International Conference
"National Critical Infrastructure Protection - Regional Perspective"
(Book of Abstracts)

Organization

University of Belgrade – Faculty of Security Studies
Ministry of Education, Science and Technological Development of Republic of Serbia
Institute for Corporative Security Studies, Ljubljana
Belgrade Chamber of Commerce
NIS Gaspromneft

Publisher

University of Belgrade – Faculty of Security Studies

For the Publisher

Dr Radomir Milašinović, Dean of the Faculty of Security Studies

Editor

Ivan Dimitrijević, Faculty of Security Studies

Proofreading

Luke Ginnell, Vladimir Ninković

Design, Graphics, and Computer Processing

University of Belgrade – Faculty of Security Studies

ISBN 978-86-84069-82-7

University of Belgrade – Faculty of Security Studies
50 Gospodara Vučića St. 11000 Belgrade, Republic of Serbia

International Scientific Conference

National Critical Infrastructure Protection
Regional Perspective

Book of Abstracts

October 24th, 2013

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

Belgrade, 2013

Contents

Editorial

The 'National Critical Infrastructure Protection: Regional Perspective' International Scientific Conference is the first of its kind organized in the Republic of Serbia, and is aimed at the strengthening of national capacities and regional cooperation in relation to the critical infrastructure protection of South-eastern European countries. This aim is in accordance with both the European perspective of South-eastern European countries and the EU Critical Infrastructure Protection Program.

The International Scientific Conference has two main targets. The first one is emergency management related to public authorities and services, and the second one is industry and commerce within the set of standards and topics in the areas of Business Continuity and Organizational Resilience. For this reason, a common spirit is needed in order to provide a holistic approach that encompasses more general and applicable points in relation to any organization and process.

The specific goals of the International Scientific Conference are the theoretical conceptualization of topics covered, and professional discussion in the field of critical infrastructure protection, with the focus on the exchange of experiences not only from South-eastern Europe, but also from other European and non-European countries. With this in mind, the International Scientific Conference is designed in a manner which allows representatives from more experienced countries to give their perspectives first, to be followed by the experiences of representatives from the South-eastern European countries.

The main focus areas of the International Scientific Conference are three equally important and interesting panels: 1) Contemporary Security Threats and Critical Infrastructure, 2) Critical Infrastructure and Protective and Risk Management Policy and Options, and 3) Critical Infrastructure Protection through Crisis and Continuity Management. It should be noted, however, that these three panels are not limited by any of the topics given by the Organizing Committee for the purpose of the call for papers.

This Book of Abstracts from the International Scientific Conference is the result of a regional call for papers made by the Programme Committee, and includes a list of all the papers submitted for the conference, along with abstracts and information about the author(s). It covers all the topics given for the purpose of the call for papers, and its structure follows the conference's scientific and professional structure, as described above.

Our hope is that this International Scientific Conference is just the first step in many similar future scientific and professional events, not only in terms of the South-eastern Europe region, but also in wider terms, regarding not just topics, but also people. We would like to express gratitude to our partners who have selflessly and generously supported the International Scientific Conference.

The Conference is a joint effort by the University of Belgrade – Faculty of Security Studies, the Ministry of Education, Science and Technological Development of the

Republic of Serbia, the Belgrade Chamber of Commerce, the Institute for Corporative Security from Ljubljana, and NIS Gaspromneft.

The topics of the Conference are as follows:

- Contemporary security threats and critical infrastructure (CI)
- New technologies and their influence on critical infrastructure protection (CIP)
- Information technologies and CIP
- New technologies and defence conceptions of CIP
- Significance of Serbian education system in CIP
- Data exchange and protection of privacy
- Public-private partnership
- CI ownership as commodity or threat
- Options for CIP
- Standardization of CIP
- New technologies and information security in CIP
- Influence of security costs on competitiveness of certain industry branches
- Risks of nonconformity with European and international standards
- National CIP strategy and programs
- Identification of interdependence of CI within industry sectors and between them
- Threat, risk, and vulnerability assessment and analysis
- Adjustment of methodologies for risk assessment with CIP program
- Human resource management from the point of view of CIP
- Significance of corporate culture, ethics, and social responsibility
- Ecology and CI threatening
- Procedures for information security
- Solutions in business environment and in public administration which are significant for CI
- Operational continuity management
- Understanding security environment and trends in comprehensive approach development
- Crisis communication in business environment

Programme Committee of the International Scientific Conference
"National Critical Infrastructure Protection: Regional Perspective"

Keynote Presentations

Ernst-Peter Döbbeling

Programs and Trends in Critical Infrastructure Protection in the European Union

Abstract: The starting point in Europe of what is known today as Critical Infrastructure Protection (CIP) was the Millennium, when industry, commerce, administration and emergency services recognized the threat of an extensive breakdown of important infrastructures as a result of the failure of IT-systems, embedded systems or communication systems. After, in 2001, the worldwide terrorist threat and the attack on the World Trade Centre reinforced in Europe the need for awareness and appropriate action with regard to CIP. The European countries and the European Council became strongly aware of the high dependency of the European economy and citizens' security upon infrastructure systems. Attacks on 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. Therefore, an EU CIP program was set into motion in 2005, followed by a directive of the EU Council in 2008 (COUNCIL DIRECTIVE 2008/114/EC) taking into account that CIP is first and foremost a national responsibility due to the subsidiarity principle of the EU. The EU commission concentrated on cross-border effects and gave support to member countries through research programs or exchange of experience. As part of the EU "Seventh Framework Programme" (FP 7) from 2007 to 2013, which is a 50 Billion EU research program, a high number of CIP-related projects were accepted, especially in relation to border security, CBRNE detection and interdependencies of CI-sectors as Electricity or transportation. An EU-wide CIP warning information network (CIWIN) was set up. Furthermore, the EU countries undertook their responsibilities in 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 in areas such as risk analysis, cascade effects or interdependencies of different critical infrastructures. Particularly with regard to 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 parallel to CIP activities, Business Continuity Management (BCM) and IT Security became an important issue. 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 such as ISO 22301 on BCM will most likely become European CEN standards. The presentation will give an overview of the mechanism of CIP in the EU and explain the objectives and activities defined in the EU Council directive and program. The multiple activities, responsibilities and interactions of the EU Council and national countries under the subsidiarity principle will be presented.

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

Dr Ernst-Peter Döbbeling, Dipl. Ing., Professor in Studies of Security & Safety Engineering, Furtwangen University, Germany, E-mail: epd@hs-furtwangen.de

David Austin

How Business Continuity Management Contributes to Critical Infrastructure Protection

Abstract: The paper deals with the emergence of business continuity management as a discipline, and with the need for business continuity in general. Author presents the relationship to legal, regulatory and governance requirements which are put in front of the business continuity management, as well as the relationship between business continuity management and national critical infrastructure. The International Standard for Business Continuity Management (ISO22301) is presented in particular, with its history, organizations which should use the standard, certification process, an overview of key requirements, and relationship to other standards.

Keywords: *business continuity management, international standards, critical infrastructure protection*

David Austin, Director, Operational Resilience Ltd., United Kingdom,
E-mail: dave.austin@oprel.co.uk

Momčilo Milinović, Zoran Jeftić

Challenges of National Defence in International, State and Private Corporative Management of Infrastructure Protection

Abstract: This paper presents the general analyses of questions and requirements which determine the global role of military forces in the protection of corporate security. Extended protection challenges, in both homeland and foreign territorial conditions, comes from integrative roles with nongovernmental and governmental non military forces. According to law obligations, they have insufficient capacity when it comes to protecting huge infrastructures of international importance in the homeland areas, while military formations may appear as supplementary protecting forces. Protection of technology infrastructures required to be protective of corporate management could be extended over a national defence system by technology and organization capabilities. The paper suggests extended interoperable treatment as an international collective, 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 to joint action with non-military actors, integrated with the smallest military units engaged in civilian and private corporative protection jobs.

