NATO Science for Peace and Security Series
D: Information and Communication Security - Vol. 39

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection

Edited by
Denis Čaleta
Vesela Radović

IOS
Press

NATO
OTAN

This publication is supported by: The NATO Science for Peace and Security Programme

COMPREHENSIVE APPROACH AS “SINE QUA NON” FOR CRITICAL INFRASTRUCTURE PROTECTION

NATO Science for Peace and Security Series

This Series presents the results of scientific meetings supported under the NATO Programme: Science for Peace and Security (SPS).

The NATO SPS Programme supports meetings in the following Key Priority areas: (1) Defence Against Terrorism; (2) Countering other Threats to Security and (3) NATO, Partner and Mediterranean Dialogue Country Priorities. The types of meeting supported are generally "Advanced Study Institutes" and "Advanced Research Workshops". The NATO SPS Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO's "Partner" or "Mediterranean Dialogue" countries. The observations and recommendations made at the meetings, as well as the contents of the volumes in the Series, reflect those of participants and contributors only; they should not necessarily be regarded as reflecting NATO views or policy.

Advanced Study Institutes (ASI) are high-level tutorial courses to convey the latest developments in a subject to an advanced-level audience.

Advanced Research Workshops (ARW) are expert meetings where an intense but informal exchange of views at the frontiers of a subject aims at identifying directions for future action.

Following a transformation of the programme in 2006 the Series has been re-named and re-organised. Recent volumes on topics not related to security, which result from meetings supported under the programme earlier, may be found in the NATO Science Series.

The Series is published by IOS Press, Amsterdam, and Springer Science and Business Media, Dordrecht, in conjunction with the NATO Emerging Security Challenges Division.

Sub-Series

A.	Chemistry and Biology	Springer Science and Business Media
B.	Physics and Biophysics	Springer Science and Business Media
C.	Environmental Security	Springer Science and Business Media
D.	Information and Communication Security	IOS Press
E.	Human and Societal Dynamics	IOS Press

http://www.nato.int/science
http://www.springer.com
http://www.iospress.nl

Sub-Series D: Information and Communication Security – Vol. 39
ISSN 1874-6268 (print)
ISSN 1879-8292 (online)

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection

Edited by

Denis Čaleta
Institute for Corporative Security Studies, Ljubljana, Slovenie
Email: denis.caleta@ics-institut.si

and

Vesela Radović
Faculty of Applied Security, University Educons, Serbia
Email: veselaradovic@yahoo.com

IOS Press

Amsterdam • Berlin • Tokyo • Washington, DC
Published in cooperation with NATO Emerging Security Challenges Division

Proceedings of the NATO Advanced Research Workshop on
Managing Terrorism Threats to Critical Infrastructrure – Challenges for South Eastern Europe
Belgrade, Serbia
12-14 May, 2014

© 2015 The authors and IOS Press.

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without prior written permission from the publisher.

ISBN 978-1-61499-477-0 (print)
ISBN 978-1-61499-478-7 (online)
Library of Congress Control Number: 2014 956 434

Publisher
IOS Press BV
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 687 0019
e-mail: order@iospress.nl

Distributor in the USA and Canada
IOS Press, Inc.
4502 Rachael Manor Drive
Fairfax, VA 22032
USA
fax: +1 703 323 3668
e-mail: iosbooks@iospress.com

LEGAL NOTICE
The publisher is not responsible for the use which might be made of the following information.

PRINTED IN THE NETHERLANDS

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.

Editorial

Denis ČALETA[1] and Vesela RADOVIĆ[2]

The world in which we live today is becoming more and more complex, both from the viewpoint of ensuring security as well as of the strong dependence of the social community on technology, which is represented by so-called critical infrastructure. We are surrounded by a dynamic security environment in which we witness various security threats and risks - which even yesterday still seemed marginal. International terrorism is much overlooked and represents one of the most important threats for a normal functioning of the modern democratic society and its values. In the period after the terrorist attack in the United States of America (USA) we have witnessed the so-called anti-terrorism war, which has not managed to eliminate or lessen the reasons for emerging and establishing new terrorist networks.

When these factors are put into the context of the development of modern technology, we can see that the provision of security against terrorist threats is extremely difficult. Despite the efforts of national security entities in the national and international context, terrorist threats are not completely preventable. This means that it is necessary to prepare the functioning of the system, starting from the wider social community response to the occurrence of a terrorist attack, to an extent that it will quickly and effectively operate even in this type of crisis.

