outside of the transport organizations. It is of crucial importance that all affected parties are aware of what is expected of them, who they will need to co-operate with and when. The size and scope is very dependent on many variables including the size of the organizations, the current level of integration, regulatory requirements, etc.

But, without systematic approach to safety and security, transportation sector would be left unprotected and not capable to accomplish its only mission which is safe and secure passenger and freight transportation.

REFERENCES

1. Edwards, J. R. D., Davey, J., Armstrong, K. (June 2013). Returning to the roots of culture: A review and re-conceptualisation of safety culture. Safety Science 55, pp. 70-80.
2. European Commission. (2006). Transport Safety and Security. Retrieved from http://ec.europa.eu/transport/index_en.htm
3. Executive Order 13010. (1996). Retrieved from http://www.fas.org/irp/offdocs/eo13010.htm
4. Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J. (2007). Safety culture: Analysis of the causal relationships between its key dimensions. Journal of Safety Research, Volume 38, Issue 6, pp. 627-641.
5. Hong Kong Labor Department, Occupational Safety and Health Branch. (April, 2002). Code of Practice on Safety Management First ed. Retrieved from http://www.info.gov.hk/labour/public/index.htm
6. International Atomic Energy Agency (IAEA). (2010). A report of the International Nuclear Safety Group, INSAG-24. An Interface between Safety and Security at Nuclear Plants. Retrieved from http://www-pub.iaea.org/MTCD/publications/PDF/Pub1472_web.pdf
7. International Air Transport Association (IATA). (March 2011). Security Management System (SeMS) for Air Transport Operators. Executive Summary. Retrieved from: http://www.iata.org/whatwedo/Documents/SEMSv32Summary1.pdf
8. Lin, P. H. (2011). Safety Management and Risk modelling in Aviation – the challenge of quantifying the management influences. Enschede: Gildeprint Drukkerijen.
9. Liou, J. J. H., Yen, L., Tzeng, G. H. (2008). Building an effective safety management system for airlines. Journal of Air Transport Management 14, pp. 20-26.
10. U.S. Congressional Research Service, Resources, Science, and Industry Division. (January 29, 2003). Critical Infrastructures: What Makes an Infrastructure Critical?. Authors: Moteff, J., Copeland, C., Fischer, J. Report for Congress, RL31556. Retrieved from http://www.fas.org/irp/crs/RL31556.pdf

UDC 726.9:75.041.5
ID 176374796

Momir Ostojić. Željko Ivaniš, Vladimir Ajzenhamer
University of Belgrade, Faculty of Security Studies
ostojicmomir@yahoo.com
landol@eunet.rs
vladimirajzenhamer@yahoo.com

CRITICAL INFRASTRUCTURE IN AIR TRAFFIC MANAGEMENT SYSTEM[1]

Abstract: The paper is devoted to the analysis of air traffic management system in the context of critical infrastructure, as a necessary requirement for the safe, regular and expeditious air navigation. The authors analyze relevant legal and professional documents in the field of air navigation and the protection of critical infrastructure, and also try to provide a functional and comparative systems analysis and a statistical analysis of essential air traffic data. At the end, the results of this analysis should provide an answer to the research question of the determination of Air Traffic Management System in national and European critical infrastructure, in relation to its supranational character which is obtained through the "Single European Sky" regulatory framework.
Keywords: *safety, security, protection, air traffic, critical infrastructure*

1. INTRODUCTION

In order to answer the question of defining Air Traffic Management System in the context of national and European critical infrastructure (CI), it is first necessary to analyze the definition and understanding of a CI. For this purpose, we will give a comparative overview of the definition and content of CI concepts in the United States (U.S.), the European Union (EU) and the Republic of Serbia.

In the U.S., homeland security is designated as the highest national priority. CI protection is under the jurisdiction of Department of Homeland Security, which defines it as follows: "critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[2] The Department of Homeland Security builds and maintains a comprehensive assessment of nation's infrastructure sectors:

1 The paper was written within the scientific research project No. 47029: "Cost-effective choice of new technologies and defense concepts through social change and the strategic orientation of Serbia in the 21st century." The Project is funded by the Ministry of Education and Science of the Republic of Serbia in 2011-2014. The project leader is Professor Momčilo Milinović, PhD.

2 http://www.dhs.gov/what-critical-infrastructure

- Food;
- Water;
- Agriculture;
- Health systems and emergency services;
- Energy (electrical, nuclear, gas and oil, dams);
- Transportation (air, road, rail, port, waterways);
- Information and telecommunications;
- Banking and finance;
- Energy;
- Chemical;
- Defense industry;
- Postal and shipping;
- National monuments and icons.[3]

The mentioned understanding and definition of critical infrastructure is described by many authors in their analyses and efforts to set up a methodology for identifying CI. For example, Baker H. G. defines CI sectors as "foundations of modern societies". He emphasizes the following: "To understand and correct exploitable susceptibilities of CI facilities, infrastructure providers and regional planners need a common, repeatable, systematic methodology to understand the comparative risks and vulnerabilities and determine where to invest scarce resources."[4]

Although European and American definitions and CI protection programs are very similar, in European documents we can identify definitions that seek to delineate the European CI and national CI of the Member States (MS). Thus, the Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP) gives separate definitions of CI and European Critical Infrastructure (ECI).

CI include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on health, safety, security or economic well-being of citizens or the effective functioning of governments.

ECI include those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more MS.

The definition of what constitutes an ECI is determined by its cross border effect which ascertains whether an incident could have a serious impact beyond two or more member states national territories.[5] The European Council clarifies that ECI means CI located in MS, the potential destruction or disruption of which would have a significant impact on at least two MS. In addition, there are two sets of criteria to identify ECI:

- *Cross-cutting criteria*: casualties, economic effects and public effects criterion

---

3 The Department of Homeland Security, White House, June, 2002.
Moteff, J., Copeland, C., Fischer, J. (2003). Critical Infrastructures: What Makes an Infrastructure Critical?, Report for Congress, Order Code RL31556, Congressional Research Service, The Library of Congress, USA, 2003.

4 Baker, H. G. (2003). A Vulnerability Assessment Methodology for Critical Infrastructure Facilities, Institute for Infrastructure and Information Assurance, http://www.jmu.edu.

5 Green Paper on a European Programme for Critical Infrastructure Protection, Commission of the European Communities, (2005). Brussels.

- *Sectoral Criteria* have been established for Transport and Energy sectors (classified).[6]

Green Paper on a EPCIP gives an Indicative List of CI Sectors which includes all sectors as defined by the Department of Homeland Security. Eleven sectors are included, within which 37 products or services are specified.

ECI includes transboundary effects resulting from interdependencies between interconnected infrastructures across various sectors. The procedure for the identification and designation of ECI, and a common approach to the assessment of the needs to improve the protection of such infrastructures will be established by means of a Directive.[7]

In the Republic of Serbia, the area of CI protection is not systematically arranged. It could be argued that some systematic solution existed there before the transitional changes, in the Law on Basic Social Self-protection,[8] and later, in the Law on System of Social Self-protection.[9] This law regulates that any company, government bodies and local authorities must have service protection organized with the levels of the organization, rights and duties. Although the system solutions were adjusted to the socialist political system, the system of social self-protection also covered the protection of CI under different names, while the organization and functioning of the system corresponded to the American Homeland Security.

Although the change of the political system did not bring new system solutions that would replace the previous ones, the process of Serbia's EU accession and the work on the implementation of European decisions led to the partial use of the term CI in certain documents and legal documents, in an attempt to cover the field of European legislation. Thus, the Strategy for Development of Information Society in the Republic of Serbia until year 2020[10] states "the need to develop and promote the protection against the attacks with the application of information technology on CI systems, which in addition to ICT systems can be other infrastructure systems that govern the use of ICT, such as electro-energy system. In this connection, it is necessary to further regulate the criteria for determining the CI from the perspective of information security, the criteria for characterizing attacks using information technology to such infrastructure in comparison to conventional forms of attack, and protection requirements in this area." The Guidelines on the methodology for the development of risk assessment and protection and rescue plans in emergency situations[11] determine CI assessment from the point of vulnerability of natural and other disasters, and the need to identify objects particularly in the areas of:

- Production and distribution of electricity
- The supply of energy (energy distribution network)
- Water supply
- To supply the population with food
- Healthcare
- Physical and cultural resources and the environment

6 European Council Directive 2008/114/EC on December 8th 2008.

7 Communication from The Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final, Commission of The European Communities, Brussels, 2006.

8 Zakon o osnovama društvene samozaštite, Službeni list SFRJ 39/73.

9 Zakon o sistemu društvene samozaštite, Službeni list SFRJ 14/86.

10 Strategija razvoja informacionog društva u Republici Srbiji do 2020, Vlada Republike Srbije, 2010.

11 Uputstvo o metodologiji za izradu procene ugroženosti i planova zaštite i spasavanja u vanrednim situacijama, Službeni glasnik RS 096/2012.

- Protected natural resources
- Telecommunications
- Traffic (traffic and road network, rail network, river navigable roads, bridges, viaducts and tunnels)
- Production of hazardous substances.

In this document, the term traffic is used to refer only to transport by land and water, while air traffic and air transport are not mentioned. In the section relating to the protection and rescue plan it is determined that they are elaborated as a whole, with strong specific actions in relation to the type of hazard, and shall include, among other things, "the organization of protection of CI facilities (utilities, electrical energy, transport)."

2. AIR TRAFFIC MANAGEMENT

As defined by the Eurocontrol Special Committee on Future Air Navigation Systems (FANS), it is a system consisting of a ground part and an air part, both of which are needed to ensure the safe and efficient movement of aircraft during all phases of operation. The airborne part of Air Traffic Management (ATM), according to FANS, consists of the functional capability which interacts with the ground part to attain the general objectives of ATM. The ground part of ATM comprises the functions of:

- *Air Traffic Services* (ATS) are the primary components of ATM, a generic term meaning: Flight Information Service, Alerting Service, Air Traffic Advisory Service, Air Traffic Control Service, Area Control Service, Approach Control Service or Aerodrome Control Service.
- *Airspace Management* (ASM), a generic term covering any management activity provided for the purpose of achieving the most efficient use of airspace based on actual needs and, where possible, avoiding permanent airspace segregation
- *Air Traffic Flow Management* (ATFM), as service is established to support ATC in ensuring an optimum flow of traffic to, from, through or within defined areas during times when demand exceeds, or is expected to exceed, the available capacity of the Air Traffic Control system, including relevant airports, and should be developed as necessary to ensure this optimum flow.