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

Dr Momčilo Milinović, Full Professor, University of Belgrade – Faculty of Mechanical Engineering, E-mail: mmilinovic@mas.bg.ac.rs

Dr Zoran Jeftić, Assistant Professor, University of Belgrade – Faculty of Security Studies, E-mail: jefticz@ymail.com

Regional Experiences

Iztok Podbregar, Teodora Ivanuša

Public-Private Partnership in Critical Infrastructure Protection

Abstract: The complicated, complex nature of modern threats requires contemporary action. At the forefront of this is the consideration of probability, insecurity as well as the consideration of the whole without deterministic simplifications, an approach with a comprehensive interdependence and a procedural thinking, something which requires extensive knowledge, contacts and influences and their interlacement in order to achieve with reasonable ease the sufficient and requisite holism and creative collaboration or multidisciplinarity. In this way, we reduce the uncertainty caused by the gap between the perception of threats and the actual reality of the threats. The dynamics of threats that tend to escalate into a pre-crisis or crisis situation increases the gap between the required and the established organization of the security system. Limited resources necessitate a search for new solutions during the voluntary, professional and vocational action; perhaps also through public private partnership. The lack of a systematic approach in light of the complex nature of the system, can lead to unilateralism, fatal oversights, and inappropriate crisis communications. One of the solutions is operation and action united in the term 'reengineering.' Contemporary threats demand immediate change, the awareness of the need to say what to do, the knowledge of how to make the changes and the values to separate what is important from what is not.

Due to low interest among the political elite for requisitely holistic future development of the national security system, guidelines for its systemic re-organization (i.e. knowledge, teamwork, dedication to the mission, and requisite holism) are enhanced in the proposed article. Serious gaps between real national needs and national political interests regarding national security systems are found. Reengineering of the national security system as inevitable, thorough, radical and dramatic intervention is suggested. The findings are supported by research of the nature of police work and the satisfaction with police work of the residents of 4 towns in the Republic of Slovenia, with 449 respondents, and 449 fulfilled questionnaires. Some results: the collected data reveals that people from rural areas are more willing to cooperate with the police; young people are more willing to participate than older; in general, people feel safe in the Republic of Slovenia; the perception of safety/security in local areas implies that 'mini' police directorates could or should be implemented. Without radical changes of the Slovenian national security system (i.e. reengineering) the entropy law will accelerate by natural inertia, and the lack of systemic thinking will lead to significant oversights and inevitable failure.

Keywords: *contemporary threats, crisis communications, national security, reengineering*

Dr Iztok Podbregar, Full Professor, University of Maribor, Faculty of Criminal Justice and Security, Slovenia, E-mail: iztok.podbregar@fvv.uni-mb.si

Dr Teodora Ivanuša, Assistant Professor, University of Maribor, Faculty of Criminal Justice and Security, Slovenia, E-mail: teodora.ivanusa@fvv.uni-mb.si

Marjan Gjurovski

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. the inability 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. This 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 the risk of catastrophes represents a national mechanism for coordination and gives a political direction in the sphere of reducing the risk of catastrophes. It is a multi stakeholder structure with interdisciplinary practice involving state institutions, civil society and the public. The approach with regard to the 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 the risk of catastrophes.

Keywords: *risks, catastrophes, platform, security, disasters*

Marjan Gjurovski, MSc, Teaching Assistant, University "St. Kliment Ohridski" - Faculty of Security, Skopje, Macedonia, E-mail: mar.gjurovski@gmail.com

Dragiša Jurišić

Critical Infrastructure Protection in Bosnia and Herzegovina and the Role of 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*

Dragiša Jurišić, MSc, Armed Forces of BiH, Bosnia and Herzegovina,
E-mail: jurisicvrs@yahoo.com

Contemporary Security Threats and Critical Infrastructure

Goran Matić, Milan Miljković

Critical Infrastructure Protection in Cyberspace

Abstract: The massive application of information and communication technology has brought about new risks and threats presented by both physical and software-related dangers to critical information infrastructure and cyberspace that are of relevance to the nation and its security. Tens of thousands of hazardous attacks are registered in cyberspace on a daily basis. The leading countries in the world, as well as international organizations, have shown a 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 specialists in particular areas (the public-private partnership concept). The protection of a highly vulnerable system, such as the national critical information infrastructure also includes the handling of classified information as one of the components through which individual segments of the organization and the functioning of the system are safeguarded. In organizational terms, crisis management in cyber defence implies engaging the capacities of the relevant Ministry of Justice and Public Administration, Ministry of Transportation, Ministry of Defence, 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 the body responsible for the coordination of the national security policy or steered by a ministerial committee.

Keywords: *threats in cyberspace, critical information infrastructure, information security, classified information, crisis management in cyber defence, CERT, national cyber defence council*

Dr Goran Matić, Director, Office of the National Security Council of Republic of Serbia, E-mail: goran.matic@nsa.gov.rs

Milan Miljković, M.M.A.S., Adviser, Office of the National Security Council of Republic of Serbia, E-mail: milan.miljkovic@nsa.gov.rs

Teodora Ivanuša, Matjaž Mulej, Iztok Podbregar, Bojan Rosi

Toward Requisite Holism of Content of the Term Critical Infrastructure

Abstract: The concept of Critical Infrastructures (CI) 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 highlighted points the phrase '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) results in the CBRN/EOD tasks never being autonomous or isolated, but instead being interdependent tasks; allocation of responsibilities is a necessary applied national routine in which the essential imperative is to avoid individual or one-sided unauthorized action. It is complex enough to require systematic thinking, which enhances interdisciplinary creative co-operation, which the Dialectical Systems Theory does more so than others in the Encyclopaedia in order to attain the requisite holism and hence success rather than failure. In forming a new definition of CI, we carried out a comparison of different written sources published at home and abroad; especially with the Dialectical System Theory by Mulej (2000). In light of modern threats (i.e. CBRN/EOD) 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 courses 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 in the case of a natural or intentional outbreak of 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. The activities must be done in an appropriately holistic manner. This is why Dialectical systemic thinking is crucial. According to Mulej et al (2008) we are trying to demonstrate that holism of thinking, decision-making, and action is necessary, as well as how much more success could be yielded in the innovation effort, if more systematic thinking was applied. The problem is rooted in mentality – in humans' thinking and worldview as well as other values and other emotions. Success has always come about thanks to an absence of oversights with crucial impact, while failure is always a consequence of crucial oversights, be it in business, scientific experiments, education, medical care, environmental care, security, invention-innovation processes, etc.