The coordination of authorities and services responsible for the first response in the event of a terrorist act is one basic requirement, which can significantly contribute to a more effective response and reduction of adverse effects. Of course, the economic and financial crisis puts us all in the position that would in the long term entail a reduction of resources for the functioning of the national security system and thus less efficient functioning of those parts of the system that are designed to respond to crisis first. On the other hand, every crisis can be an opportunity to achieve a more rational look at the system as a whole and critically define the role of each individual segment. Through a thorough analysis of national security systems, conducted after 11 September 2001, the main findings were primarily focused on the lack of coordination, duplication of responsibilities, non-systemic approaches and the capability development in the field of countering complex threats, which certainly include international terrorism. A few steps towards improving coordination and concerted action have definitely been done, but still not enough.

Due to rapidly changing environment and related forms of individual threats, which are increasingly moving into the cyber environment, the national security systems, which in many cases are burdened with bureaucratic approaches to changes, face great difficulties in monitoring this dynamics. In this respect, the largest problem lies in the countries which have luckily not yet been submitted to major terrorist threats, but are, due to this virtual safety, responding to terrorist risk much slower than other countries. In a mutually interdependent environment this can become a serious problem, since

[1] Dr. Denis Čaleta, Institute for Corporative Security Studies, Ljubljana, Slovenia, e-mail: denis.caleta@ics-institut.si.

[2] Dr. Vesela Radović, Faculty of Applied Security, University Educons, Serbia, e-mail: veselaradovic@yahoo.com.

international terrorism knows no borders and in such environments, it benefits from exploiting the lack of system control measures. In the international community, it has long been recognized that an effective system of international response to terrorist threats can only be successful as much as individual countries, including those less well prepared. From this perspective, the above-mentioned crisis can be considered an advantage, in the sense that we are forced to respond more rationally to the structuring of the national security system and thus eliminate barriers of cooperation between line ministries, which just yesterday seemed insurmountable. The realization that the bodies of national security system are no longer a sufficient condition for a successful functioning of the counter-terrorism system is also strongly enforced. This process certainly requires the inclusion and participation of other non-state actors, which are developed in the framework of private and corporate security sector. To respond effectively to terrorist threats, it is important to mobilize a comprehensive range of levers, not necessarily of state character. The development of public and private partnerships is increasingly penetrating even to the area of security, thus these processes need to be seriously taken into account in building a stronger and more efficient system. If, however, this framework includes threats by individual terrorist groups to use the means of mass destruction, we see that effective participation of the full range of bodies and organizations is the key factor, which in the phase after a terrorist act, sufficiently maintains the effects of such an act at an acceptable level. Of course, there is always a dilemma, which is the acceptable level of risk management, because every human life is invaluable. However, as a suitable level one should look for a critical point that has to be attained for the society to establish normal functioning as soon as possible, despite a crisis situation.

Terrorist attacks do not only cause material damage; their effect is especially problematic from a psychological perspective. From this perspective, an effective system of responding to terrorist threats should not only include initial emergency measures to reduce damage to property and protect human lives, but should continue through later stages of managing post-traumatic disorders of individuals in a wider social environment. With the development of information and other technologies, the society has become complex and vulnerable. We live in an increasingly high-risk society. The positive aspects of development also bring several strongly negative consequences that can, in their extreme form, present an increasing threat to individual, national or international security. The remarkable development of technology has certainly facilitated progress in all segments of the functioning of the society. However, on the other hand, the dependence of the society on the functioning of technological systems is strong; a minor system malfunction might have important consequences for the functioning of the society. For this reason, the reliance on the functioning of this infrastructure has obvious direct and indirect impacts on its threat and represents a tempting target for international terrorist operations.