The aggregation of ground based (comprising variously ATS, ASM, ATFM) and airborne functions is required to ensure the safe and efficient movement of aircraft during all appropriate phases of operations.[12]

In relation to the above, the ATM is a key system for the safe, orderly and efficient air transport which is identified, in every definition of CI, as one of the most important sectors. In terms of methodology and identification of the CI and interdependences of functions, its most sensitive part is the Air Traffic Control system, because the degradation of that system dictates the degradation of air transport itself.

12 Glossary of Terms and Definitions & List of Acronyms, Eurocontrol (2002). Safety Regulation Commission document, SRC DOC4.

3. AIR TRAFFIC MANAGEMENT IN THE UNITED STATES

The Air Traffic Control (ATC) system manages air traffic from various sources throughout the United States National Airspace System (NAS). The mission of ATC is "to promote the safe, orderly, and expeditious movement of aircraft." The Federal Aviation Administration (FAA) is responsible for providing the NAS infrastructure to enable continuous air operations in the U.S. ATC, the primary component of the NAS architecture, is a complex system comprising many types of facilities, a plethora of hardware and software systems, and complicated interactions between humans and machines. The ATC system has:

- 496 ATC Towers, at each airport are responsible for control of the aircraft on the ground before and after take-off and close to the airport.
- 180 Terminal Radar Approach Control (TRACON) control aircraft approaching and leaving the busiest airports.
- 21 Air Route Traffic Control Centres (ARTCCs), also called En Route Centres, which control aircraft over the continental U.S., each centre handling a region of airspace.
- Air Traffic Control System Command Centre (ATCSCC) coordinates operations between en route centres and provides scheduling and monitoring support.
- 75 flight service stations.
- 61 automated flight service stations.
- 40,921 operational facilities of all types.
- 36,349 employees.

The ATC system is strategic and is closely linked with the military ATC system. Considerable cooperation exists between the Department of Defence (DOD) and the ATC. Considerable thought has also been given to how the ATC system would operate in time of war. Many of the plans developed in this process also have application for dealing with terrorism.[13]

In terms of methodology and identification of the CI and interdependences of functions, the most sensitive parts are TRACON and ARTCCs whose work is reflected in the work of several airports and the system as a whole.

4. AIR TRAFFIC MANAGEMENT IN EUROPE

Operative part of the ATM in Europe is organized similarly as in the U.S., with the airport, approach, and terminal control (equivalent to American Towers, TRACON and ARTCCs) under the jurisdiction and sovereignty of European states and national providers of air navigation services.

The conceptual idea of creating a single European airspace, which dates back to the seventies when members of the Western European Union established Eurocontrol, has been a

13 Data Sources:
Knigh, C. J., Elder, C. M., Flinn, J, Marx, P. (1998). Analysis of Four Critical Infrastructure Applications, Computer Science Report No.CS-97-27 September 19, Department of Computer Science, University of Virginia.
Moteff, J., Copeland, C., Fischer J. (2003). Critical Infrastructures: What Makes an Infrastructure Critical?, Report for Congress, Order Code RL31556, Congressional Research Service, The Library of Congress, USA.
National Infrastructure Protection Plan, (2009). Partnering to enhance protection and resiliency 2009, US Department of Homeland Security.

political decision made in 1999 under the leadership of the EC. Regulatory support consists of two sets of regulations:

- SES (Single European Sky) I package: framework, airspace, service provision, interoperability regulations + implementing rules
- SES II package: performance regulation: performance Regime, Functional Airspace Blocks (FABs), Network Management; new technologies; capacity on the ground.

This regulation defines European airspace as a continuum that will not be affected by national borders and which corresponds to the operational requirements of civil and military aviation. In this sense, the Functional Blocks of Airspace (FABs) across national borders are introduced.

National air navigation services (ANS), which previously were government bodies, are transformed into the corporate organizations with the possibility of privatization and, as such, they entered the competition for the allocation of responsibilities in the FABs.

That is practically the case with a national ATM systems of European countries which compete against each other and each has a vision „...to stand out as the leading ANS provider in the region, and to be recognized as prestigious partner among our users and other business associates." In expert analysis, this reorganization is explained by the forecasted growth in air traffic, in order to reduce the delay and cost of services providers of ANS. After a number of different initiatives and negotiations over the past 10 years and the investment of huge amounts of money into the modernization and capacity building of national systems, well above their own needs, in order to become a "leading ANS provider in the region", the 9 FABs illustrated in Figure 1 were established. However, each state retained its Area ATC within the FABs. FABs sectorial boundaries, which are the border of states in the FAB, indicating that they are a group of states and that they are, in the background of explained operational needs, the outcome of political and other interests of some other European countries and NATO.

Eurocontrol has gathered all the countries of the European continent and Turkey with a defined mission: "To harmonize and integrate ANS in Europe, aiming at the creation of a *uniform* ATM System for *civil and military* users, in order to achieve the *safe, orderly, expeditious and economic* flow of traffic throughout Europe." It is declared as a civil-military intergovernmental organization with 39 Member States across the European continent that has a predominant role in the field of civil-military coordination, with civil-military ATM coordination in its portfolio. In cooperation with NATO, Flexible Use of Airspace concept has been developed based on the fundamental principle that airspace should not be designated as purely civil or military, but rather be considered as a continuum in which all user requirements should be accommodated to the greatest possible extent, and recommended the integration of civil and military ATM systems.

In the current European ATM system, there are:

- Eurocontrol – European Agency for Air Navigation Safety with
  - Central Flow Management Unit (CFMU)
  - Maastricht Upper Area Control Centre (MUAC), operated by Eurocontrol on behalf of four States, provides air traffic control for the upper airspace (above 24,500 feet, i.e. approximately 7,500 metres) of Belgium, the Netherlands, Luxembourg and north-west Germany.

- 69 Area Control Centres under States, of which 47 operate with 10 sectors or fewer at maximum configuration
- Over 600 sectors when at full capacity
- Approx. 16,000 Air Traffic Controllers
- Approx. 36,000 support staff
- Total revenue B€7.6/year.[14]

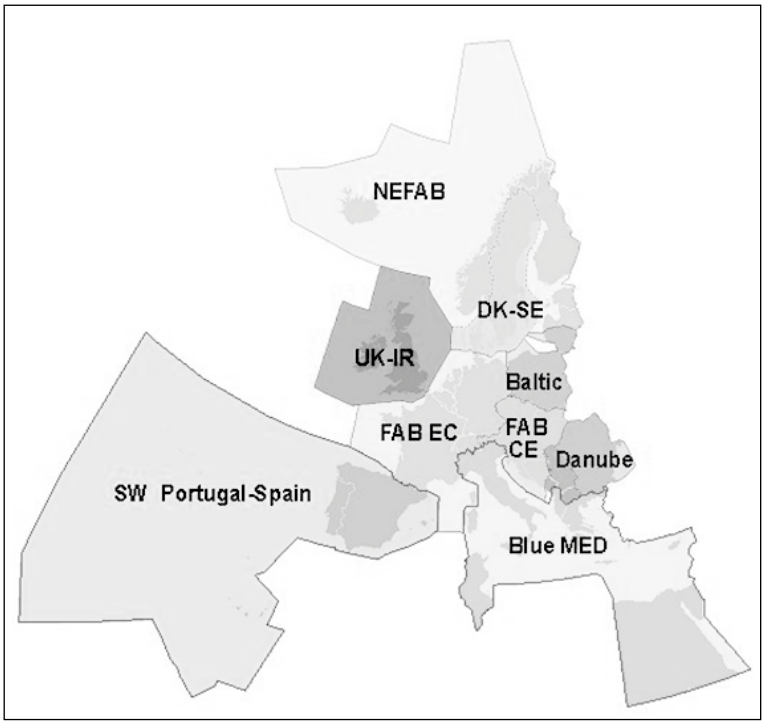


Figure 1: Functional Airspace Blocks
(Source: A Blueprint for the Single European Sky, IATA, 2013.)

From the perspective of the definition of national CI and ECI, the most sensitive part are the ACC under the jurisdiction of the states, whose work is reflected in its entire air transport within the state in which it is located, and in neighbouring states, and then in the flow of traffic in Europe. However, if the FAB comes to streamlining the current ACC in one location, the degree of criticality will increase in proportion to it.

The European Commission's Joint Research Centre and Eurocontrol, as the body responsible for managing Europe's air traffic are now about to sign a collaboration agreement as part of the EPCIP. Eurocontrol said that the expected outcome of cooperation is two-fold:

14 Data Sources:
Nogueras, A. (2012). Air Traffic Management moving into European Critical Infrastructure, MOTIA Conference, Rome, 29/03/2012.
Matsoukis, E., Poulimenakos, S. (2007). Air traffic management in the South East European countries. Current situation and prospects, European Transport\Trasporti Europei n. 37 (2007): 16-34.

a reinforcement of its role as Europe's Network Manager as regards security and crisis management, and the provision of additional means of improving network resilience, and that this development could also pave the way towards a centralized security service.[15]

5. AIR TRAFFIC MANAGEMENT IN THE REPUBLIC OF SERBIA

ATM System in Serbia is part of Serbian and Montenegro Air Traffic Services (SMATSA LLC) which was established on 29 December 2003 as a limited liability company, by the decision of the Government of the Republic of Serbia and the decision of the Government of Montenegro. SMATSA replaced the functions of the Federal Air Traffic Control Authority (FATCA), which previously functioned as a state government unit or a government unit of the former Yugoslavia's Ministry of Transportation, and then it repeated this role in the State Union of Serbia and Montenegro, with an integrated civilian and military ATC service.

SMATSA LLC is responsible for the provision of Air Traffic Service in airspace of the Republic of Serbia, Montenegro, and a part of the airspace over the Adriatic Sea and 55% of the upper airspace over the territory of Bosnia and Herzegovina, illustrated in Figure 2.

The owners of SMATSA LLC are the Republic of Serbia to 92% and the Republic of Montenegro to 8%.

Primary objective of the ATM provided by SMATSA LLC is the provision of air traffic services to civil and military aircraft in order to maintain and enhance safe, orderly, expeditious and efficient flow of air traffic within the airspace of the founding states and other neighbouring countries based on the bilateral state agreements. ATM comprises the jobs of airspace control, protection and allocation – civil-military coordination at pre-tactical and tactical levels.