Keywords: *critical infrastructure, strategic definition, CBRN/EOD devices, dialectical systemic thinking, requisite holism*

Dr Teodora Ivanuša, Assistant Professor, University of Maribor, Faculty of Criminal Justice and Security, Slovenia, E-mail: teodora.ivanusa@fvv.uni-mb.si

Dr Matjaž Mulej, Professor Emeritus, University of Maribor, Faculty of Economics and Business, Slovenia

Dr Iztok Podbregar, Full Professor, University of Maribor, Faculty of Criminal Justice and Security, Slovenia, E-mail: iztok.podbregar@fvv.uni-mb.si

Dr Bojan Rosi, Full Professor, University of Maribor, Faculty of Logistics, Slovenia

Denis Čaleta, Aleš Kotnik

Cyber Threats and Dilemmas of Critical Infrastructure Protection in Small States: Comparison between Attacks in Georgia and Estonia

Abstract: Rapid development of cyberspace is the main reason and motivation for dealing with this issue. The international environment is becoming more unpredictable, and challenges more complex, particularly the asymmetric threat. 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? The aim of the research is also to determine whether a threat is one or more threats to critical infrastructure. The achieved objectives represent an understanding of concepts and processes that have occurred in recent years in protecting critical infrastructure and how it can be threatened from cyber space. This paper is the result of scientific and professional methods of work: an analysis of domestic and foreign literature from the field of critical infrastructure protection and security of cyber space, case studies (Estonia, Georgia), experiential knowledge of the method and the method of authority, where we rely on certain authority from this field. The theoretical part of the paper will give a basic insight into the problem and allow further development, research and introduction of solutions into practice. The study will show what were the situation and the consequence of the attack from cyberspace in Estonia and Georgia. The comparison between these two cases will provide us a better understanding of the current international cyber conflict. The discussion will be devoted to finding solutions in the field of risk management when it comes to cyber attacks in the country. The critical infrastructure (ICT) of smaller countries will be analyzed in detail, something which is linked to cyberspace. The analysis will be the basis for further research. The contribution will provide in-depth thinking and theoretical knowledge of the problem, which leads to practical solutions and serve for the further development of the problem. The paper is aimed at all professionals who are involved on any level with the problem of critical infrastructure protection connected to threats from cyber space.

Keywords: *critical infrastructure, cyber threats, cyber attacks, Estonia 2007, Georgia 2008*

Dr Denis Čaleta, Assistant Professor, Institute for Corporative Security Studies and Faculty of State and European Studies, Ljubljana, Slovenia,
E-mail: denis.caleta@ics-institut.si

Aleš Kotnik, MSc, Institute for Corporative Security Studies, Ljubljana, Slovenia,
E-mail: kotnik@t-1.si

Branko Mihaljević, Ivan Toth, Alen Stranjik

Impact of Critical Infrastructure Ownership on the National Security of the Republic Of Croatia

Abstract: Based on property law, the owner has the right and the power to exercise and protect his interests over the property at his disposal. This is one of the fundamental principles of lawful action and procedures of the legal state. The above premise is also important for 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 underway, which will serve to systematically define the issues stated above in the context of national security. In general, legal rulings and definitions to date have 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 to say, 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*

Dr Branko Mihaljević, Lecturer, University of Applied Sciences Velika Gorica, Croatia, E-mail: branko.mihaljevic@vvg.hr

Dr Ivan Toth, University of Applied Sciences Velika Gorica, Croatia, E-mail: ivan.toth@vvg.hr

Alen Stranjik, MSc, University of Applied Sciences Velika Gorica, Croatia

Dejana Jovanović Popović, Zoran Keković,
Miroljub Milinčić, Dejan Šabić

Nanotechnology and Food Safety: Applications and Emerging Opportunities

Abstract: Rapid advancements in nanosciences and nanotechnologies in recent years have opened up new prospects in relation to the numerous potential applications of food critical infrastructures. In this review, the intention is to summarize food system vulnerability as well as the applications of nanotechnology relevant to food packaging and pathogen detection, together with the outstanding challenges that 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 the area of food safety,

rapid developments in nanotechnologies have also raised a number of health and safety and regulatory issues.

Keywords: *nanotechnology, food safety, nanoscience*

Dr Dejana Jovanović Popović, Associate Professor, University of Belgrade – Faculty of Security Studies, E-mail: dejana_kastor@yahoo.com

Dr Zoran Keković, Full Professor, University of Belgrade – Faculty of Security Studies, E-mail: zorankekovic@yahoo.com

Dr Miroljub Milinčić, Associate Professor, University of Belgrade – Faculty of Geography

Dr Dejan Šabić, Associate Professor, University of Belgrade – Faculty of Geography

Nasir Hussain

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 difficult methodological 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 in multi-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 describes recent 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 sub-

ject matter, 2) a case study, demonstrating the generation of possible threat 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 backgrounds via a user-friendly graphical program, 5) The potential for collaboration between 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*

Dr Nasir Hussain, Founder and Partner, Strategy Foresight LLP, London, United Kingdom, E-mail: hussain@strategyforesight.org

Saša Mijalković, Vladimir Cvetković

Vulnerability of Critical Infrastructure by Natural Disasters

Abstract: Natural disasters are an increasing threat to the safety of mankind. Moreover, in past decades, there has been a clear increase in the number of natural disasters, as well as an increase in their destructiveness. This results in a higher loss of life, in addition to both material and non-material damage. Furthermore, the compromising of 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 the prediction and early warning of disasters can be improved, meaning that the resilience and capacity for faster and more efficient revitalization of endangered values and goods can be increased. Aside from the degree of destruction, the response strategy in an emergency situation will depend not just 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 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 the capability of critical infrastructure protection against natural disasters.

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

Dr Saša Mijalković, Associate Professor, Academy of Criminalistic and Police Studies, Belgrade, E-mail: sasa.mijalkovic@kpa.edu.rs

Vladimir Cvetković, MSc, Teaching Assistant, Academy of Criminalistic and Police Studies, Belgrade, E-mail: vladimir.cvetkovic@kpa.edu.rs

Ljiljana Dapčević-Marković

Border Risk Analysis and Protection of Critical Infrastructure

Abstract: As a result of the specific geographical position of the Western Balkans and the Republic of Serbia, intensive regional trade and traffic infrastructure have contributed to a large traffic of passengers and vehicles crossing state borders. Serbia connects Western Europe with the Eastern Europe and Far East. Besides that, Serbia is a neighbour of several EU Member States. Because of this, Serbia is ideal when it comes to migration activities, trafficking of human beings and drugs, smuggling of excise goods, such as cigarettes and jewellery, stolen vehicles, weapon and other cross border criminal activities. In this paper the author explains the state of Serbian border policing, based on both Schengen and EU standards of integrated border management, including the analysis of the risks for internal security and the analysis of the threats that may also affect the security of the EU external borders. The preparation of Risk Analysis must seek to improve border protection and support the decision as to how and where to install and use necessary infrastructure, as well as what powers, measures and activities have to be implemented along the state border between the border crossing points and at border crossing points outside working hours in order to prevent illicit crossing of the state border and protection of its inviolability. Based on the Law on State Border Protection, which is analyzed in this paper, the border police are authorized to collect personal data from persons subject to the exercise of powers of the border police, and to enter these data into records and process them. In order to keep records, the border police are authorized to collect personal data by applying technical and other means used with the aim of searching, determining identity and detecting and apprehending perpetrators of criminal offenses and misdemeanours during state border protection, by photographing, recording and video surveillance. For border security frequency of information exchange on different levels, the exchange of reports of mutual border patrols with neighbouring countries, the exchange of reports in bilateral and multilateral operations and reports on cross-border cooperation with neighbouring countries and other police departments is highly important. In order to explain relations between risk analysis, the protection of critical infrastructure and border security, the author analyzes risk as a function of threat, vulnerability and impact. According to The Common Integrated Risk Analysis Model (CIRAM) which was originally developed in 2002 by a European Council Expert Group, the author defined a 'threat' as a force or pressure acting upon external borders that is characterized by both its magnitude and likelihood, while 'vulnerability' is defined as the capacity of a system to mitigate the threat, and 'impact' is determined as a potential consequence of a threat. At the conclusion, the author gives the findings and recommendations as to how to both maintain and improve the protection of border critical infrastructure and border security. The author has based this paper on present national and European law, standards and good practice.