Due to the obvious interdependence, terrorist operations, which used to have local dimensions in the past, are now taking on new regional and global dimensions. The complexity of international relations and the functioning of the international system make national security systems interact with the regional and international environment. In fact, contemporary terrorism has helped the regional community recognize it as a regional phenomenon that requires regional response at different levels. Since terrorist activities are not confined to national borders, the international community can fight terrorism effectively only with the improvement of measures in the area of cooperation, organisation, solidarity between countries, initiatives combining different strategies and mechanisms, and specifically with an increased exchange of information that are important for countering this regional problem. That was one of the main goals of this NATO Advanced Research Workshop ”Managing Terrorism Threats to Critical Infrastructure – Challenges for South Eastern Europe“, which was held in Belgrade, Serbia in 2014. The participants from fifteen NATO and partner countries and three international organisations had the opportunity to share their knowledge and experiences on the future improvement of critical infrastructure protection from various terrorist threats. At the same time a collaborative link between scientists and specialists in the region was created. This network of stakeholders will foster further collaborations and the exchange of ideas regarding critical infrastructure protection from terrorist attacks.

In this book, we presented and pointed out authors’ main dilemmas and challenges that might influence the process of managing terrorist threats in the region of SEE. It also helps uncover a part of challenges which the complex security environment with its threats brings to the subjects of national, regional, as well as international security in South Eastern Europe.

In the end Editors, on their behalf and on the behalf of all authors, express their deep gratitude to NATO Emerging Security Challenges Division for the moral professional and financial support, which made possible organization of this event. The Editors wish to acknowledge with appreciation the assistance of Dr. Iztok Podbregar and Dr. Anita Perešin in reviewing the manuscripts for this publication.

Dr. Denis Čaleta
Institute for Corporative Security Studies

Dr. Vesela Radović
Faculty of Applied Security, University Educons

This page intentionally left blank

Contents

This page intentionally left blank

Section 1:
Strategic Environment and Critical Infrastructure Protection

This page intentionally left blank

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-3

Contemporary Aspects in Critical Infrastructure Protection and Combating Terrorism

Ferdinand ODŽAKOV [a,1] and Metodija DOJČINOVSKI [b]
[a] *Military Service for Security and Intelligence, Ministry of Defense, Republic of Macedonia*
[b] *Military Academy, "General Mihailo Apostolski", Skopje, Associated member of the University "Goce Delcev"-Stip, Republic of Macedonia*

Abstract. The paper points out the specific challenges of possible appearances, threats, risks and dangers to critical infrastructure caused by the activities of modern terrorism. Sensitivity and protection of networks and systems at the national level is priority for national security and the basics on prevention and coordination of measures and activities between the security services. Modern terrorism knows no borders, regions, states. It is focused on critical infrastructure, whose damage or destruction accelerates the motivation for achieving goals. Targets are: pipelines, telecommunications, information technology, financial systems, social, economic, industrial, medical and other important segments of the society, where important preventive roles have not only national, but also international actors and institutions, the European Union, NATO, OSCE, INTERPOL. The new millenium has shown that there is no country that is completely safe and protected from modern forms of asymmetrical threats. The World is "bombarded" with information on a daily basis about events that create feelings of insecurity, fear, threat and danger. Critical infrastructure have become the target of new forms of terrorist threats, known as cyber-terrorism, bio-terrorism, eco-terrorism, nuclear-terrorism and others. This suggests opportunities and the increasing effects of terrorist threats that are more difficultly controlled and managed. Republic of Macedonia follows the efforts of the international community in preventing and countering activities of modern terrorism. Besides participation in NATO operations for the establishment and provision of peace and security in crisis regions worldwide, national security structures have an important role in protecting national critical infrastructure. Contemporary aspects of prevention and protection in society are the basis for establishing, monitoring, detecting, preventing and managing the potential threats directed against critical infrastructure. Besides this, the paper contributes to defining the measures, activities and functions of state authorities in preventive action and combating modern terrorism aimed at social goods, critical infrastructure and security of society as a whole.

Keywords. critical infrastructure, terrorism, threats, prevention, security, risk managing

Introduction

This paper is a research of the organization and protection of system for crisis management of Republic of Macedonia, regarding the protection of critical infrastructure and the

