SUMMARY OF CONTENTS

Section 1: PUBLIC AND PRIVATE ASPECTS OF CRITICAL INFRASTRUCTURE PROTECTION

A COMPREHENSIVE APPROACH TO THE MANAGEMENT OF RISKS RELATED TO THE PROTECTION OF CRITICAL INFRASTRUCTURE: PUBLIC-PRIVATE PARTNERSHIP

Denis Čaleta

The globalisation of the world, and thus indirectly of security, poses serious dilemmas for the modern society about how to continue basing its development on the fundamental requirements related to the free movement of goods, services and people, and, on the other hand, about how to keep threats at an acceptable risk level. The emergence of asymmetric forms of threat to national and international security is based on completely different assumptions and perceptions of the basic concepts of providing security. The changing social conditions and tensions caused by the rapid technological development found particular social environments totally unprepared for confronting the new global security situation and, above all, the newly-emerging complex security threats. The integration of critical infrastructure protection processes into a comprehensive system of national security provision at the national and consequently the international level will be a vey demanding project in terms of coordination and awareness of the necessity or regulating that area. In addition, it will represent a very significant shift in the attitude and mentality of all the participants involved. This paper addresses in detail some important dilemmas and factors which have a strong impact on the level of awareness, cooperation and confidence of all partners in the public and private environment that share the need for the protection of critical infrastructure.

THE PUBLIC AFFAIRS ASPECTS OF CRITICAL INFRASTRUCTURE PROTECTION

Paul Clarke

Governments in South Eastern Europe will find themselves somewhat constrained in using public affairs initiatives to prevent and mitigate against threats to critical infrastructure, in part, because the citizen has limited opportunities to understand the nature of such

infrastructure. But drawing from past experiences with natural disasters, governments in the region can develop a public affairs campaign that can help to both prevent attacks and reduce impacts. In a more general sense, a concerted campaign can increase awareness and preparedness and also create a sense of resilience within society, which will reduce impacts from terrorist attacks and support a rapid recovery.

THE ROLE OF SUPERVISORY BOARDS IN CORPORATE SECURITY SETUPS: THE CASE OF SLOVENIA

Jaka Vadnjal

After the privatization process, Slovenia, like many Central European transition economies, adopted a two-tier system of corporate governance consisting of a management board and a supervisory board which is appointed by the company's assembly, represented by its owners. The role and competences of the supervisory board is generally defined in the Slovenian Companies Act, but can be expanded in line with the company's statute regulations. The main corporate governance power tool possessed by the supervisory board is the hiring and firing of management board members. This power may be directly used to influence both long-term strategic orientations and short-term operational tactics. The actual roles of supervisory boards in Slovenia can be very diverse: from a body with a strict control function to an advice-giving body, which brings the corporate governance system closer to the Anglo-Saxon one. This paper deals with the issue of and dilemmas associated with corporate security systems which can be directly or indirectly influenced by supervisory boards. The main concern appears to be the way of understanding that establishing a corporate security policy and system means costs for the company rather than investment. Thus, supervisory boards, faced with possible unnecessary expenditures, may prefer short-term resource saving to long-term opportunity and sunk cost avoidance.