Keywords: *border security, risk analysis, critical infrastructure, risk, threat, integrated border management*

Dr Ljiljana Dapčević-Marković, Lecturer, Union of South-Eastern Europe Faculties, Novi Sad, Serbia, E-mail: ljiljana_dm@yahoo.com

Marjan Marjanović, Ivan Nađ

Vulnerability Assessment of Critical Infrastructure Facilities Serious and Organized Crime

Abstract: From a social and economic perspective, the protection of critical infrastructure is an essential element for the maintenance of vital societal functions. The need for the selection of optimum and appropriate safeguards and security requires the establishment of a framework for the assessment of critical infrastructure protection and the related risk assessment. Presently, the majority of critical infrastructure facilities are still not taking enough preventive measures in order to be protected from serious and organized crime, something that should be discussed in detail with regard to the risk analysis and evaluation of data. Basic forms of potential threat for facilities, which may cause more or less damage and are in the direct domain of physical and technical protection, are various forms of terrorist activities, sabotage, explosions, fire, burglary and theft, robbery, and industrial espionage. Tackling all forms of serious and organized crime means defining the most effective strategy to counter the perpetrators of serious and organized crime based on data collected by operational activities from criminal and intelligence agencies. This paper investigates the threat assessment model known as 'SOCTA' which has been developed within the EU, as well as two key methods - PESTLE and SWOT data analysis, which may be one of the potential models for risk assessment of critical infrastructure facilities. The authors have placed special emphasis on the fact that the vulnerability assessment of the critical infrastructure against serious and organized crime, which in their opinion, in relation to current literature, is a neglected segment of preventive measure, and in this context a more active approach to the study of this matter is suggested in order to improve the protection of critical infrastructure facilities.

Keywords: *risk assessment, critical infrastructure, serious and organized crime, threat assessment, data collection, intelligence analysis, data evaluation, evaluation of sources, SOCTA, PESTLE, SWOT analysis and competing hypotheses*

Marjan Marjanović, BSc, Director, Security Guard Montenegro,
E-mail: marjan@securityguardmn.com

Dr Ivan Nađ, Assistant Professor, University of Applied Sciences, Velika Gorica, Croatia, E-mail: ivan.nadj@vvg.hr

Ozren Džigurski, Goran Mandić, Mladen Milošević

Critical Infrastructure Security and Social Networks and Social Engineering

Abstract: The purpose of this article is to analyse the problem of critical infrastructure security. With this objective in mind, the authors focus on three main aspects of this problem – SCADA system security, social engineering and the impact of Internet social networks as a higher level of threat**.** The term SCADA (Supervisory Control

and Data Acquisition) usually refers to computerized industrial control systems which monitor and control entire sites, or complexes of managing systems spread out over large areas (anything from an industrial plant to government activities). The security of the SCADA system is the key technological component in the process of controlling and managing critical infrastructure. SCADA systems are exposed to a higher security risk due to their spatial and network architecture and the latent possibility of unauthorized access to certain components of the network and system. The authors present the basic methods of system protection – the separation of the system from public and global networks (Internet, VPN) and the prevention of unauthorized access through implementation of different instruments and procedures (physical protection, technical security, logic protection, specialized hardware and software for blocking the penetration into the system). The article also deals with penetration tests as an instrument for identification of eventual vulnerabilities of the system.

The next analyzed aspect of critical infrastructure security is social engineering. The perpetrators of social engineering acts, aside from the usual methods and procedures of social engineering, usually possess high levels of expert knowledge and practical experience in the domain of concrete critical infrastructure (electronics, telecommunications, informatics, technology, energetics etc.). Due to this fact, social engineering acts have maximum effect when they are perpetrated through the synergy of internal and external subjects. Internet social networks, authors conclude, also have an important role in critical infrastructure protection, especially in crisis situations, such as floods, nuclear accidents and epidemics and terrorist attacks. Social networks and appropriate software can significantly contribute in the process of overcoming organizational deficiencies. They also can mitigate the impact of crisis situations and speed up the recovery of critical infrastructure, and can also be used as a substitute for or supplement to the command and control functions. From another point of view, social network can be identified as a part of the same critical infrastructure that must be protected. Bearing in mind that social networks have become one of the main sources for information gathering process, e-government functioning, the organization of charitable activities and NGO resources, what would happen if they were attacked or disabled? The authors highlight the issues concerning the methods and techniques for the protection of social networks as a critical infrastructure. They pose a question - who will be responsible for planning and implementation of urgent procedures for social network recovery? The question, the authors claim, is one of great importance, as the loss of social network contacts can lead to a reduction of our capabilities for adequate response in crisis situations, which further implies problems in organizational functioning and crisis management.

Keywords: *security, critical infrastructure protection, social networks, social engineering, SCADA*

Dr Ozren Džigurski, Dr Goran Mandić, Dr Mladen Milošević, University of Belgrade – Faculty of Security Studies, E-mail: odzigurski@gmail.com

Miroslav Mitrović, Željko Ivaniš, Vladimir Ajzenhamer

Comprehensive Approach to the Asymmetric Endangerment of National Critical Infrastructure

Abstract: Contemporary global security moments are characterized by great interaction between national and supra-national security structure, the interdependence of national, regional and multilateral forms of higher security integration. However, the role of the state as a single security entity in international relations remains a crucial and indispensable role in the broadest observation of security organization. Also, in the contemporary global security paradigm, actualization of asymmetric forms of endangering state security should not be overlooked. The pertinent question is: how many individual countries, especially those in the transition process, could comprehensively respond to the current form of asymmetric national security threats to critical infrastructure? Moreover, South East Europe (SEE), or more specifically the Western Balkan region, is a part of European continent that we can, through a historical overview, refer to as the cradle and arena of complex, escalating conflicts. All of them are concluded by the mediation of third part, usually through the negotiation and bargaining of the "big players" on the world's stage. The nations of this region desire their own national paradigms, which often correlate with the interests of global powers. The beginning of the twenty-first century reflects the aspiration of all countries in this part of Europe for the development of partnership and allied relations with regard to contemporary security risks and threats. Acknowledging the declarations and growing bilateral and multilateral cooperation in the field of security and defence, the questions is thus: Do the states of Southeast Europe identify the same security risks and threats? Do they have a unanimous opinion of the potential vulnerabilities of critical national infrastructure? Do they share the perception that the security of Southeast Europe is equally a national as well as a regional issue? The complexity and multifaceted nature of these questions points to the necessity for a comprehensive approach to the analysis of forms of potential endangering elements of national critical infrastructure which are crucial for security. In addition, particular attention should be paid to unconventional, asymmetric forms of the jeopardizing of national security and the potential endangering effects on elements of national critical infrastructure. The authors of this paper offer a possible overview of the cross analysis of asymmetrical endangering of the national critical infrastructure of Western Balkan countries, as part of SEE. In the paper the authors use comparative analysis of contemporary approach to the concept of asymmetric security threats, through the prism of particular states' perception of endangering forms regarding their national critical infrastructure.