In 2011 SMATSA had:

- 1 Area Control Centre
- 6 Terminal Control Centres[16]
- 6 civilian and 3 military Towers
- 550,874 flights (IFR)
- 2,460 flights during peak day
- 865 number of employees
- 178 flights during peak hour
- 8,466,897 (000 RSD) operating revenues

The air traffic within the jurisdiction of ATCC Beograd continued its growth in 2011. During the year, a record number of flights represent an increase by approximately 3% in comparison to 2010. In the last ten years, the air traffic has recorded an average increase of about 10% per year.

Conditioned by the volume and the expected traffic requirements, within the provision services to civil and military aircraft, SMATSA LLC contributes to the implementation of the Single European Sky.[17]

---

15 Brussels mulls security police for ATM network, (July 5, 2013) Air Traffic Management Net., www.airtrafficmanegement.net.

16 Integrated approach and area control functions in Air Traffic Control Centre (ATCC).

17 Annual Report 2011, (2012). Serbian and Montenegro Air Traffic Services, SMATSA, Belgrade.

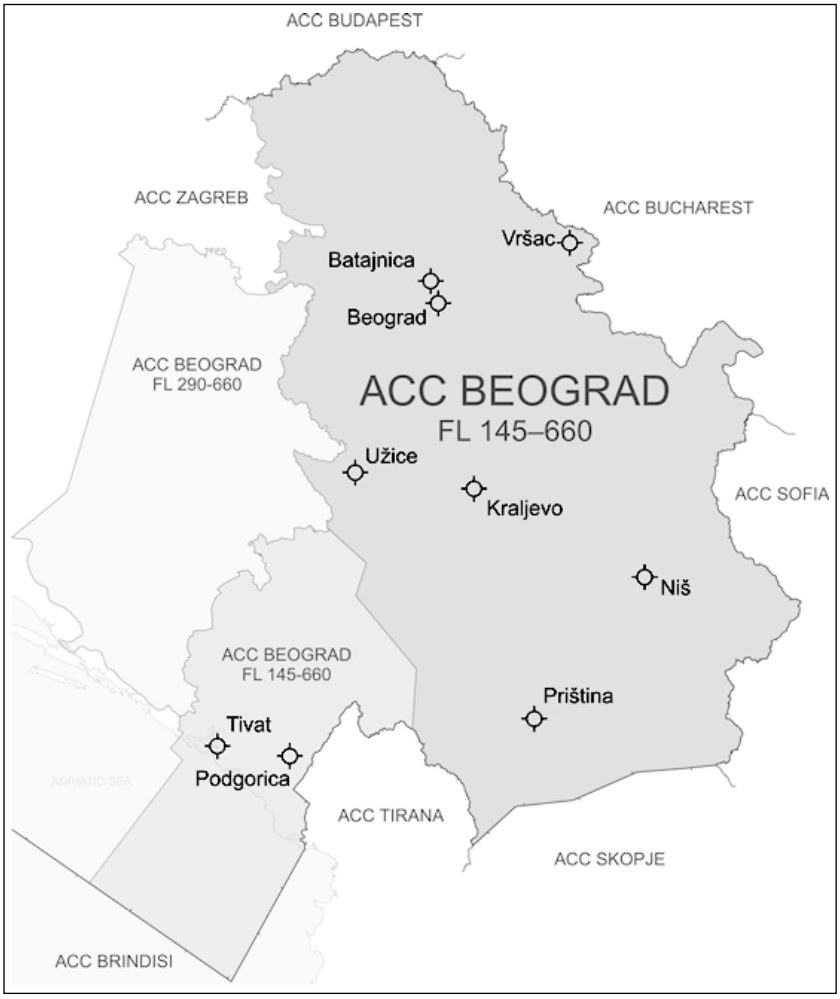


Figure 2: SMATSA Area of Responsibility
(Source: Annual Report, SMATSA, Belgrade, 2012.)

5.2. The problem ATM over the territory of the Autonomous Province of Kosovo and Metohija

SMATSA LLC operates in full compliance with the national and international legislation, as well as with relevant international agreements, and it became a member of the most important international aviation organizations with the integration into the European ATM system as a Eurocontrol member.

Although the integration of the entire ATM System into the incessantly developing European ATM system represents a great challenge that SMATSA LLC is facing with great success, there is a serious problem which concerns the airspace of the Autonomous Province of Kosovo and Metohija. This province is recognized by the U.S. and most European

countries as a self-proclaimed state of Kosovo, while the Serbian government considers it as an integral part of its territory and officially declares that Serbia will never, under any circumstances, recognize Kosovo independence. The operating result was the closure of airspace over the province for commercial aircraft flights from 1999 to this date.

Chicago Convention[18] guarantees the right of exclusive sovereignty of UN member states to manage their airspace, and may issue regulations which may differ from the set of international standards of ICAO. Serbian autonomous province of Kosovo and Metohija, as a self-proclaimed Republic of Kosovo is not a UN member, and therefore cannot dispose of the airspace.

After the NATO aggression against the Federal Republic of Yugoslavia (FRY) in 1999, which ended in the adoption of resolutions 1244 of the UN and the signing of the Military Technical Agreement between the International Security Forces ("KFOR") and the Governments of the FRY and the Republic of Serbia, the military forces of the FRY withdrew from the territory of the province, and before that, the province due to security reasons was left without the civil parts of the ATC service.

Resolution 1244 provided a possibility for the Military Technical Agreement to specify additional modalities, including the roles and functions of Yugoslav/Serbian personnel in Kosovo.[19] Military-technical agreement *temporarily* provided military commander of KFOR with jurisdiction over the airspace, with the possibility of transfer of competencies in the air space for the "*control of normal civilian air activities to appropriate FRY institutions.*" The transfer of this jurisdiction from KFOR Commander on International or any other institution is not intended by any provision of the Agreement or the Resolution. On the contrary, the relevant provision of the Agreement clearly provides that "*control of civil air traffic to be returned to civilian authorities as soon as practicable.*"[20] Despite such clear terms and uncompromising Serbia's accession to all European integration projects, NATO decided to assign the responsibility for air traffic control to the Hungarian air traffic control company "*Hungarocontrol*".[21]

6. CONCLUSION

The resemblance between the definitions and program activities in terms of the protection of CI indicates that the EU is trying to fully implement the U.S. model. However, the U.S. are example of a single national CI and uniform institutional approach to the matter of protection, while in the case of the EU the issue of definition and approach to European (ECI), and the issue of national CI of the member states, is treated separately.

The segments of the national Air Traffic Management systems (ATM) are recognized as both CI and ECI, due to interdependence of functions present in civil air traffic, and also due to tight correlation with the aviation component of the national defense systems and NATO. In the U.S., ATM system is centralized and operationally adjusted both to the civil and military needs. The EU regulatory framework establishes a similar model through

18 Convention on International Civil Aviation, ICAO, Doc. 7300/8, (2002). Eighth Edition.

19 In paragraph 10 Annex 2, UN Resolution 1244 (1999). Adopted by the Security Council at its 4011th meeting, on 10 June 1999.

20 In Section 2 Item 3 c) Military Technical Agreement between the International Security Force ("KFOR") and the Governments of the Federal Republic of Yugoslavia and the Republic of Serbia, 9 June 1999.

21 Source: Hungarian Air Navigation Services Pte. Ltd. Co. „Hungarocontrol", 20.06.2012.

"Single European Sky", but the influence of political (and other) interests on actual, operational needs is more than evident. As an argument for this claim we can use, among other things, the fact that NATO, contrary to the UN documents and standards, decided to assign the responsibility for the ATM in the airspace over Kosovo and Metohija to Hungarian "Hungarocontrol". This has been done despite the fact that this "portion" of the airspace is naturally and operationally linked to other parts of the Serbian airspace, which is an integral part of the "Single European Sky".

Considering that, due to the limited scope of this study, it was not possible to elaborate a complete explanatory analysis, we have focused primarily on the description of the baselines which are crucial for the identification of CI in the ATM system. We stressed those starting points that clearly indicate the need for national and European scientific community to devote their research activities to this serious security issue, but from the perspective of CI protection, both at national and at European level. Also, we pointed out that this should be done with respect to the principles of scientific objectivity and beyond the influence of experts and lobbyist "explanation" which in reality frequently descent from various interest groups.

SOURCES

1. Annual Report 2011, (2012). Serbian and Montenegro Air Traffic Services, SMATSA, Belgrade.
2. Baker, H. G. (2003). A Vulnerability Assessment Methodology for Critical Infrastructure Facilities, Institute for Infrastructure and Information Assurance, http://www.jmu.edu.
3. Brussels mulls security police for ATM network, (July 5, 2013) Air Traffic Management Net., www.airtrafficmanegement.net.
4. Communication from The Commission on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final, Commission of The European Communities, Brussels, 2006.
5. Convention on International Civil Aviation, ICAO, Doc. 7300/8, (2002). Eighth Edition.
6. European Council Directive 2008/114/EC on December 8th 2008.
7. Glossary of Terms and Definitions & List of Acronyms, Eurocontrol (2002). Safety Regulation Commission document, SRC DOC4.
8. Green Paper on a European Programme for Critical Infrastructure Protection, Commission of the European Communities, (2005). Brussels.
9. Knigh, C. J., Elder, C. M., Flinn, J, Marx, P. (1998). Analysis of Four Critical Infrastructure Applications, Computer Science Report No. CS-97-27 September 19, Department of Computer Science, University of Virginia.
10. Matsoukis, E., Poulimenakos, S. (2007). Air traffic management in the South East European countries. Current situation and prospects, European Transport\Trasporti Europei n. 37 (2007): 16-34.
11. Military Technical Agreement between the International Security Force ("KFOR") and the Governments of the Federal Republic of Yugoslavia and the Republic of Serbia, 9 June 1999.
12. Moteff, J., Copeland, C., Fischer J. (2003). Critical Infrastructures: What Makes an Infrastructure Critical?, Report for Congress, Order Code RL31556, Congressional Research Service, The Library of Congress, USA.
13. National Infrastructure Protection Plan, (2009.) Partnering to enhance protection and resiliency 2009, US Department of Homeland Security.
14. Nogueras, A. (2012). Air Traffic Management moving into European Critical Infrastructure, MOTIA Conference, Rome, 29/03/2012.
15. Strategija razvoja informacionog društva u Republici Srbiji do 2020, (2010). Vlada Republike Srbije, Beograd.
16. UN Resolution 1244 (1999). Adopted by the Security Council at its 4011th meeting, on 10 June 1999.
17. Uputstvo o metodologiji za izradu procene ugroženosti i planova zaštite i spasavanja u vanrednim situacijama, Službeni glasnik RS 096/2012.
18. Zakon o osnovama društvene samozaštite, Službeni list SFRJ 14/86.
19. Zakon o sistemu društvene samozaštite, Službeni list SFRJ 39/73.