THE ROLE AND RISKS OF OUTSOURCING IN THE PROCESSES OF PROVIDING CORPORATE SECURITY IN CRITICAL INFRASTRUCTURE

Miran Vršec

This paper discusses risk management in terms of importance, role and risks of outsourcing integrated into the processes of providing corporate security in entities that are part of critical infrastructure in Slovenia. Taking into consideration that Slovenia is only part of the global market, outsourcing needs to be considered in a wider context, i.e. from a global perspective and together with the related impacts. The reason for it is that outsourcing entities, too, are increasingly operating on a global scale. Therefore, it is crucial that a wider global perspective is adapted in discussions. In the context of growing globalization resulting in the networking and integration of business, cultural and other entities coming from different geographic and cultural environments, the opening of the labour market and the related free movement of workers, new risks have emerged which can significantly change the view on outsourcing and its role in the processes of providing corporate security, the mission of which is the provision of safe and smooth operation of business and other processes in business and other critical infrastructure entities in everyday situations, and especially in crisis situation (natural disasters, major accidents at work and environmental disasters, epidemics, terrorist acts, organized international crime etc). The need for a more detailed and, indeed, a scientific research study of the topic arises from my personal findings and conclusions based on research and projects related to a comprehensive and systematic regulation of the management of business security risks and to the adequacy of managing them in commercial and other business entities that operate in practically all areas of critical infrastructure. Obviously, outsourcing is paid far too little or even no attention in building comprehensive integrated security systems, which may have a critical (negative) impact on risk management and may lead to unexpected loss events and failure of individual processes or entire systems, despite systematic security solutions of great quality. The purpose of this paper is to show the significance and role of outsourcing in providing corporate security both at the operational and the strategic levels, as well as to present the risks related to the integration of outsourcing into the processes of providing corporate security.

Section 2: CYBER THREATS TO CRITICAL INFRASTRUCTURE

STRATEGY FOR INFRASTRUCTURE PROTECTION AND CRISIS MANAGEMENT IN THE CYBER AGE: AN ELUSIVE QUEST?

Phil Williams

It is instructive when thinking about infrastructure protection to compare the cyber revolution with the nuclear revolution. Both have had a pervasive impact on security, presenting both challenges and opportunities; both required innovative thinking about the future and about the extent to which traditional concepts and approaches to security were still relevant; and both required radical shifts in mindsets and strategies. Yet in many ways the two revolutions were very different. Nuclear weapons were remote, an ultimate sword of Damocles that demanded prudence, risk aversion, and even cooperation with adversaries. Their very existence changed the calculation of risk. The nuclear club was small and exclusive and, although it has expanded over time, the expansion has been neither as rapid nor has disruptive of stability as often feared. Cyberspace, in contrast, is not remote or "out there;" rather it has become a pervasive and even indispensable part of life in much of the world. It is a reflection of globalization and a contribution to globalization.

DEFENDING CYBER THREATS: WHAT TRADITIONAL NATIONAL SECURITY APPROACH CAN CONTRIBUTE?

Uroš Svete and Anja Kolak

The aim of this paper is to briefly analyse the main trends in cyber security debate as well as to present the existing deficient mechanisms of the national security systems when dealing with threats coming from cyberspace. The deficiency of these mechanisms calls for a **new type of strategic thinking within the "alternative" security concepts,** which would take into account the nature of the threats to cyber security. There is no doubt, cyber space complexity demands a new security paradigm and a broader social consensus, but at the same time it is clear that conventional security instruments can also play a significant role, when cyber space security is an issue.

CYBER TERRORISM AND GREEK DEFENCE STRATEG

Georgios X. Protopapas

Cyber terrorism is considered a hot topic of the 21st century that challenges the structure of conventional national security. Unlimited access to internet technology systems creates preconditions for possible cyber attacks. Cyber terrorism is an asymmetrical and faceless enemy that can threaten the critical infrastructure of states, organizations and military

alliances. This paper discusses how an effective and coherent cyber defence strategy against cyber attacks can be incorporated into the strategies of the USA, NATO, the European Union and Greece. An important finding of the study is that cooperation and coordination at both the international and national levels is the most effective “weapon” against cyber terrorism.

Section 3: CRITICAL INFRASTRUCTURE PROTECTION AND ENERGY SECTOR

MANAGING CORPORATE SECURITY IN THE ENERGY SECTOR: ENERGETICS AS A VITAL (CRITICAL) INFRASTRUCTURE FOR THE FUNCTIONING OF A STATE, ECONOMY AND CIVIL SOCIETY