Keywords: *critical national infrastructure, comprehensive approach, asymmetric security threats*

Dr Miroslav Mitrović, Research Associate, Ministry of Defence of Republic of Serbia, E-mail: mitrovicmm@gmail.com

Dr Željko Ivaniš, Associate Professor, University of Belgrade – Faculty of Security Studies, E-mail: landol@eunet.rs

Vladimir Ajzenhamer, MSc, Teaching Assistant, University of Belgrade – Faculty of Security Studies, E-mail: vladimirajzenhamer@yahoo.com

Critical Infrastructure Protection and Risk Protection and Management Policies and Options

Bojan Zrnić, Veljko Petrović, Branko Medan

Aspects of Critical Infrastructure Protection in the Defence Industry

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. Issues that could be principally dealt with from within the work emphasize the risks that critical infrastructure in the defence industry may be exposed to in the fields of physical and technical security of infrastructure capacity, accidents resulting from the disturbed pyrotechnic safety and industrial security. Physical and technical security is a basic form of protection of human and material resources of critical infrastructure in the defence industry, and this aspect of protection is focused largely on the consideration of direct threats by external influence risks. Accident situations caused by disturbed levels of pyrotechnic safety are of particular interest because they are categorized as the risks that may generate large-scale negative consequences, not just at the level of the subjected critical infrastructure within the defence industry. Possible aspects of protection are reviewed by improvement of the internal work organization, technological processes and environmental conditions. From the point of view of industrial security, the defence industry and its capacity are critical resources, and threatening them can lead to long-term consequences, mainly through the loss of technological preferences and imbalances in terms of competitive advantages in the common market, and also to the overall development and industrial potential of the state. All the aspects of critical infrastructure protection in the defence industry as mentioned above represent one inseparable unity, which requires an integrated approach to risk analysis and development of the necessary level of organizational culture for corporate action in order to prevent undesirable consequences. The concluding remarks will highlight the importance of the aforementioned aspects of protection, their under-representation in our scientific literature, the problems of practical implementation within the real systems, the need to regulate these aspects legally and to strengthen monitoring mechanisms in this area because of the sustainability of the critical infrastructure potential in the defence industry, and thus further improvement and development of the national resources of the state.

Keywords: *critical infrastructure, defence industry, risk, industrial security, protection*

Dr Bojan Zrnić, Ministry of Defence of Republic of Serbia, Defence Technology Department, E-mail: bojan.zrnic@vs.rs

Veljko Petrović, MSc, Ministry of Defence of Republic of Serbia, Defence Technology Department, E-mail: veljko.petrovic@mod.gov.rs

Branko Medan, BSc, Ministry of Defence of Republic of Serbia, Defence Technology Department, E-mail: branko.medan@mod.gov.rs

Dejan Radović, Ivica Radović, Vladimir Jakovljević,
Zoran Čvorović, Boban Tomić

Implementation of GIS Technology in the Management of Natural Protected Areas: Case Study of National Park "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. In Serbia there are 1,032 protected natural areas, covering 534,232 ha, which is equivalent to 6.5% of the national territory. Five of the protected natural areas are National Parks: Mt. Fruška gora, Mt. Tara, Mt. Kopaonik, Mt. Šara and the Đerdap gorge, covering 158,853 ha. Tara National Park (since 1981, covering 19.175 ha) surround s most of the Tara mountain, and the mountain itself is one of the most important centres of Balkan and European ecosystems and species diversity. They represent a unique example of well preserved forests in south Eastern Europe with numerous endemic and relict species of flora and fauna. Among this floristic diversity of Mt Tara, of the greatest interest is the Serbian (Pančić's) spruce *Picea omorika*. Mt. Tara NP is characterized by specific geomorphologic, hydrologic, geologic, soil and climatic features. Mt. Tara NP was nominated in 2004 within the UNESCO – ROSTE program, for Man and the Biosphere (MAB) Reserve status in Serbia as transboundary "Peace Park" status between Serbia and Bosnia & Herzegovina. The geographical information system (GIS) that we have created has proved to be an excellent tool for the spatial planning strategy in assessment and conservation of all natural characteristics of Mt. Tara NP, and is helpful to Park management for sustainable use of landscape resources. GIS of Mt. Tara NP includes data on natural, artificial and management themes.

Keywords: *GIS, natural protected areas, geodiversity, biodiversity, sustainable managing, landscape resources*

Dr Dejan Radović, Assistant Professor, University of Belgrade – Faculty of Biology, E-mail: dejanr@bf.bg.ac.rs

Dr Ivica Radović, Full Professor, University of Belgrade – Faculty of Security Studies, E-mail: ivica.radovic@mpn.gov.rs

Dr Vladimir Jakovljević, Full Professor, University of Belgrade – Faculty of Security Studies, E-mail: vladimir.jakovljevic@fb.bg.ac.rs

Dr Zoran Čvorović, Assistant Professor, University of Belgrade – Faculty of Security Studies, E-mail: zoran.cvorovic@fb.bg.ac.rs

Dr Boban Tomić, Assistant Professor, National Park Tara & University Singidunum, Belgrade, E-mail: boban.tomic@nptara.rs

Vesela Radović, Husam Majeed Hameed

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 relation to disasters. During a disaster the first responders (police units, emergency services and fire department) should be at the first line in order 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 disasters as a necessary contribution to 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 kind of disasters. This paper has special value as it presents the results of research of authors from countries which were often connected in the global policy: Iraq and Serbia. Disasters caused by human beings form a significant threat to the health and life of population in these countries, and represent a great threat to their future development. In both countries, the population has faced a lack of organization, inadequate help to the affected population, who require shelter, food, and other related services. In one part of the paper, the authors examine how first responders are faced with a lack of resources in the most important sectors, such as the health sector, communications sector, energy sector, sector of water supply and waste management etc.

During disaster first responders are entirely aware of risks to which they are exposed, but think primarily about the safety of affected population. Thus, critical infrastructure has to be protected as one of the most important preconditions for adequate response to disaster. In the final section, the authors present a study which confirms that critical infrastructure protection –if adequately protected – means that first responders are enabled to conduct an appropriate level of disaster management. This paper contributes to the academic and public community by addressing the urgent need for improvement in relation to the protection of infrastructure as the top priority for a successful response to disaster. Decision-makers in Iraq and in Serbia must also understand that the protection of critical infrastructure and efficient response to disasters can be achieved only if the first responders have built critical skills and the necessary conditions are in place.

Keywords: *autocratic regime, critical infrastructure, protection, risks, first responders*

Dr Vesela Radović, Educons University – Faculty of Applied Security, Sremska Kamenica, Serbia, E-mail: veselaradovic@yahoo.com

Dr Husam Majeed Hameed, Associate professor, ENT Specialist, Dean College of Medicine, Wassit University, Iraq, E-mail: husam_majeed@yahoo.com

Dušan Davidović, John Kanalis

Protection of Classified Business Information in Critical Infrastructure Protection

Abstract: This paper is an attempt to analyze *Confidentiality* in critical infrastructure protection in Serbia, with the acknowledgement that critical infrastructure protection is quite a new notion in security-related vocabulary in Serbia. Until recently those assets, networks or organizations were known either as national companies or public enterprises. Noting the main characteristics of the importance of safeguarding critical business information, the authors try to analyze the confidentiality situation in critical infrastructure after a general introduction to the idea of safeguarding sensitive business information in critical infrastructure protection. In the past, when vast fortunes were made during wartime, war became a business. Now that vast fortunes are created by business, business is war. The entire ecosystem of any type of critical infrastructure (CI) is first and foremost business. As with any business entity, assets (People, Materials, Property) are vulnerable to intentional or unintentional risks which can lead to an undesirable outcome known as *Loss*. Effective security requires a comprehensive 'systems' approach that protects all the assets of a CI company in order to avoid *Loss,* since *Loss* equates to *Cost(s)*. Providing a CI or site of a CI with effective security involves several factors, some relatively obvious, others less so. The situation is always asymmetric and, additionally, when security is poorly managed it can leave CI vulnerable to the risk of losing sensitive business information – classified or not – through espionage activity. Why? Because, while the attacker needs only to identify a single weak point to concentrate upon, the security manager must cover all points of attack. Espionage and the theft of sensitive business information is a violation of law in many countries. The best source of intelligence by an adversary or hostile intelligence agency is to use primary employee(s) which are the *'weakest link in the chain'* having as they do access to the confidential information they seek. Each CI must identify what information is to be protected and for how long and develop a review program to determine if the information is current and needs to be protected. It is also important to determine the monetary or competitive value of the information. If information is stolen, for effective prosecution and recovery of damages there needs to be a monetary value for the information and/or impact of its loss. CI must ensure that confidential information should be properly marked and that staff part of an education program understands this requirement. In addition to proper marking the organization must ensure that the information is properly stored and secured. *Confidentiality security* is a complement to other 'traditional' security measures that evaluate the organization mainly from an adversarial perspective using available 'tools.'