[1] Corresponding Author: Dr. Ferdinand Odžakov, Military Service for Security and Intelligence, Ministry of Defense, Republic of Macedonia, e-mail: odzakov@hotmail.com

comparison of it with crisis management in European countries and the European Union in general. The publication gives instructions and directs experts to perception, access, prevention, legal norms, measures and activities, development and perspectives on organization and functioning of the system under the existing conditions and opportunities. The authors' basic assumptions of the research are conducted using scientific methods from different areas, gaining model that could meet the challenges, risks and threats aimed at critical infrastructure, thus improving national security. The results of the research methods and techniques, suggest the need for a combined approach to critical infrastructure protection and countering terrorism, with precisely defined measures for prevention and early detection, with rational deployment of the available forces and means of security and protection of crisis management system departmentally created primarily by government institutions, with the support of non-governmental and private organizations self-organized society entities. This paper aims to identify the security dilemmas that arise in the realization of the multi-disciplinary implementation of security measures and activities, through identifying the impact of global security events and challenges and their implications for achieving internal security policy. The model of the contemporary aspects of the critical infrastructure's protection and countering terrorism is based on positions and settings of the Constitution of the Republic of Macedonia, as well as strategic documents that guide the national security and defense, and analyzed throughout the research process.

1. "Critical infrastructure" – divergences, dilemmas and multi-discipline

The term "critical infrastructure" is basis for discussion development at many scientific conferences, expert meetings, even international governmental and non-governmental organizations. The challenge of the term complexity is challenge of time, threats, endangering and violence of security and peace worldwide. One can barely find intelligence or security assessments, reports, analysis or attempts to define terrorism, where there is no connection to infrastructure. There are many dilemmas, and it is the complexity of critical infrastructure protection that makes the problem multi-discipline. What does "critical infrastructure" mean? When approaching the problem at national level, contemporary democracies under "critical infrastructure" understand:

- Germany: organization or facilities of high importance, that if damaged would cause lack of material, disorders and other consequences [1];
- United Kingdom: assets, services and systems that support economical, political and social life of the UK, that if damaged would cause loss of lives, violation of economic stability, important consequences in social life and concerned national government [2];
- USA: systems and assets of vital importance for the USA, that if damaged would have weakening effects on security, economy, public health, or combination of the aforementioned [3];
- Netherlands: products, services and processes that if threatened or failed would cause serious social violations (casualties, economic damage etc.) [4];
- Canada: physical and information technology, assets, networks and services , that if cut or destroyed would cause serious consequences on health, security or economic well – being , and functioning on government and its institutions [5];

- Australia: physical capacities, supply chains, information technologies and communications network, that if damaged, degraded or became unavailable for use for a longer period, would substantially interfere social and economic wee-being and would cause alert for activation of national defense, in order to establish national security [6].

"Critical infrastructure" refers to networks and systems that a nation demands to function properly, and actually, figuratively stated represent economic, social, and political "backbone of the state" [7]. This critical infrastructure includes first of all electricity production systems and its transfer, water and sanitary capacities, financial systems, information networks and systems, capacities for the production and transportation of food, industrial capacities, medical facilities, not to neglect trade and transportation facilities, since they represent blood systems of a state [8].

Divergence in critical infrastructure concepts differs from many aspects, first of all from national interest, security policy objectives, security and defense development, approach towards the implementation of international interest, cooperation at bilateral and multilateral levels, etc. By defining the concept within national security institutions and their governments, they attempt identify and align national recourses that could represent critical infrastructure, or part of it. In the USA and Europe, there is tendency to differentiate systems and processes in different areas. One of the group resources that is critical infrastructure upon which societies and existence are based, refer to: financial system (including banking); energy system, telecommunications; oil and oil products (their logistics and transportation); industrial and transportation branch; governmental services and systems and emergency services systems; security and fire services [9]. Another group of resources that completes the implementation of the national interest and security policy is: agricultural sector (agriculture, water, and food), public health, chemical and other hazard substances, postal services and deliveries, supply of materials [10]. In general, the term "critical infrastructure" is used to describe assets of importance for essential functioning of a state [11].

The rapid development of information science and technology (communication and information systems and the Internet) is extremely important aspect for critical infrastructure protection). Criticality in information technology is challenge of interest in data transferring, financial transfers, electronic payments and banking, at national, regional and global level. In a time of turbulent development of information technology, more attention is paid to fourth generation threats (asymmetric threats), cyber–terrorism threats or the "infection" of computing networks with viruses to disable normal functioning and unauthorized access for use of sensitive, secret and confidential information [12].

The number of "information experts" hired for needs of terrorist, criminal organizations and intelligence services worldwide is increasing, aiming penetration in computing system of financial institutions (banks first of all) and state institution sites (ministries of interior, defense, security and intelligence services) and others.