Milan Vršec

The topic of this paper has been of current global, regional and local interest for several years already. The topicality will increase over years, since energy is of vital importance to humanity. Access to energy will become increasingly expensive and more difficult, not only as a consequence of limited natural conditions and business interests of energy corporations, but also as a result of security threats. In order to cope with energy and security challenges, the EU needs to invest more than a thousand billion Euros in the maintenance and modernisation, and the development of new of energy projects by 2020, since the EU is the world's largest energy importer in the world, accounting for one fifth of the world's energy. This signifies that, in the future, EU member states (and the EU as a whole) will deal with the energy issue more than ever. One of the major problems is the managing of energy security at EU level, at the level of individual member states and at the level of energy companies. This paper focuses on security management in energy companies, proceeding from the European regulation, national legislation and findings of our research and security projects related to Slovenian energetics. We have established that, within the area of energetics, very little emphasis is given on security management. A probable reason for this might be the fact that nothing catastrophic or terrifying has ever happened in the Slovenian energy sector, which would rouse owners, operators, supervisors and the security management. This paper, hence, aims at presenting European energy corporations and energy projects as well as providing a short outline of Slovenian energetics. The second part of this paper provides a general overview on the approach to an improved professionalization of the security management in the energy sector. For this purpose, the paper offers some original solutions for the threat

assessment, control of security risks and establishment of integral security systems within energy companies.

CRITICAL INFRASTRUCTURE PROTECTION AND THE ENERGY SECTOR

Klemen Grošelj

Contemporary societies, despite all their efforts, are still energy-intensive societies which, without reliable and economically acceptable energy, could not function as they do today. Even more fossil energy-intensive are those societies in which a smooth, continuous and affordable supply of energy products is still crucial. Consequently, the importance of critical infrastructure protection (CIP) in the energy sector, which meets the societies' needs in light of contemporary asymmetric and other threats, is that much more pressing and important. This is also the main issue of the article which, in the first part, attempts to present the key theoretical aspects and the basis for critical infrastructure protection in the energy sector. The second part is devoted to a short analysis of the Slovenian energy sector in terms of the concept of critical infrastructure protection.

VULNERABILITY ASSESSMENT: NEW NUCLEAR POWER PLANTS UNIVERSAL METHODOLOGY FOR TERRORISM THREATS AND NATURAL DISASTERS ANALYSES AND PREDICTIONS

Venceslav Kostadinov

National emergency systems in the past did not include vulnerability assessments of the critical nuclear infrastructure as a part of a comprehensive preparedness framework. After the terrorist attack of 9/11, decision-makers became aware that critical nuclear infrastructure could also be a target for terrorism, with the purpose of using the physical and radioactive properties of the nuclear material to cause mass casualties, property damage, and detrimental economic and/or and environmental impact. The necessity to evaluate critical nuclear infrastructure vulnerability to threats like human errors, terrorist attacks and natural disasters, as well as preparation of emergency response plans with optimized costs, are of vital importance for the assurance of safe nuclear facilities operation and national security. This paper presents a new universal methodology and solution for nuclear power plants (NPPs). Vulnerability assessment can help the overall national energy sector to identify and

understand the terrorist and natural disaster threats to and vulnerabilities of its critical infrastructure. Moreover, an adopted methodology could help national regulators and agencies to develop and implement vulnerability awareness and education programs for their critical assets to enhance the security and safe operation of the entire energy infrastructure. New methods can assist nuclear power plants to develop, validate, and disseminate assessments and surveys of new efficient countermeasures. An original contribution is also presented for three different nuclear power plants, one of which is Fukushima in Japan. Particularly important is the qualitative and quantitative temporary assessment of the vulnerability of the nuclear power plant in Fukushima to the recent natural disaster.

THREE EVILS AND THEIR SIGNIFICANCE FOR THE PROTECTION OF THE CRITICAL ENERGY INFRASTRUCTURE IN CENTRAL ASIA

Fu Xiaoqiang

The emerging non-traditional threats, in particular the three evils in Central Asia and China, raise serious questions about the critical oil and gas infrastructure protection in this region, since the regional powers are not ready to protect the oil and gas fields and thousand miles of pipelines vulnerable to any terrorist attacks. In the post-9/11 period, with Al-Qaeda's strategic emphasis on economic jihad, the associated movements in Central Asia have a strong desire to attack critical energy infrastructure in this region, which is becoming an impendent threat. It is very important to make regional countries realize the impendence of the critical energy infrastructure protection, encouraging outside powers to bear more responsibilities, and enhance cooperation and coordination between the US and the regional countries.