Keywords: *critical infrastructure protection, espionage, confidentiality, security, risk*

Dušan Davidović, MSc, Institute for Criminology and Sociology Research, CCO, BECCA Serbia and Montenegro Administrator, Belgrade, E-mail: dlagavulin@gmail.com

John Kanalis, CCO, CPOI, CSSMP, CPO, BECCA Europe Administrator, Athens, Greece, E-mail: jkanalis@otenet.gr

Momir Ostojić, Željko Ivaniš

Critical Infrastructure in Air Traffic Management System

Abstract: The paper is dedicated to the analysis of air traffic management systems in the context of critical infrastructure, as a necessary requirement for safe, regular and expeditious air navigation. The results of the analysis of relevant legal and professional documents in field of air navigation and the protection of critical infrastructure, the functional systems analysis and statistical analysis of data on threats and changes of air traffic provide an answer to the research question of the determination of this system in national and European critical infrastructure, in relation to its supranational character within the 'Single European Sky' regulatory framework.

Keywords: *safety, security, protection, air traffic, critical infrastructure*

Momir Ostojić, MSc, PhD Candidate at University of Belgrade – Faculty of Security Studies, Belgrade, E-mail: ostojicmomir@yahoo.com

Dr Željko Ivaniš, Associate Professor, University of Belgrade – Faculty of Security Studies, E-mail: landol@eunet.rs

Kristina Radojević, Zoran Dragišić

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 both our way of life and economic vitality. Ensuring its security is a mission charged to all sector partners, including governments (national, regional, local) and private industry stakeholders. Transportation systems represent an important part of critical infrastructure. The security and safety of transportation influence all other social and industrial processes. Disruption of this system causes disruptions in all other segments of social life. 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. 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 these problems, this paper presents an integrated approach to safety and security and a model of safety and security management system for transportation organizations.

Keywords: *security, safety, management, transportation, safety and security management system*

Dr Kristina Radojević, Teaching Assistant, University of Belgrade – Faculty of Security Studies, E-mail: kristinaradojevic@gmail.com

Dr Zoran Dragišić, Associate Professor, University of Belgrade – Faculty of Security Studies, E-mail: zoran.dragisic@yahoo.com

Slobodan Marković, Sonja Dragović

Social Capital – Security Factor of National Infrastructure

Abstract: In times of great crisis and profound social changes, such as in the state of Serbia, a country currently undergoing a period of transition, there is a need to analyze the entire infrastructure that underlies its development. However, it is the intention of this paper to analyze the security of the society and the state in terms of social capital, based primarily on its expected social functions, and then on its condition and involvement in finding solutions for the security of national and regional infrastructure, by empirical analysis of capital in determining the direction and focus of future activities. Trying to analyze this problem in terms of volume, space and time, is one of the most complex types of social change, with the scope and depth on turn of the XXI century surpassing all expectations. It is a process that results in optimism being quickly transformed into social crisis, thus leading to great discontent. The security disparity that exists between the high hopes of the new changes and the perception of the objective situation in the new reality has been marginalized by the power of knowledge in political practice. In parallel, there have been manifestations of different forms of social discontent and of other groups in public, no recognition of the role and activity of social capital - particularly its intellectual part–for the higher level of security and social development, whether it be on a national or a wider scale. In this regard, attention will

be focused on the contrast between the social function of the intellectual elite as a generator of knowledge, which we appreciate to be found on the defensive, and its opposite, which is found in the offensive. As a result of these relations, the paper will seek to answer the achieved level of (un)safe state of the national infrastructure, and the state of the overall power of the state and society, based on the findings and conclusions that opinion to overcome the situation.

Keywords: *social security, social capital, a new security dilemma, security feature of social capital*

Dr sc. Slobodan Marković, Assistant Professor, High School of Business and Law Studies "Dr Lazar Vrkatic", Novi Sad, E-mail: slomark@gmail.com

Sonja Dragović, MsBA, Teaching Assistant, High School of Business and Law Studies "Dr Lazar Vrkatic", Novi Sad, E-mail: sonja.dragovic@hotmail.com

Ljubinka Katić

Education as the Critical Infrastructure Protection Factor

Abstract: The aim of this paper is to note the necessity of reassessment and 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 a 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, also containing a significant material component, 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 instrumental value, as well as independent protection value. In the first instance, its purpose is to contribute to security culture development for the entire population, as well as professional education for security staff and the security aspect of engineering-technological staff's professional education.

The author concludes that the human development humanistic model, which points to economic development as the means to achieve human goals, positions education among critical societal systems and processes. Throughout history, it has proven to be a powerful resource – not just for knowledge acquisition, but also for developing values that assure permanence of a given culture. If, in relation to the field of education, we are to apply the commonly used metaphor of critical infrastructure being the "bloodstream" of a society, this field could be considered its "nervous" system, probably superseding everything else in vital significance.

Keywords: *critical infrastructure, critical criteria, education, protection, education strategy*

Dr Ljubinka Katić, Teaching Assistant, University of Belgrade – Faculty of Security Studies, E-mail: ljkatic@gmail.com

Dane Subošić, Dragan Mlađan

Main Features of the Fire Fighting Intervention Carried Out by the Belgrade Fire and Rescue Brigade

Abstract: Fire and rescue units are an important component in 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 protected values (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. In order to make this time shorter, fire and rescue units should arrive at 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. Thus, this paper considers the time of arrival at the scene of intervention at objects of critical infrastructure and its influence on the duration of fire-fighting at those objects, as carried out by the Belgrade Fire and Rescue Brigade in the period 1986-2009. The research was conducted in such a way that all the interventions at objects of critical infrastructure have been sorted by year in the aforementioned 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. 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, analysis of which 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 conditions for the prediction of further engagement of fire and rescue units in Belgrade and other major cities.