UDC 726.9:75.041.5
ID 176374796

Ana Juzbašić
Airport Nikola Tesla, Belgrade
ana_juzbasic@yahoo.com

INTEGRATED PROTECTION OF CRITICAL TRANSPORTATION INFRASTRUCTURES: AIRPORT EXAMPLE

Abstract: Critical infrastructures consist of assets, facilities, services and information systems essential to the health, safety, security and economic well-being of citizens or the effective functioning of the government. They are to be protected comprehensively in the context of protected values/ system risks: economic, social, environmental, security and safety. One of the state responses to the crisis is restructuring of critical transportation infrastructure. Restructuring due to economic reasons and development of critical infrastructure protection are synergistic phenomena sharing the same goal - sustainable development. Analysis can determine whether restructuring contributes to their better performance. National critical infrastructure protection in the Balkans region is dealing with the challenges of contemporary threats. Among many classical issues, there are some recent momentums that contribute to the wide scope of critical infrastructure protection called integrated protection. This paper highlights the risks and vulnerability assessment and methodology to encompass airports as national critical transportation infrastructures. The research questions are: does airport restructuring affect compliance with all relevant protected values (system risks) and what aspects of protection are to be thoroughly investigated? Case study was used to analyze the restructuring of airports as public monopolies in transport. Several methods were used for collecting empirical evidence and analysis. General scientific research methods (analysis, synthesis, induction, deduction, analogy) were added to active research of theoretical and empirical data, relevant literature analysis, comparative method and case study. Content analysis was used to systematize the findings of various scientific disciplines. Research found each of the mentioned aspects in critical transportation infrastructures undoubtedly more valued after the restructuring with ownership change. This paper analyzed the activities to be implemented to mitigate system risks of safety, security, environment, economy and social momentum of airport operators in three layers - strategic, tactical and operational. These integrated protection aspects at an airport proved not to be directly affected by restructuring, privatization or deregulation. Sufficient regulatory incentives exist for an airport, in order to achieve and maintain the adequate level of safety and security at least in one layer - operational, thus compensating the failures in other layers. Economic incentives are sufficient motivator for social responsibility and environmental protection. The improvement of financial performance, operational efficiency and profitability reflect lower economic risks. The contribution of this paper is stressed by global interest in this subject.

Key words: *critical transportation infrastructures, integrated protection, risk analysis, public interest.*

1. INTRODUCTION

In this paper the author covers critical transportation infrastructures. They represent the group of interdependent and heterogeneous networks and systems, including industry,

institutions, distribution chains, personnel, equipment, physical facilities and communication (*cyber*) systems, which must be operational constantly to ensure the survival, the continuity of operations and the success of its mission. As the traffic is basic economic momentum, a special place in the consideration belongs to the main arteries of the transport sector - railways, ports and airports (DHS, 2003).

Having an insight into numerous references, there is evidence that until 1960s the notion dominated that public ownership is the best guarantor of critical transportation infrastructure protection. The turning point came in 1970s, observing that private sector bureaucracy is more efficient and that state ownership is obsolete for public monopolies.

Observing the contemporary socio-political, economic, financial, technical and technological phenomena, their great influence on critical transportation infrastructures is noted. The most important determinants of this sector development form the following frame, according to the previous research work of the author (Juzbašić, 2009):

- Transport market globalization and technological innovation through the process of association in alliances create pressure on the critical transportation infrastructures, requiring higher capacities and lower prices;
- The imperative of environmental compatibility, energy efficiency, safety and security measures, modern management techniques, inter-modality, interoperability, etc., all extend the range of requirements, which makes transportation industry quick to respond;
- Sustainable mobility guides the wellbeing of the future generations, increasing competition, the promotion of combined transport and creation of dynamic sector with market imperfections less influence, as well as the separation of growth in transport from economic growth;
- Deliberative democracy creates a policy framework for strategic decision making on critical transportation infrastructures, in order to protect the public interest during restructuring;
- Market opening and privatization of transport infrastructure monopolies is affected by the change in the ownership structure of these companies, by global profit-oriented shareholders and by the loss of the will of taxpayers to subsidize the costly transportation system;
- The relationships that cannot be established by the principles of competition must be regulated. Regulation and liberalization (aggregated as regulated deregulation) eliminate the negative effects of autonomous action of imperfect transport market.

Two imperatives for the convergence of policies of restructuring and the protection of critical transportation infrastructure have been determined (Juzbašić, 2009). These are the sustainable development, as a positive stimulus and the changing nature of global security threats that disrupt these resources.

During the research the author found out that restructuring is how states most commonly respond to the economic crisis, and it did not spare the transportation resources of public interest. In the focus of interest in the world is the revision of business risks protection (protected values) during their restructuring (including the change of ownership) as a necessary state action.

The author's interest is in the field of airports. Airports are caught in the middle of global changes and their business expanded beyond the previously well-defined national (bilat-

eral) borders and economies. From an economic point of view, they provide a vital link between production, distribution and consumption, enabling mobility of people, affecting the quality of life and economic growth. Thus, the need for their protection is a high priority for every nation.

Practice analysis revealed that late transition countries such as those in the Balkans suffer from various asymmetric threats (Štrbac, 2011). Faced with fiscal pressures and poor functioning of state enterprises, they coordinate public and private roles in transportation (Kessides, 2004). Accordingly, the author concluded that the expansion of an airport's traditional responsibilities is affected by changed market image, political support for the concept of sustainable development and greater responsibility for users.

Although essential to the function of societies, critical transportation infrastructures proved to be going through institutional restructuring (privatization, liberalization, and deregulation) (Buyck, 2007). 70.6% of the developing countries with low incomes and high potential are reforming their port sector, 68.4% of them airport sectors, and 55% the rail sector (Briceño-Garmendia et al., 2004). There is a broad agreement that the state should practice planning, restructuring and regulation, and leave management, investment and financing for the private sector.

There is a lot of evidence in literature showing that critical infrastructures protection is not a new phenomenon. At the end of the 19th century, infrastructures were considered to be very important for the military, economic and social development. The dominant protection policy stimulated their nationalization, and most of them had historically strong ties to the public sector. Wide public attention in the Western civilization at the end of the 1990s came with new forms of threat (*Y2K* cyber problem) together with the basic threats (*9/11* terrorist attack), so that continuous evolution of the corrective measures and the responses is also important (Buyck, 2007).

Protection issues actuality in Serbia coincides with profound economic, social, technological, and still present global economic crisis. In the available literature there is fragmented approach in the studies of this subject. In addition to traditional security and safety values, the restructuring of transportation capacities of public interest turned out to be a complex phenomenon in terms of financial and social responsibility and in terms of sustainable development **[6].** Thus emerged the concept of integrated protection and methodology for airports which is proposed below.

2. DIMENSIONS OF AIRPORT PROTECTION – INTEGRATED APPROACH

The resources gathered for this study testify to the importance of aviation as an industry. Its economic impact (direct, indirect, induced and catalytic) is estimated at $ 3,560 billion, equivalent to 8% of global GDP. Air transport is the largest global employer, generating the total of 32 million jobs worldwide. Annually, it accommodates more than 2.2 billion of passengers. The total value of goods transported by air is 35% of international trade (ATAG, 2008). A part of this success surely belongs to the airports.

It is proven that diversity and interdependence of global security issues (like environment, global, technological, cultural and political change, reduction of non-renewable resources, violent conflicts, etc.) relocate airport protection polemics outside of the traditional framework (Rinaldi et al., 2001). Modern society promotes the need for integrated risk management when restructuring critical transportation infrastructures (Chifu, 2011), as a

prerequisite for a successful business. The author suggests that dimensions of protection[1] should be considered in the context of risks for security, ecology, economy, safety and society. These infrastructures are analyzed to determine whether restructuring contributes to their better performance.

Closer authors' interest in the field of airports directs us to risk analysis of monopoly abuse, i.e. whether the behaviour of an airport after restructuring would lead to the reduction of system risks. Five system risks provide the image of how an airport operator is involved in the activities of public interest and how the implementation of these activities is ensured in the event of restructuring (Tables 1-10) (Juzbašić, 2013).

2.1. Security

It is proved that security requirements must be included in the conceptualization of infrastructures from the beginning, i.e. from the design. The activities to reduce system risks to airport security (Table 1) are given in three layers of action - operational, tactical and strategic. The analysis was carried out according to whether the existing legislation is sufficient to maintain an acceptable security level (Table 2). In a similar way we discuss all other system risks.

The security level is not directly affected by restructuring, privatization and deregulation of an airport operator. Sufficient regulatory incentives exist to maintain an adequate level of security at least in one of the layers observed. The primary importance of security is at the operational layer, where it compensates the failure in other two layers - tactical and strategic.

Table 1: Structure of incentives for an airport operator to adequate security level (Source: Juzbasic, 2013)

Activity	Strategic layer	Tactical layer	Operational layer
Inspection of all checked baggage and cargo	Framework regulations ICAO, IATA. ECAC detailed regulations. National regulations	National sector specific regulations	ECAC recommendations. National regulations
Inspection of all hand luggage, passengers and staff	Framework regulations ICAO. IATA improvement of passenger flows. ECAC detailed regulations. National regulations	National regulations. General staff regulations	National regulations
Protection of airport perimeter from unauthorized access	Framework regulations ICAO, IATA. Detailed regulations ECAC. National sector specific regulations	National regulations. General staff regulations	ECAC recommendations. National regulations

1 Many different terms in references are used with the same meaning: sustainability dimensions, business dimensions or protected values, system risks, risk factors or opportunities, attributes, aspects, criteria, etc. For more see (Juzbašić, 2013).