Protection of social and economic elements of infrastructure of systems and their functions are not only important to state institutions and their installations. Security dilemmas in critical infrastructure protection may appear in private sector that enables partnership in accomplishing missions and tasks. Significant outages, damage or destruction of systems supporting critical infrastructure, may bring to huge scale consequences and damages in different zones of interest. Such crises can lead to a reduction of power inefficiency and critical infrastructure [13].

2. Impact of global changes and terrorism against critical infrastructure

It is considered that there is no society that can fully protect its infrastructure from fourth generation wars. In the US National Strategy for Physical Protection of Critical Infrastructure and Key Assets [14], new key elements are being identified and state bodies that belong to the program for infrastructure protection, including the department of national security, departments of defense and the interior, the department of energy, the department of justice and governmental agencies that implement national security policy (USA Critical Infrastructure as follows: Sector for food and agriculture 1,912,000, farms 87,000 and plantations , water supply covers 1,800 and 1,600 federal reservoirs water supply local facilities, public health concerns of 5,800 registered hospitals . The base industry, participating in defense system 250,000 companies and 215 industries, and telecommunications uses 2 billion miles different cables. The energy sector holds around 2,800 power stations and about 300,000 buildings in the area of production of oil and gas. In the area of transport there are 5,000 public airports, 120,000 miles of roads, 590,000 bridges, pipeline 2,000,000 miles, 300 ports and so on. Financial institutions cover about 26,000 institutions; insurance, chemical industry uses 66,000 facilities. National icons and monuments, total 5,800. Nuclear facilities counted about 104, with about 80,000 dams).

Guided by assessments of security threat and vulnerability, the EU in 2003 passed a security strategy which required member states to introduce crisis management systems, while in 2004 developed a strategy for critical infrastructure protection that further produced a document “Protection of critical infrastructure in combating terrorism”. This publication improved European security in the domain of prevention, preparedness and response to terrorist attacks against capacities and infrastructure of EU member states. Applying the principle that treats preventive measures as efficient to extent that provides protection to the weakest recourses [15], the EU defined critical infrastructure in terms of energy, information and communication technologies, water, food, finances, civil government, public and legal systems, security, transportation system, chemical and nuclear facilities cosmos and scientific research.

Table1. Country, facilities and strategic documents regarding infrastructure

	Country	Critical infrastructure (facilities)	Type of document
1.	USA	Energy, financial and banking system, telecommunications, gas, water supply, transportation, industry, government bodies	Strategy
2.	EU	Energy, information and communication technologies, water, food, finances, civil government, public and legal systems, security, transportation system, chemical and nuclear facilities cosmos and scientific research	Strategy
3.	Germany	Power supply, public health, food, information and communication technologies, emergency cases and rescue, transportation, government organizations, water supply, finance, insurance business, media and cultural heritage	Strategy
4.	United Kingdom	Emergency services, communications, energy sector, finance, government institutions, water, food, transportation, health	Separate strategic (sectoral) legislation
5.	Serbia	Petroleum, petroleum products and gas, water, electricity, radio active and other dangerous and hazard substances, transport, science, culture and arts, public facilities	Law on emergency situations
6.	Croatia	Critical National Infrastructure (trade, energy, communication and information systems, finance, banking system, health care, food, water), climate changes and environmental disruption	Strategy
7.	Slovenia	Economy, health, security, social welfare	Resolution

Throughout the literature, one can see that countries approach critical infrastructure protection differently. To the largest extent this depends on threat assessments and their intensity, but it also depends on state sustainable and vital interests. In Review number 1 (countries, facilities, and strategic documents), one can see that a large part of European countries and the USA, even the Balkan states, consider energy and energy system or facility/area of national interest related to economy, telecommunication systems, trade, power etc, to be object of critical infrastructure [16]. This comparative review of critical infrastructure identifies the major areas in the field of social and economic life. Basically, different approaches to the definition of critical infrastructure reveal elements belonging to the protection of vital and important interests of national security.