Keywords: *critical infrastructure, fire and rescue brigade, arrival to the scene, intervention, duration*

Dr Dane Subošić, Associate Professor, Academy of Criminalistic and Police Studies, Belgrade, E-mail: dane.subosic@kpa.edu.rs

Dr Dragan Mlađan, Associate Professor, Academy of Criminalistic and Police Studies, Belgrade, E-mail: dragan.mladjan@kpa.edu.rs

Ivica Đorđević, Zoran Pavlović

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 in relation 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 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 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 and 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*

Dr Ivica Đorđević, Assistant Professor, University of Belgrade – Faculty of Security Studies, E-mail: ivicadj@fb.bg.ac.rs

Zoran Pavlović, English Language Lecturer, University of Belgrade – Faculty of Security Studies

Critical Infrastructure Protection through Crisis and Continuity Management

Želimir Kešetović, Nenad Putnik, Marko Rakić

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 the normal function of contemporary society. This 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 subject to a specific situation, facing as they do severe transformation in all spheres (democratization of the society, overcoming authoritarian legacy, transformation of social property, deteriorating infrastructure, outdated technologies etc.). They fall significantly behind developed countries which have more developed 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 said problems, which are faced by the majority of countries in transition, 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, the comparative method has been used in order 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*

Dr Želimir Kešetović, Full Professor, University of Belgrade – Faculty of Security Studies, E-mail: zelimir.kesetovic@gmail.com

Dr Nenad Putnik, Assistant Professor, University of Belgrade – Faculty of Security Studies, E-mail: nputnik@fb.bg.ac.rs

Marko Rakić, MSc, PhD Candidate, University of Belgrade – Faculty of Security Studies, E-mail: m.rakic01@gmail.com

Dejan Škanata, Ivan Toth

Development of National Critical Infrastructure Protection Plan

Abstract: Critical Infrastructure (CI) is the backbone of a country's economy, security and health. The fundamental property of CI systems is their interdependency. The result of such a property is the well-known cascading effect, meaning that disruption of a particular CI may cause tremendous losses not only in the sector considered, but in the other CI sectors as well. This is why CI must be secure and able to both withstand

and rapidly recover from all predictable hazards. In other words, CI protection, recovery and rescue action plans should be developed on both the sectorial and national level of a country.

It seems clear that the application of upstream and downstream risk assessment methodologies and decision-making based on usage of these methodologies are the best procedures to approach such a challenging goal. In fact, risk analysis methods are widely used to inform decisions in areas where equipment failures, human errors, natural phenomena or deliberate human behaviour may cause significant impacts to society.

Establishing criticality, the development of an appropriate national legislative framework, performing upstream risk analyses and corresponding protection plans of the CI systems analyzed, modelling interdependencies between different assets, performing downstream risk analyses and building confidence between public and private sectors are the essential steps to be taken in reaching a consistent National CI Protection Plan (NCIPP) in a country. It is clear now that Croatia is approaching this concept as well. After all, it is an obligation that arises from Council Directive 2008/114/EC.

Keywords: *critical infrastructure, upstream risk analysis, downstream risk analysis, protection plan*

Dr Dejan Škanata, Professor, University of Applied Sciences, Velika Gorica, Croatia,
E-mail: dejan.skanata@enconet.hr

Ivan Toth, MSc, Lecturer, University of Applied Sciences, Velika Gorica, Croatia,
E-mail: ivan.toth@vvg.hr

Dragan Trivan, Vladimir Radović

Corporate Security Role in Protecting Critical Infrastructure

Abstract: An increase in the risk of asymmetric security threats, especially after the terrorist attacks in the U.S. in 2001, has led to the protection of critical infrastructure becoming one of the priorities of national security in almost all countries. Although in theory there is no complete consensus 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 function 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 the target of different threatening acts, including terrorism. Therefore, critical infrastructure facilities are specially protected, along with the creation of regulatory, organizational, technical and security conditions for its normal function in order to prevent or reduce the probability of occurrence of the natural or man-induced incentives that could lead to catastrophic disruptions within the protected systems. In this regard, research of the issues related to the role of corporate security in the protection of critical infrastructure requires the use of different scientific methods (his-

torical-comparative method, case studies, content analysis, testing). When it comes to 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 public enterprises that have been transformed in the past period into independent companies providing security services. Other facilities of 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 doesn't include an adequate legal basis. The function of corporate security in 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, as well as 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 for their protection to implement the integrated model of corporate security, along with the outsourcing of the less sensitive functions of the system (physical and technical security) to the external specialized providers. Analysis of the research results suggests the necessity of adopting the encompassing normative regulation and the establishment of the appropriate organizational form of corporate security at critical infrastructure facilities in Serbia. In particular, the research can help agencies in the area of private security with regard to their engagement to perform some of those functions according to the outsourcing model.

Keywords: *critical infrastructure, security threats, corporate security, protection, Republic of Serbia, outsourcing*

Dr Dragan Trivan, President, Serbian Association of Corporate Security Managers, Belgrade, E-mail: dtrivan@gmail.com

Vladimir Radović, Postal Communications "Srbija", E-mail: vradovic@jp.ptt.rs

Zoran Keković, Sandra Vučić, Radosav Despotović, Nenad Komazec

Accordance of Education Programs with the Need for National Critical Infrastructure Protection

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 inter-

est 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 employer 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*

Dr Zoran Keković, Full Professor, University of Belgrade – Faculty of Security Studies, E-mail: zorankekovic@yahoo.com

Sandra Vučić, MSc, PhD Student, University of Belgrade – Faculty of Security Studies, E-mail: sandra.vucic@gmail.com

Radosav Despotović, Security Manager, NIS, Novi Sad, E-mail: radosav.despotovic@nis.rs

Nenad Komazec, MSc, University of Defence – Military Academy, Belgrade

Dragana Nikolić, Ana Kovačević, Srboljub Stanković

Threat Assessment for the Design of the Effective Protection System for Nuclear Installations

Nuclear installations, such as nuclear power plants, research reactors, reprocessing facilities and other components of the nuclear fuel cycle, including the transport between these sites, are among the most critical infrastructures not only for their importance in the energy sector, but also because of the severity and the extent of the potential consequences in case of accidents involving nuclear and other radioactive materials. The possible threat ranges from extreme natural occurrences (such as earthquakes, tornadoes, flooding), failures of structures and components, installation internal type events and human errors, to unauthorized removal of nuclear material and malicious acts intended to cause damage, culminating with terrorist attack. Some of these threats are primarily taken into account in safety analysis, while others are in the focus of security assessment. Although nuclear safety and security regimes have a different focus, they overlap with each other and have a common objective - to prevent radiological damage to population, property and the environment, and to avoid negative economic effects and social disruption. Therefore, establishing and maintaining effective protection of nuclear installations and nuclear material is a complex task that requires careful evaluation of risks and consideration of both safety and security measures for risk prevention and mitigation of the consequences. 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.

Keywords: *critical nuclear infrastructure, nuclear security regime, design basis threat, physical protection, nuclear safety, unauthorized removal, sabotage, terrorist attack, integrated risk management*

Dr Dragana Nikolić, Project Manager, University of Belgrade – Institute of Nuclear Sciences "Vinča", E-mail: anikol@vinca.rs

Dr Ana Kovačević, Assistant Professor, University of Belgrade – Faculty of Security Studies, E-mail: kana@rcub.bg.ac.rs

Srboljub Stanković, MSc, Chief of Metrology, Ionising Radiation Protection, University of Belgrade – Institute of Nuclear Sciences "Vinča", E-mail: srbas@vinca.rs

Ivana Simović-Hiber

The Role of the Criminal Law in Protecting Information Society

Abstract: Post-modern society is often characterized as an "information society" as a result of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society lays 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 attacks on the integrity of IT have become serious threats that affect not only individual interests but also the critical infrastructure and 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 make it necessary to employ criminal law in relation to the prevention and sanctioning of acts that interfere with the integrity of communications based on IT. However, many of the general problems of criminalization (ex precisely defining the criminal act) are found in this area, with some of them being especially acute when a legislature sets out to incriminate assaults on the integrity of IT. The following specific problems come to mind: how can criminal law keep up with the quick pace of the development of information technology 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 vulnerability of "information society" create new challenges to the criminal law, testing the limits of the criminal law as we know it.