Section 4: NATIONAL APPROACHES TO CRITICAL INFRASTRUCTURE PROTECTION

A POSSIBLE MODEL OF THE RESPONSES IN THE REPUBLIC OF SERBIA IN THE PROTECTION OF CRITICAL INFRASTRUCTURE AGAINST A TERRORIST ATTACK

Gačić Jasmina, Mandić Goran, Jakovljević Vladimir

The growing ruthlessness in regard of the kind of victims, especially collateral ones, as well as endangerment of the complete critical infrastructure, testify to the manifest progression of terrorism. The emergence of global terrorism, personified in the consequences of 9/11, 2001, has caused the USA to introduce a new conceptual approach in the management of terrorist threats. Also, the European Union has stressed the need for a different approach in the identification and control of critical resources at its disposal. The Republic of Serbia, essentially interested in the process of approximating European integrations, opted for a novel approach to the problem of terrorism. Besides harmonization of the normative-juridical aspect of combating terrorism, the promotion of the intelligence-security system and the reorganization of the integrated system of protection and rescue, a series of legal and sub-legal acts is adopted by which the state comes closer to solutions in the final determination of critical infrastructure and its protection against terrorist threats. This paper presents a possible model of response in the protection of critical infrastructure against terrorist acts (the proactive-reactive model), that is to be adopted and implemented by critical infrastructures through the use of the System of Property, Persons and Business Protection Measures. That system, as the internal subject of security, along with clear communication and coordination with the external subjects of security, represents a real and valid basis in the protection of the state's critical infrastructure from potential terrorist attacks.

THREATS TO THE CRITICAL INFRASTRUCTURE OF SOUTH-EAST EUROPE POSED BY AL QAEDA AND ITS ASSOCIATED MOVEMENTS: THE CASE OF MACEDONIA

Metodi Hadji-Janev

None-state actors like Al Qaeda and its associated movements have given a new dimension to international terrorism and security since the Cold War. The 11 September 2001 attacks, attacks in Bali (2002), London (2004), Madrid (2005), Mumbai (2009) and Moscow (2010) attest that these non-state actors' agenda has become global, apocalyptic and critical infrastructure focused. Connections to Al Qaeda by some Muslim groups and individuals from South-East Europe in an age of globalization, corrupt transitions, violent Yugoslav conflicts and active support to the Global War on Terror, rise serious concerns to the safety of the critical infrastructure in the region of South-East Europe (SEE).

Like the rest of the South East European countries Macedonia lacks effective strategy for critical infrastructure protection. To be effective this new strategy needs to ensure centralized planning and decentralized execution. The new strategy should focus on preventive measures which require government's involvement in coordination, facilitation and stimulation of all stakeholders involved in critical infrastructure protection. Nevertheless, there will be no effective critical infrastructure protection in an age of globalization without intensive regional cooperation and coordination.

NATIONAL CRITICAL INFRASTRUCTURE PROTECTION: THE ROLE OF PRIVATE SECURITY

Dušan Davidović, Želimir Kešetović, Olivera Pavičević

This article attempts to analyze critical infrastructure protection in Serbia and the role of private security, stating that critical infrastructure protection is quite a new notion in security-related vocabulary in Serbia, since these assets, networks and organizations were known as national companies, or public enterprises. Explaining the main characteristics in a short history of development of private security in Serbia in the last two decades, the authors try to analyze the situation in Serbian critical infrastructure after introducing readers with a European approach to critical infrastructure protection. Adopting the CoESS` definition of critical infrastructure, the authors present the outcomes of the CoESS` White Paper on Public-Private Partnership in critical infrastructure protection. In the conclusion, the authors try to define the main conditions for more intensive and more efficient public-private partnership in the field of critical infrastructure protection and security.