Public peace and order inside structures and outdoors	ECAC framework regulations. National regulations	General regulations. National sector specific regulations	General regulations. National regulations
Emergency response	ECAC, ICAO framework regulation. National sector specific regulations	ECAC. National sector specific regulations	National regulations

Table 2: Analysis of incentives for an airport operator to adequate security level (Source: Juzbasic, 2013)

Activity	Strategic layer	Tactical layer	Operational layer
Inspection of all checked baggage and cargo	OK. Investing in security only with the benefit of greater capacity.	OK. Fee for security check point area increase at the expense of commercial content.	OK. State authorities shall decide on operational constraints. Need detailed regulations for cargo checks.
Inspection of all hand luggage, passengers and staff	OK with simplification of processes and technologies.	OK with additional regulation of working condition of personnel.	OK with more detailed regulation of hand luggage search of passengers.
Protection of airport perimeter from unauthorized access	OK	OK. Need for defying jurisdiction of public peace and order entities.	OK. Need for defying jurisdiction of public peace and order entities.
Public peace and order inside structures and outdoors	Insufficient incentives to invest. No guarantee of interorganizational collaboration.	Insufficient incentives to invest. No guarantee of interorganizational collaboration.	Insufficient incentives to invest. No guarantee of interorganizational collaboration.
Emergency response	OK. Incentive- fear of bad publicity. Need for contingency planning and global harmonization	No incentives for improvement of practices and procedures for high level of security threats	No incentives for improvement of practices and procedures for high level of security threats

2.2. Safety

The practice showed that when using the infrastructure it is necessary to continuously identify hazards and manage the risks of injury to persons or damage to property. *Ex-post* introduction of safety in any assessment is not economically viable nor socially acceptable. The analysis in this paper is focused on answering the questions what incentives exist for an adequate level of safety of an airport operator (Table 3), and whether they are sufficient to guarantee the safe conduct of activities by the restructured airport operator (Table 4).

The level of safety at an airport turned out not to be directly affected by the restructuring of the full scale. Sufficient regulatory incentives exist for an airport operator, in order to achieve and maintain an adequate level of safety in the operating layer.

Table 3: Structure of incentives for an airport operator to adequate safety level (Source: Juzbasic, 2013)

Activity	**Strategic layer**	**Tactical layer**	**Operational layer**
Control of wildlife presence in manoeuvring area	ICAO regulations ICAO decisions on airport accountability	(Inter)national regulations	Pressure on effective transport operations and optimal use of runway
Construction / maintenance of manoeuvring area	(Inter)national regulations. Monitoring and surveillance	(Inter)national regulations	Operational decisions of air traffic control on optimal capacity
Aircraft ground handling	(Inter)national regulations	(Inter)national regulations	Control, monitoring and accountability
Emergency response	(Inter)national regulations. Responsibility and involvement of third parties	(Inter)national regulations. Responsibility and involvement of third parties	Monitoring and surveillance of third parties
Safety management system	(Inter)national regulations. Monitoring and surveillance	(Inter)national regulations. Monitoring and surveillance	Monitoring and surveillance

Table 4: Analysis of incentives for an airport operator to adequate safety level (Source: Juzbasic, 2013)

Activity	**Strategic layer**	**Tactical layer**	**Operational layer**
Control of wildlife presence in manoeuvring area	OK	OK	OK
Construction / maintenance of manoeuvring area	Investing in safety only with the benefits of greater capacity	No direct incentives for big preventive maintenance work	*OK. Air traffic control decides on operational runway capacity*

Aircraft ground handling	*OK*	Insufficient incentives for ground handlers	*OK*
Emergency response	*OK*	*OK*	*OK*
Safety management system	*OK. No guarantee for interorganizational cooperation*	*OK. No guarantee for interorganizational cooperation*	*OK. No guarantee for interorganizational cooperation*

2.3. Sustainable development

It is found that the environment is a factor equal to the economic and social considerations, as are the side effects of the environment equal to economic and social factors (about 7% of GDP cost each of them) (Juzbašić, 2009). In the same way as previously, we selected regulatory incentives to maintain an adequate level of environmental protection (Table 5) and analyzed these impacts (Table 6).

Table 5: Structure of incentives for an airport operator to adequate environment level (Source: Juzbasic, 2013)

Activity	Strategic layer	Tactical layer	Operational layer
Noise and vibrations in the airport vicinity	ICAO regulations	International and national regulations	National regulations. Local procedures
Emissions and pollution of air, water and soil	ICAO strategic framework. International regulations	National regulations	ICAO regulations. National regulations. Local procedures
Land use	General and detailed urban planning in airport vicinity	Economic incentives	International regulations (EU) for capacity use (airport slots)
The use of water and energy	Economic incentives	Marketing incentives	General national regulations
Waste management	Economic incentives	Marketing incentives	General national regulations. Sector specific regulations

The analysis revealed that environmental protection is not directly affected by the restructuring of the airport operator to the full extent. Economic incentives are sufficient motivator to socially responsible behaviour. In some areas there is a need for regulatory incentives for an adequate level of environmental awareness in the operating layer.

Table 6: Analysis of incentives for an airport operator to adequate environment level (Source: Juzbasic, 2013)

Activity	Strategic layer	Tactical layer	Operational layer
Noise and vibrations in the airport vicinity	OK	OK. Additional fees for technological development	OK. Operational restrictions as direct incentive
Emissions and pollution of air, water and soil	OK. Global pressure without specific sector regulations	OK. Additional fees as direct incentives for technological innovations	OK. Additional fees for airlines according to aircraft performance
Land use	OK. Economic incentives for adjustment of airport content and function	OK. Control measures and revision of urban plans	OK. Large effort in communication with local community
The use of water and energy	OK. Economic incentives for greater savings	OK. Need for more detailed regulations	OK
Waste management	OK. Economic incentives for waste disposal and recycling capacities	OK. Economic motivation and good publicity are enough incentive	OK. Economic motivation and good publicity are enough incentive

2.4. Economics

Aviation in total has made a cumulative loss since its inception (subsidies for aircraft development and airport construction). Numerous factors affect the economic performance of the airport. The activities selected to determine the effects of restructuring on this system risk are given in Table 7. The analysis is summarized in Table 8, analogous to the previous aspects. The analysis of economic risks to airport operators due to restructuring confirms the improvement of financial performances.

Table 7: Structure of incentives for an airport operator to adequate economical level (Source: Juzbasic, 2013)

Activity	Strategic layer	Tactical layer	Operational layer
Labour productivity	IATA. General national regulations	Internal regulations	Internal regulations
Cost effectiveness	Internal regulations	Internal regulations	Internal regulations
Operational profit	General national regulations	General national regulations	General national regulations
Price levels	Sector specific regulations	Sector specific regulations	Sector specific regulations
Risk on investments	No standardized indicators. General national regulations	No standardized indicators. General national regulations	No standardized indicators. General national regulations

Table 8: Analysis of incentives for an airport operator to adequate economical level (Source: Juzbasic, 2013)

Activity	Strategic layer	Tactical layer	Operational layer
Labour productivity	OK	OK	OK
Cost effectiveness	OK	OK	Maximizing the use of resources has been balanced with general regulations
Operational profit	OK	OK	Pressure on more profitable business-the matter of business policy
Price levels	OK if sector specific regulations prohibit extra profits	OK	OK
Risk on investments	OK	OK	OK

2.5. Society

Having in mind a social aspect, an airport operator effects greatly on life forms in its vicinity (sublimated in Table 9 as system risks to the social aspect, and analyzed in Table 10). We determined that the degree of societal interest protection will not be less after airport operator full restructuring, if there are economic incentives provided and socially responsible behaviour promoted, particularly in the field of employment and of public transport to isolated areas.

Table 9: Structure of incentives for an airport operator to adequate social level (Source: Juzbasic, 2013)

Activity	Strategic layer	Tactical layer	Operational layer
Employment	International agreements and labour regulations. National regulations	National regulations on employment and occupational health and safety	Internal regulations
Links to isolated regions	National regulations on regional development and social protection	Local regulations	Local regulations
Possibilities to travel	General sector regulations	---	Local and internal regulations

Service quality	IATA. National regulations on consumer protection. Specific regulations	International standards. Local and internal regulations	Local and internal regulations
Relations to local community	National regulations. Local regulations	Local and internal regulations	Local and internal regulations

Table 10: Analysis of incentives for an airport operator to adequate social level (Source: Juzbasic, 2013)

Activity	Strategic layer	Tactical layer	Operational layer
Employment	OK if bad effects to employment neutralized	OK	OK
Links to isolated regions	OK with subventions for non-commercial travel market segments	OK with subventions for the provision of goods and export facilitation	OK with local employment
Possibilities to travel	OK. Direct economic interest for opening new routes	OK. Enough incentives for lower travel costs and greater user figures	OK with subventions for new routes
Service quality	OK	OK	OK
Relations to local community	OK	OK	OK

It is estimated that more than 1,100 of restructuring was carried out in the transport sector worldwide for the past 20 years, with the worth of about $ 360 billion(OECD, 2002). The analysis showed that the factors considered within the critical transportation infrastructures are undoubtedly valued more after restructuring with the ownership change. Viewed through the complete prism, the restructuring contributes to better business results of these monopolies. There are further expectations to standardize the issues of citizen' security, critical infrastructures, products and services (Keković et al., 2011).

3. CONCLUSION

The restructuring together with privatization stems from the ideological belief in the superiority of market discipline. The analyses have proven this process must not be planned without the protection of public interest, which is difficult due to contemporary social and business features (terrorism, global economic crisis, the growing level of energy dependence, etc.). Planning a sustainable transport system should take into account the wider impacts.

After examining the numerous sources, it is revealed that the protection of critical transportation infrastructure has not been addressed in comprehensive, integrated and complementary way, so this paper systematized the protection aspects. Heterogeneous and

divergent dimensions of this issue are analyzed on the example of the airport as a critical transportation infrastructure.

It is determined that integrated observation becomes a necessity in order to achieve the sustainable success of the organization. No recommended way of management systems integration exists as a widely accepted methodology and an international norm. With this paper we try to give an answer how to consider integrally the management system requirements of critical transportation infrastructures and we found out that the protection aspects of their business risks, i.e. the protected values of a society consist of environmental, economic, security, safety and social factors.

Practice has shown that these aspects of observation are certainly more valued after restructuring. The safety and security performances are better, business efficiency and economy are at a higher level and care about a user's wishes and interests are in entrepreneur's focus. The complexity and importance of this problem require a multidisciplinary approach.