Keywords: *ICT, criminal law, surveillance society, new legal interests, protection*

Dr Ivana Simović-Hiber, Full Professor, University of Belgrade – Faculty of Security Studies, E-mail: ivanassss@hotmail.com

Milica Bošković, Violeta Ivković, Nenad Putnik

Risk Management in Public-Private Partnership over Critical Infrastructures

Abstract: In the process of system and organization management, aside from top-management, production and financial management, one of the key roles is the risk management process and the associated duties. Security and risk management of critical infrastructures are tasked with providing for it owners (public or private) business stability and continuity as well as safe work conditions for their employees, along with environmental protection. By implementing privatization processes over critical infrastructures without adequate control, so-called transition countries, characterized by weak institutions, legislative and economy, face the challenge of choosing the right model for re-building systems and institutions, in order to provide better public services and improve socio-economic conditions. This is the reason why public-private partnership has become an attractive choice for state government, besides strictly public (state) and private ownership and professional and unprofessional management of critical infrastructures. In this article we analyze the possibilities and capabilities with regard to the implementation of the preventive phase of the risk management process, in the case of a public-private partnership over critical infrastructures. By describing and analyzing various theoretical approaches to the issue of the management of critical infrastructures, we will examine scientific knowledge and practical experience of different countries in order to perceive and explain the possible benefits of public-private partnerships for the risk management process. The aim of this article is to examine the possibility that public-private partnership could theoretically improve the established approach to elements, processes and activities of prevention and risk management. We will analyze public-private partnership in relation to 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.

Keywords: *critical infrastructure, risk management, public-private partnership, prevention*

Dr Milica Bošković, Associate Professor, University of Belgrade – Faculty of Security Studies, E-mail: boskovicmil@gmail.com

Violeta Ivković, MSc, Teaching Assistant, University of Belgrade – Faculty of Security Studies, E-mail: leta@ptt.rs

Dr Nenad Putnik, Assistant Professor, University of Belgrade – Faculty of Security Studies, E-mail: nenad.putnik@gmail.com

Ana Juzbašić

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 government. They are to be protected comprehensively in the context of protected values/systemic risks: economic, social, environmental, security and safety. One of the state responses to crisis is restructuring of critical transportation infrastructure. Restructuring due to economic reasons and the 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 Balkan region is faced 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, known as integrated protection. This paper sheds light on the risks and vulnerability assessment and methodology to encompass airports as national critical transportation infrastructures. The research question asks whether airport restructuring affects compliance with all relevant protected values (systemic risks) and which aspects of protection are to be thoroughly investigated. The case study analyzed the restructuring of airports as public monopolies in transport. The complexity of this paper determines complementary use of several methods 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 were used. Content analysis was used to systematize findings of various scientific disciplines for topic and border areas. The paper found that each of the aforementioned aspects of critical transportation aspects undoubtedly become more valued after restructuring and ownership change in critical transportation infrastructures. Viewed through the whole prism, it contributes to improved business results of these monopolies. This paper analyzes activities to be implemented in order to mitigate systemic risks of safety, security, environment, economy and the social momentum of airport operators in three sections - the strategic, tactical and operational level. It was found that these integrated protection aspects at the airport are not directly affected by restructuring, privatization or deregulation. Sufficient regulatory incentives exist for the airport in order to achieve and maintain the adequate level of safety and security at least in one section-operational, which compensates for failures in other levels. Economic incentives are a 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 with global interest in this subject.

Keywords: *critical transportation infrastructure, integrated protection, risk analysis, public interest*

Dr Ana Juzbašić, "Nikola Tesla" Airport, Belgrade,
E-mail: ana_juzbasic@yahoo.com

Dragan Simeunović

Serbian Efforts in the Protection of Transport as Critical Infrastructure from Terrorism

Abstract: This paper aims to help identify best practices in relation to reaching a better understanding of new threats regarding critical infrastructure, including transportation security matters which must be addressed. Additionally, this paper aims to facilitate a better understanding of Serbian efforts in the protection of transport, including co-operation and collaboration between government agencies, security experts and critical infrastructure experts on the issues of prevention, preparedness and consequent management. The strong presence of the violent, extremist Islamist ideology in Serbia and other countries of the region and the region's continuing problems leave it vulnerable to terrorism in the future.

Dr Dragan Simeunović, Full Professor, University of Belgrade – Faculty of Political Science

Ljubodrag P. Ristić, Bojana Miljković-Katić

Borrowing for Construction of Railways and Protection of Critical Infrastructures in the Kingdom Of Serbia (1881-1895)

Abstract: By taking loans for the construction of railways, as well as for budget deficit rehabilitation, Serbian governments were essentially pledging fiscal revenues in order to be able to service those loans, in addition to setting up the special revenue funds for the collection of finances earmarked for the repayment of due annuities. These funds were managed by two representatives – a Serbian one and a creditor's one. In addition to borrowings used for the construction of railways (1881, 1885, and 1886) that were contracted, creditors were also put in charge of the 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 (customs and railways revenues, duties, turnover taxes, revenues of both salt and tobacco monopolies…). In order to get its own financial control retrieved, as well as to ensure the protection of the strategically important transport route, the state began buying out, from 1888, all pawned revenues and railway exploitation rights. However, at the same time it was making additional borrowings in order to fund the necessary payments. By establishing the *Directorate of Serbian Railways* the state took over both railway management and control of future railway line development, 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.

Keywords: *Serbia, Austro-Hungary, 19th century, state railways, foreign loans, state revenues, monopolies, nationalization, Independent Monopoly Administration*

Dr Ljubodrag P. Ristić, Research Associate, Institute for Balkan Studies – Serbian Academy of Sciences and Arts, Belgrade, E-mail: risticljp@yahoo.com

Dr Bojana Miljković-Katić, Research Associate, Institute of History, Belgrade, E-mail: bojana.miljkovic.katic@iib.ac.rs

University of Belgrade – Faculty of Security Studies

Core Activity and Affiliation

The Faculty of Security Studies is a graduate-level member institution of the University of Belgrade and it belongs to the group of the humanities faculties. By its syllabus and curriculum, the Faculty covers interrelated philosophical, sociological, political, legal, economic, psychological, ethical, humanitarian, civil-military, and other aspects of security studies, human and social resources, defence, civil defence and environment protection. Within its core activity – the security studies, the Faculty offers basic academic and undergraduate studies, Master's degree studies, doctoral, and specialist undergraduate studies, as well as professional training and education. The Faculty carries out basic scholarly, applied and development research and has been accredited as a scholarly institution by the Ministry for Science and Environment of the Republic of Serbia.

History

The Faculty of Security Studies evolved from the Institute, later Section, for National Defence of the Natural Sciences and Mathematics Faculty, University of Belgrade, in the school year of 1975/76. In October 1978, the Section for National Defence divided from the Natural Sciences and Mathematics Faculty and grew into an independent university-level educational and scientific institution – the Faculty of People's Defence. To build upon and keep abreast of scientific achievements in the field of defence, protection and security, the Syllabus and Curriculum of the Faculty was renewed and its name was changed into the Faculty of Defence and Protection of the University of Belgrade, and then changed again into the Faculty of Civil Defence in the school year of 1990/1991. As of May 2006, the official name of the Faculty is University of Belgrade – the Faculty of Security Studies.

Cooperation

The Faculty has had intensive cooperation with national and international institutions, as well as numerous business organizations. Based on agreements on scientific and technical cooperation, diverse educational and commercial programs have been implemented.