This paper contributes on theoretical and practical level through the inclusion of sustainability considerations in broad (comprehensive) manner in methodological framework for the protection of critical transportation infrastructures. The proposed integrated framework for system risk assessment develops the criteria and protection analysis. From the above presented we can conclude that the system risks of given activities in the existing regulatory system are secured at all layers with the appropriate structure of incentives.

To conclude, the sufficient regulatory incentives exist for an airport, in order to achieve and maintain the adequate level of safety and security at least in one layer - operational, which compensates failures in other layers. The economic incentives are sufficient motivator for social responsibility and environmental protection. Improved financial performance, operational efficiency and profitability reflect lower economic risks.

4. REFERENCES

1. Air Transport Action Group. (2008). *Air Transport Drives Economic and Social Progress: The Economic and Social Benefits of Air Transport 2008*. Genève: ATAG.
2. Briceño-Garmendia, C., Estache, A. & Shafik, N. (2004). *Infrastructure Services in Developing Countries: Access, Quality, Costs and Policy Reform*, Working Paper WPS 3468. Washington, D.C.: World Bank Policy Research.
3. Buyck, C.A. (2007). Public Monopolies, Private Profits. *Air Transport World*, 44, 6, 32-37.
4. Chifu, I. (2011). Influence of Religious Extremism on the Stability and Security of Democratic Societies. У S. Butiri, D. Mihailovic (Eds.), *Evolving Asymemetric Threats in the Balkan*, 85, 37-53. Amsterdam: IOS Press.
5. Juzbašić, A. (2009). *Privatization of transportation capacities of public interest in accordance to regulated deregulation policy*. Master thesis. Belgrade: Faculty of traffic and transportation engineering, University of Belgrade.
6. Juzbašić, A. (2013). *Crisis management and integrated policy to protect public interest*. Doctoral dissertation. Belgrade: Faculty of security studies, University of Belgrade.
7. Keković, Z., Savić, S., Komazec, N., Milošević, M. & Jovanović, D. (2011). *Risk assessment in protection of humans, property and business*. Belgrade: Centre for risk analysis and crisis management.
8. Kessides, I.N. (2004). *Reforming Infrastructure: Privatization, Regulation and Competition*. A World Bank Policy Research Report, Washington D.C.: World Bank/ Oxford University Press.
9. Organization for Economic Cooperation and Development. (2002). *Impact of Transport Infrastructure Investment on Regional Development*, Paris: OECD. Lasr opened May 2013 on http://www.internationaltransportforum.org/pub/pdf/02RTRinvestE.pdf.
10. Rinaldi, S., Peerenboom, J. & Kelly, T. (2001). Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies, *IEEE Control Systems Magazine*, 21, 6, 11-25.
11. Štrbac, K. (2011). General Overview of the Asymmetric Threats in the Balkans. У S. Butiri, D. Mihailovic (Eds.) *Evolving Asymmetric Threats in the Balkan*. 85, 3-10, Amsterdam: IOS Press.
12. U.S. Homeland Security. (2003). *Critical Infrastructure Identification, Prioritization and Protection*, Presidential Directive HSPD-7. Washington, D.C.: DHS. Last opened, May 2013 on http://www.dhs.gov/homeland-security-presidential-directive-7.

UDC 726.9:75.041.5
ID 176374796

Ljubodrag P. Ristić
Serbian Academy of Sciences and Arts, Institute for Balkan Studies, Belgrade
risticljp@yahoo.com

Bojana Miljković-Katić
Institute of History, Belgrade
bojana.miljkovic.katic@iib.ac.rs

BORROWING FOR CONSTRUCTION OF RAILWAYS AND PROTECTION OF CRITICAL INFRASTRUCTURES IN THE KINGDOM OF SERBIA (1881–1895)

Abstract: By taking loans for construction of railways, as well as for budget deficit rehabilitation, Serbian governments were putting in pledge fiscal revenues in order to be able to service those loans, in addition to setting up the special revenue funds for collection of finances earmarked to repayment of due annuities. These funds were managed by two representatives – a Serbian one and a creditor's one. In addition to borrowings for construction of railways (1881, 1885, and 1886) that were contracted, creditors were also given management of railways, on the grounds of the fact that exploitation revenues were among the loan warranties. From year to year, more and more revenues were put in pledge, and by 1888 foreign banks extended their supervision to all of the most important revenues of the state of Serbia. In order to get its own financial control retrieved, as well as to get the strategically important transport route protected, the state was buying out, starting from 1888, all pawned revenues and railway exploitation rights. However, at the same time it was making additional borrowings. By establishing the *Directorate of Serbian Railways* the state took both railways management and control of the future railway lines over, and by establishing the *Independent Monopoly Administration* it managed to retrieve a part of control of public finances and to reduce the foreign creditors` impact.

Key words: *Serbia, Austro-Hungary, 19th century, state railways, foreign loans, state revenues, monopolies, nationalization, Independent Monopoly Administration*

1. INTRODUCTION

According to some theoretical approaches to research of both critical infrastructures and protection of them, in addition to the classic infrastructures such as land, water or air services, these structures comprise state public finances as well, i. e. banking system, securities trade and financial investments.[1] In that sense, the historical approach to construction and management of the railways in the Kingdom of Serbia in the last two decades of 19th century were doubly connected to the analysis of the role of critical infrastructures because problems of protection of the new infrastructure, as well as of the state financial system, were closely tied to construction and exploitation of the railways themselves. These problems were generated by the conflict of strategic interests of many countries on one

1 Communication SOM (2004) 702. http://www.infotrend.hr/clanak/2012/11/objektivne-opasnosti-%E2%80%93-subjektivna-mjerila,75,972.html

hand, and by Serbian international obligations in circumstances of bad state finances and its remorselessness in international banking and investment market on the other.

Austro-Hungarian interests in construction of the first railways in Serbia were obvious, since it was to get the Ottoman railways connected to the Austro-Hungarian ones. In the aftermath of the Russian-Turkish War (1877/78) the Monarchy tried to get its primacy in relation to Russia in its break trough to the East, which greatly depended - in peacetime circumstances – on the question whether it was to bring the construction of Balkan railways under its sphere of influence. (С. Јовановић 1990, I, 396; A. Mitrović 2004, 26–27) Germany had similar interests in getting routes to the East shorter. Unlike the Great Britain, these two countries exported their capital primarily to European countries, to so-called European periphery, and they were interested in mediation in funding and construction of all the Balkan railways. They and their banks and financial groups became a dominant factor not only in domain of funding the construction of railways, but in investments in the Kingdom of Serbia state loans in the course of last decades of 19th century. French capital, however, was not able to access this market until late 19th century. (А. Митровић 1985, 167–197; А. Митровић 1997, 9–24)[2]

In accordance to provisions of the contract made at the Berlin Congress in July 1878, Serbia obtained its independence and territorial extension (§§ XXXIV–XLII). However, among its obligations taken at the time, it accepted, in accordance to the Article XXXVIII, that „la principauté de Serbie est substituée, pour sa part, aux engagements que la Sublime Porte a contractés, tant envers l'Autriche-Hongrie qu'envers la Compagnie pour l'exploatation des chemins de fer de la Turquie d'Europe par rapport à l'achevèment et au raccordement ainsi qu'à l'exploitation des lignes ferrées à construire sur le territoire novellement acquis par la principauté". Right after the Treaty of Berlin had been signed it was meant to get, by additional separate contracts between Austro-Hungary, Turkey, Bulgaria and Serbia, regulated the future realization of the accepted obligations (*Traité de Berlin*, 1888, 666 (No 361); Ф. Мартенс 1909, 121; Ј. Ристић 1898, 232–236, 244–247, 262–263; Ђ. Мрђеновић 1974, 77–80)[3]

Upon long lasting and tough negotiations conducted on the basis of provisions of both the Ristić-Andrássi Convention (July 8, 1878) and the Treaty of Berlin (July 13, 1878), the *Convention on construction of the two-arm Belgrade-Niš railways, as well as on connecting it to Austro-Hungarian railway line* was made on April 9, 1880. The agreement period was to be three years long, provided that the obligation on the three-year term of construction of the Niš – Pirot – Bulgarian frontier railway line depended on signing a contract between Serbia and Bulgaria.

Notwithstanding that Serbia and Montenegro were the only European countries of the time without any railway lines, there were discussions on whether the state needed a railway line at all. Political elite was aware of the importance of that technical accomplishment (M. Marković, 1972, 75). Back in April 1880 the *Convention* had already initiated fierce discussions in the National Assembly. While the Government deputies were emphasizing international, economic and political importance of construction of railways, the opposition Radicals criticized the document arguing that there would not be any of the promised ben-

2 In detail, see: А. Митровић, Стране банке у Србији 1878–*1914*.

3 In detail, see: M. Samardžić, *Roads to Europe,* 2010, 53–94.

efits realized, on the grounds that the provisions were superimposed, the newly acquired independence was jeopardized and the railway connection to Thessalonica was missing, so the new traffic service "was not to bear a nature of a World-class railway line". That, the Radicals argued, would mean "economic bankruptcy and political enslavement" (Србија 1878 1978, 524–530, 556–575; Зборник 1880, 298–321; M. Marković 1972, 67–80). That was the reason why the Radicals unanimously pronounced against the construction of the railways, picturing it as the peril to come, equal to the Kosovo defeat. The very essence of the opposition lied in the fear of foreign control over strategic property as well as in the fear of foreign capital. The railway line was, to both the Progressionists and the Liberals, a fatedly impulse, but in domains of modernization of society and market development only. (Ж. Живановић II, 1924, 79–96; M. Samardžić 2010, 94–106, 131–132, 138–140; L. Perović 2010, 388) Financially exhausted by two previous wars as it was, Serbia nevertheless was not going to avoid the construction of the railways but it only tried to postpone it. However, under rigorous pressure made by Austro-Hungary, it had to accept the beginning of construction on June 15, 1880, to be completed on June 15, 1883. (Историја српског народа 1983, 18; В. Вучковић 1956, 49–50)

As the political objective of the Progressionist governments (from late 1880 to late 1887) was modernization of the state (reorganization of both state administration and the army, regulation of finances, facilitation of education, political rights and economic conditions), so much money was necessary to realize it, and as the state Budget did not hold enough money available, they abandoned a realistic budgeting policy. A fictitious budgeting meant that state revenues without a real foundation were calculated as very high ones. (Б. Мијатовић 2006, 40, 70; М. Недељковић 1909, 84–85) Increased Government expenditure in the course of eighties used to be covered by growing budget deficits (about 375,000 Dinars in 1880, and as much as 13.2 million in 1886) being hidden as booked into the Extraordinary Budget, which was just named as such, or being presented as credit deposits to be – immediately upon passing the budget – over and over treated as so-called *floating debts*. Funding of the construction of railways and settlement of state finances were to be solved in bridge , so therefore the Progressionist governments decided to get the two key problems solved by new foreign borrowings. In six years only seven big loans were taken, out of which three were used for the construction of railways, and the remaining ones for settlement of public finances, reform of the army and preparations for the 1885 war. However, the budget deficit problem was not solved, because money obtained had not been spent for specific purposes.

2. RAILWAYS CONSTRUCTION LOANS AND LOSING FISCAL REVENUES CONTROL

The railways construction loan was the very first foreign loan Serbia contracted below par. It was negotiated on February 3, 1881 with the General Union (*La Société de l`Union Générale*) „at the time among the most respected financial institutions in France", without a public tender, in other words through both backlog-stage activities and secret mediation of Austrian diplomacy. The Agreement comprised the following three contracts: *The Contract on the Railways Construction Loan, The Contract on Construction of Railways* and *The Contract on Utilization of Railways*. According to these, *The General Union* (*l`Union Générale*) was to grant Serbian Government a 100 million Fr. Francs credit, to get a contractor engaged, to organize both construction of the railway line at the price of 198,000

Dinars per kilometer and its exploitation in the course of the forthcoming 25 year period with a guaranteed revenue of 7,800 Dinars per kilometer, in addition to an obligation of the Government to compensate any possible not-supplied part of it. That way, instead of being a concessionaire that takes a job over, either by proper money or out of a loan, the *General Union* was engaged in the railway construction on money taken by Serbian state in the form of a credit taken from the *General Union* itself, in addition to exploitation of it which was also relinquished to the *Union*. (Зборник 1882, 201–203; M. Samardžić 2010, 121–129; В. Вучковић 1956, 50–51; D. Gnjatović 1991, 27)

In addition to the above, the Serbian Government committed itself to huge warranties. The Government secured repayment of the loan by some of the most important state revenues: net earnings of both the railways and customs and, in the case they were insufficiently high for payment of annuities, a part of citizens' toll. It agreed to establish, within the Ministry of Finance, the special *Railways Loan Fund*, doubly controlled by a state official and by *The General Union* representative. The *Railway Exploitation Administration* ought to place net railways and customs revenues collected at railway stations to the *Fund*, and the state ought to pay, on monthly basis, the remaining revenues the loan repayment was warranted by. The *Railways Loan Fund* deposited, in three-month periods, the annuity to the *General Union*, Paris, France. Although the state of Serbia became the owner of the mortgaged railways, upon the startup of it in 1884 the only rights it realized in domain of its exploitation were rights on pricing and making time-tables. (М. Недељковић 1909, 31–33, 36–37, 42–43)

Since the *General Union* was a speculative enterprise, the competitors provoked its bankruptcy. In order to prevent depreciation of its shares (in 1879 a share was 1,750 Fr. Francs worth, and in 1881 as much as 3,400) the *Union* had to repurchase them. The *General Union* collapse was of a political background in France, and it was able to endamage Serbia both in economic (abruption of the railways construction) and in political sense (fall of the Progressionist Government). (М. Недељковић 1909, 28–31)[4] In order to avoid financial loss caused by the *General Union* bankruptcy, Serbian minister of finance Mr. Čedomilj Mijatović managed, with a help of Austro-Hungarian diplomacy, to negotiate with the *National Escont Comptoar* (*Comptoir National d`Escompte*) in Paris, France, takeover of all the *General Union* obligations considerate towards Serbia, under the same credit conditions as those that had been negotiated in 1881, and therewith to get the price of the railway construction decreased by about 33,000 Fr. Francs per kilometer. Therefore, Serbia financially connected itself firmly to the *National Escont Comptoar* and through it to the Vienna *Lenderbank* making them its permanent creditors.

The Escont Comptoar established, for the purpose of railways construction, *The Association for Construction and Exploitation of Serbian State Railways*. It was assigned, under the same conditions, construction of the Niš – Pirot railway line, for the purpose of which a new loan was contracted with the same creditor, on March 17, 1887, in the same manner as the former one. (М. Недељковић 1909, 43, 68, 73–75; Историја српског народа 1983, 18) That was the way Serbia avoided financial loss and cessation of the construction of railways. At the same time, a model of ensuring of foreign loans repayment was established the way that resulted, in time, in almost total control executed by foreign banks over the

4 There are indicies that the House of Rotshild also took a part in the *General Union* collapse. (Ч. Мијатовић – Председнику, 25. јануар 1882, Париз, АС, МИД – ПО, 1882, Ф-I, Г/9; В. Вучковић 1956, 63–71).

major part of Serbian state revenues.[5] (Мемоари В. Ј. Петровића 2009, 29) Another loan was contracted with *The Escont Comptoar*, on October 15, 1885, under similar conditions as former ones. (D. Gnjatović 1991, 32–33) That loan was used for the purpose of buying up the temporary railway line Velika Plana – Smederevo, constructed to supply the main track with necessary materials, as well as to help with construction of the Lapovo – Kragujevac main railway line. As bought up, the Velika Plana – Smederevo railway line was given to the *Association for Construction and Exploitation of Serbian State Railways* to exploit it, together with both guaranteed 240,000 Dinars gross revenues and a liability of the *Association* to hand any possible surplus over to the state Budget. *Marko O. Marković and Comp*. were entrusted of construction of the Lapovo – Kragujevac railway line at the price four times lower than the price contracted with the *Escont Comptoar* for construction of the Beograd – Vranje railway line. (П. Миленковић 1936, 56; М. Недељковић 1909, 88–89, 92; Историја српског народа 1983, 26)

3. RESTITUTION OF STATE CONTROL OF FISCAL REVENUES

The fact that the total borrowings, until 1910, on 596 million Dinars par value, only yielded 444 million (74%) to the state, and that it had to pay 1.4 billion Dinars as repayment, shows how expensive were the loans Serbian Government contracted. (H. Sundhaussen 1989, 458-459) Putting ever growing share of the budget revenues as security of foreign loans repayment, the Government of Serbia was loosing more and more control in domain of public finances, since almost all fiscal revenues were mortgaged until 1888.

Mr. Mihailo Vujić, a Radical and the Minister of Finance, prior to the Mr. Jovan Ristić Coalition Government (1887) and afterwards to the Radical governments, determined that the state foreign loan annuities engaged around one third of the planned budget expenditure in the fiscal 1886/7 year, as well as, despite inaccurate recording of debt repayments, that the country was 254.12 million Dinars indebted on the basis of funded debts, and on the basis of provisory debts 32.06 million. Vujić pointed at provisory debts as "the most expensive and the most destructive form of national debts". Repayment of these debts he considered the most important to both real budgeting and recovery of public finances. (M. Недељковић 1909, 111–121, 126) For the purpose of repayment of that loan a special fund was established as well, making therefore direct tax the only remaining non mortgaged one. (D. Gnjatović 1991, 53; М. Недељковић 1909, 129; Б. Мијатовић 2006, 61)

Under pressure of the necessity to raise a loan to be used for the war funding purposes, the Progressionist Government agreed to disadvantageous conditions under which the *To-*

5 Financial system was additionaly jeopardized by application of the same way of warranting of repayments of foreign loans taken for financing of both beginning of construction of railways and repayment of a part of the Serbian Public Loan (1881) taken for armament of the Army and repayment of landowners' feudal rights in *New Areas* (1882), for settlement of financial issues in the country itself (1884-1886), for reform of the Army and funding of defence (1885). Repayments of these loans resulted in mortgaging more and more state public revenues, while repayment of annuities was warranted by establishment of special funds dedicated to each of those loans. These funds were funded the same way the *Railway Loan Fund* was. At the same time, two newly-established monopolies were mortgaged – salt and tobacco monopolies, and monopoly companies were relinquished to creditors, which was the reason why the state was deprived from control of booking of monopoly revenues. The last one of these funds – the *Five Percent Mortgage Loan Fund* was even more independent from the Ministry of Finance than the former ones were, since it was entitled to collect interest payments directly from the *Fund Administration* debtors – in cases of deferred annuity payments. (Зборник 1882, 162–169; М. Недељковић 1909, 96–98, 106; D. Gnjatović 1991, 28, 31, 42–44, 48–49; Историја српског народа 1984, 26; Б. Мијатовић 2006, 64–67)

bacco Monopoly Lease Society took the Serbian Monopoly over. In 1887, when the *Society* presented the alleged 1.57 million Dinars loss that the state was due to compensate out of its budget revenues, while Minister Vujić was going to reintroduce the racking lease tax on imported tobacco, contract was cancelled. (Б. Мијатовић 2006, 68–72; М. Недељковић 1909, 131) The Government took a loan from the Vienna *Banking Society (Bankverein)* to buy the Monopoly up, mortgaging the Tobacco Monopoly revenues remained upon settlement of the *Tobacco Rent* annuities. The financial transaction proved to be partly worthwhile because the state treasury used to gain profits of the Tobacco Monopoly after annuities were settled. In the course of years, profits grew from 2.2 million (1889) to 5.5 million (1893) and stabilized at that level until 1898. (D. Gnjatović 1991, 56; М. Недељковић 1909, 134; Б. Мијатовић 2006, 72)

Upon the occasion of *Escont Comptoar* bankruptcy (1889) Serbian Minister of Finance timely made an agreement concerning Serbian loan obligations by taking the advantage of the opportunity to get exploitation of railways repurchased. The state was interested in the repurchase because it had to compensate growing deficits of the *Association for Exploitation of Serbian State Railways* every year. It was not successful in covering the warranted profits by its revenues made at any of its own railway lines, even after Serbian railways were connected to both Bulgarian and Ottoman ones. In 1884, at the time the railways were put in service, deficit amounted around 78,000, and in 1888 as much as 860,000 Dinars. All railway lines managed by the *Association* recorded cumulative deficit amounting 2.5 million Dinars until January 1, 1889. (Мемоари В. Петровића 2009, 127, 129, 146; М. Недељковић 1909, 137–138) At the same time, the only railway line exploited by the state (Kragujevac – Lapovo) was making 45,000 Dinars profit. In the course of London negotiations with the *Association for Exploitation of Serbian State Railways* ministers of civil engineering and finance, with mediation of the French Government, brought to pass buy up of the rolling stock and recompensation of 10 million Dinars lost profit. From the French banking group *Banque Hoskier et Cie* and from the *Privileged National Bank of the Kingdom of Serbia* the 20 million loan was secured for the purposes of railway repayment and repayment of provisional debts. (Зборник 1891, 203–244, 593–612; М. Недељковић 1909, 139–140) However, by buying the railway exploitation up the state control of revenues given as security was not increased, because gross revenues the railways made were handed over, through the *Railways Loan Fund,* directly to the creditor. At the same time, the Fund used to collect turnover tax revenues, stamp duty and public house tax and to send them to the creditor on monthly basis. Not before the end of a year a possible surplus used to be handed over to the Treasury. (М. Недељковић, 1909, 140)

Upon taking the railways exploitation over, Serbia established the *Directorate of Serbian State Railways* to manage the railways and was more interested in improving exploitation of the railways, since profits were not guaranteed. (Зборник 1893, 147–197; 1899, 108–109; 1902, 659–661; 1903, 445–453) Therefore, no wonder that the railways revenues were growing irrespective of Serbian administrative services that were ill-conditioned to manage the railways. By establishment of the *Directorate* the railways management standard was established as well. All concessionaries were due to apply that standard.[6] By taking up the exploitation of railways the state took up control of technical and all the other conditions of exploitation at all the other lines as well, in ac-

6 In the course of 1897 and 1898 only, revenues grew from 9,435.90 Dinars to 100,000.00 Dinars. (АС, МФ, Управа државних дугова, кут. I, 1898, unordered records)

cordance to the principle established on the occasion of construction of the Lapovo – Kragujevac line. (Зборник 1884, 360–361)

In 1889, Minister Vujić inspected operations of the *Salt Monopoly Lease Society* as well, and found it operating unlawfully in spite of enormously high gains it made in the business, having an obvious intention to endamage the state of Serbia, and therefore the contract was cancelled. (D. Gnjatović 1991, 64, Note 111) It ought to be paid to the *Anglo-Austrian Bank*, on behalf of both buying up of inventories and stored salt and recovery of damages, around six million Dinars. Money was provided by the credit contracted in 1890 with the banking group *Hoskier,* and repaiments were secured by the Salt Monopoly revenues. (M. Недељковић 1909, 142)

Since state finances could not be settled, and as collection of taxes, supertaxes and basic non mortgaged state revenues was extremely inefficient, they were regularly to low and, while floating debts were growing, Serbia was slowly gliding into bankruptcy. There were attempts to avoid it by negotiating few loans, from 1890 to 1895, for the purposes of budget deficit rehabilitation and making regular payments of foreign loan annuities, but debts were still growing. (M. Недељковић 1909, 147–153) A solution was found in the form of a huge 355.5 million Dinars conversion loan, contracted in Karlsbad, Germany, with the *Ottoman Bank* from Paris, France, the Vienna *Trade Society* and *Lenderbank* in 1895, by which ten loans contracted before were converted into a single one, at 4% interest rate. Actually, the remaining banks-creditors were therefore made to reduce interests on their loans. The loan was to be used to get provisional debts (around 40.2 million Dinars) settled and, by means of extension of term of payment (to 72 years), to disburden the budget by making annuities lower. (Зборник 1899, 409–417; D. Gnjatović, 1991, 70–71, 73; M. Недељковић 1909, 146, 178) Annuity amounts were lowered (from 18.1 to 13.2 million), but all revenues put in pledge before were pledged again, in addition to revenues of the new Gas Monopoly (established in 1893). The *Independent Monopoly Administration*, as an independent creditors' state revenues administration, was established to service the loan. (Зборник 1899, 458–459; D. Gnjatović, 1991, 70–71)

By establishing the *Independent Monopoly Administration* Serbia partly regained control of public finances. Namely, its Board comprised six members, out of which two were creditor's representatives. All that resulted in decrease of influence the creditors had in that institution in relation to special funds of specific loans. In addition to that, in the case of even distribution of votes in the Board, the President's vote was decisive, since he was at the same time a Governor of the National Bank, therefore additionally ensuring interests of the state of Serbia. Control of public finances was partly regained by the ruling pursuant to which revenues were to be collected on monthly basis, with every surplus, left after one twelfth of annuities was settled, paid to the State Treasury. However, the *Independent Monopoly Administration* was an administration that managed, by acting independently of the Ministry of Finance, not only revenues by which a loan was guaranteed, but the remaining state revenues and securities as well. That restricted, once more, the state control of the own most reliable revenues. Although establishment of the *Independent Monopoly Administration* was a stroke right into financial independence of Serbia, it still lowered the impact foreign creditors representatives made in domain of practical disposition of fiscal revenues. Namely, it used to happen in the past that a creditor's representative to special funds by which loans were guaranteed agreed to make a certain part of a fund revenues temporary available to the Ministry of Finance. Since there was not enough money to get

these borrowings paid back, they were converted into provisional debts to these bank-creditors and afterwards into permanent debts at 60–65% flotation rate. (М. Недељковић 1909, 185) The practice of the kind was not possible anymore because revenues put in pledge were taken out of the state administration hands immediately after collected. The *Independent Monopoly Administration* was matchlessly more clear, accurate and efficient as compared to earlier separate funds, since regularly collected monopolies secured surpluses of not mortgaged revenues.[7]

Even with so restricted rights of its own revenues, the Serbian state had extremely high degree of control of public finances, since it made majority of the *Independent Monopoly Administration* Board. The *Administration* members (plus two representatives of the creditor) were appointed by the King. That provided Serbia with some kind of influence when it came to election of officials. By its exception from the Ministry of Finance competence, it was made protected from the political fight without quarter that kept on devastating all the other institutions in the course of second half of 19th century. That made possible for that institution of strategic importance to be managed in accordance to the best interests of the state instead of the best interests of political parties. The *Administration* conscientiously collected the fiduciary revenues and made annuity payments regularly, thus making Serbia relieved of problems in the domain of irregular repayment of foreign debts. That improved its credit rating in the period when indebtedness rate was growing. Fears of enormous foreign intervening able to undermine its financial independence and, by some more radical positions, even Serbian sovereignty itself, did not materialize. (Д. Протић 1908; A. Mitrović 2004, 27–28; H. Sundhaussen, 1989, 459)

Translated by: Mirjana Nikolajević

7 АС, МФ, Управа државних дугова, кут. II, 1897; unordered records.

SOURCES

4.1 Unpublished documents:

1. Архив Србије, Министарство иностраних дела – Политичко одељење, 1882.
2. Архив Србије, Министарство финансија, Управа државних дугова 1887, 1898.

4.2 Published documents and papers:

1. Gnjatović, Dragana (1991), *Stari državni dugovi. Prilog ekonomskoj i političkoj istoriji Srbije i Jugoslavije 1862–1941*, Beograd.
2. Историја српског народа (1983), VI-1, СКЗ, Београд.
3. Јовановић, Слободан (1990) Влада Милана Обреновића, I, Сабрана дела С. Јовановића IV, Београд.
4. Marković, Milan (1972), Međunarodnopravne odredbe o železnicama i izgradnji pruga u Srbiji do Prvog svetskog rata, *Jugoslovenska revija za međunarodno pravo*, 1.
5. Мартенс, Ф. (1909), Европска политика (Историја међународних односа и међународног права), Београд.
6. Мемоари Вукашина Ј. Петровића (2009) ed. Слободан Турлаков, Споменик Српске академије наука и уметности CXLIII, Одељење историјских наука 16, Београд.
7. Мијатовић, Бошко [2006], Дуван и српска држава у XIX веку / *Tobacco and the Serbian State in the 19th Century*, Београд.
8. Миленковић, Петар (1936), Историја грађења железница и железничка политика код нас (1850–1935), Београд.
9. Митровић, Андреј (1985), Berliner Handelgesellschaft и Србија, Зборник Филозофског факултета у Београду XVI – 1.
10. Митровић, Андреј (1997), Стране банке у Србији 1882–1914, Југословенски историјски часопис 1, год. XXX.
11. Митровић, Андреј (2004), Стране банке у Србији 1878–*1914*, Београд.
12. Мрђеновић, Ђурађ (1974), Гвоздени пут Србије, Београд.
13. Недељковић, Милорад (1909), Историја српских државних дугова, Београд.
14. Паларе, Мајкл (2010), Балканске привреде око 1800. до *1914.* године. *Еволуција без развоја*, Београд.
15. Perović, Latinka (1994), Politička elita i modernizacija u prvoj deceniji nezavisnosti srpske države, u: *Srbija u modernizacijskim procesima XX veka*, Beograd.
16. Протић, Драгутин (1908), Карлсбадски аранжман и страна контрола у Србији, Недељни преглед, 11–14.
17. Ристић, Јован (1898), Дипломатска историја Србије за време српских ратова за ослобођење и независност 1875–*1878*, II, Други рат, Београд.
18. Samardžić, Momir (2010), *Roads to Europe. Serbian Politics and Railway Issue, 1878–1881*, Pisa.

19. Србија 1878. Документи. (1978) ed. Михаило Војводић, Драгољуб Р. Живојиновић, Андреј Митровић и Радован Самарџић, Београд.
20. Sundhaussen, Holm (1989), *Historische Statistik Serbiens 1834–1914. Mit europäischen Vergleichsdaten*, Südosteuropäischen Arbaiten 87, München.
21. Traité de Berlin, 1 (13) juillet 1878. Собраніе Трактатовъ и Конвенцій заключенныхъ Россіею съ иностранными державами. Составилъ Ф. Мартенсъ, Томъ VIII, С. Пертербургъ 1888.
22. Вучковић, Војислав (1956), Пад Генералне уније и проглас краљевине (1882), Глас САНУ CCXVIII, Одељење друштвених наука, Нова серија 4, Београд.
23. Зборник закона и уредаба у Кнежевини / Краљевини Србији 35 (1880); 37 (1882), 40 (1884), 41 (1885), 42 (1887), 45 (1890), 46 (1891), 50 (1899), Београд.
24. Живановић, Живан (1924), Политичка историја Србије у другој половини деветнаестог века, II: 1878–1889, Београд.
25. http://www.infotrend.hr/clanak/2012/11/objektivne-opasnosti-%E2%80%93-subjektivna-mjerila,75,972.html

CIP