Global change consequences. Protection of critical infrastructure goes along with development of societies that as part of international community depend on global changes and their consequences. The last two decades have been a period of transition in many societies that came to manifest the internal and external forms of threat, and asymmetric threats (modern terrorism, extremism, organized crime, proliferation of weapons and the threat of weapons of mass destruction) and others. They caused economic and military crises in several continents and regions. As a consequence of scientific and technological development and advancement of the modern world, global changes have contributed to the dreadful disorder of planetary peace and stability and the polarization of the world. Many international governmental and non-governmental organizations, humanitarian organizations, scholars, experts and many others point out threats to critical infrastructure from natural disasters such as earthquakes, volcanoes, floods, fires, typhoons and other natural phenomena, thought to be result global disturbances caused by humans [17]. Human activity does not end with announcements of self-destruction caused by the violation of natural laws, exploitation and destruction of the environment, the ruthless exploitation of natural resources, the development of new technological breakthroughs, global development in the field of economy, industry, computer science, electrical engineering, scientific experiments, the spread of infectious diseases and so on. It emphasized a desire for economic prosperity, rapid enrichment and providing long-term life existence, the emergence of economic crimes, changing the ideological matrix, inter-cultural and mass emigration, the fragmentation of nations and ethnic groups, religious and national confrontation, corruption, urban crime, murders, and societies' criminalization [18].

The effects of globalization have led to a global economic crisis, felt most among middle-income and developing countries and regions. As a result of the slow and ineffective response to global threats and already existing regional and global crises, 5,000,000 people each year are in exile, over 600,000 people die, 10-11,000,000 become poor, about 25 million people are displaced through world for different reasons and about 5,000 people are killed each year with weapons [19], not counting the daily suicide attacks around the world, recognized as the "new face of terrorism" [20]. There are concerning findings that according Persons Peace Center [21], pointing that every 15th person in the world is in possession of illegal weapons and the younger control seniors in behavior, money, weapons and more. Global changes and developments since 2001, when U.S. security was threatened, symbolically marked the period of modern terrorism and the threats of weapons of mass destruction, as threats against critical infrastructure of countries, and new internal problems expressed in the region of the Soviet Union, Central and Eastern Europe, the crisis in the Gulf and Middle East [22].

The impact of terrorism on critical infrastructure. Internal problems of societies are influenced by many factors such as poverty; economic stagnation; the unequal distribution of resources; discrimination; oppression of smaller ethnic groups; refugee crises; social injustice and other [23]. Such systems' dissolution, dragged backwards certain countries, which on other hand generates larger volumes of crises, and the idea of global terrorism gets their potential allies in terms of recruiting people for terrorism, terrorist logistics, facilitating transit through certain areas, funding paramilitary formations and so on, by which weakened regions allowed separatist movements to get growing. Terrorism has not only become a serious threat, but contributed to the emergence of new challenges and threats. It is estimated that a large percentage of the transition countries in Southeast Europe does not fully control its territories, allowing exactly those areas to carry out activities in support of terrorism (preparation for firing, illegal border crossing, creating corridors and routes, smuggling of people, drugs and weapons, and others).

Certain forms of terrorism (blackmail, attacks, abductions, organized crime, murder, arson, suicide attacks), result from the practice of "aristocratic rule," which is associated with corrupted behavior by disabling or avoiding acceptance of democratic processes and observance of fundamental human rights without respecting the basic principles of civil society. This becomes a recognizable and synonymous way of maintaining their own positions. Ineffective governance is still the main culprit for inducing affairs, spreading misinformation, misjudgment, conspiracy against individuals or groups, the support of individuals and criminal uncontrolled armed groups and even paramilitary formations. Thearistocratic mode of operation affects the creation of "controlled instability" in order to accomplish its goals, creating profit, obtaining wealth and utilization of their own position.

One of the goals of modern terrorism is the desire to create new (one-nation-states). Armed forces sometimes are used not to disable a potential opponent, but to crowd people into a state or the region [24]. In this context, the impact of terrorism on the development of certain regions brings to divergences in the behavior of religions, and acceptance of extreme behavior. Terrorism as deviance is dispersed in various directions, with or without the possibility of his opposition. The cconnection of terrorism with threats from the proliferation of weapons of mass destruction is the greatest threat to the world and challenge for national and collective security systems. The presence of suspected weapons is mostly with unconfirmed origin. It is often pointed out that the black market offers the most sophisticated military equipment and material and technical devices with origin and characteristics of world class manufacturers. Revolution in military potential "gains importance," with the rapid expansion of the desire of possessing weapons, which in turn reduces safety and peace. Thus enabling the creation and support of armed conflicts feeling threat to their own survival. Threats come from the desire for appropriation of territories "taking destiny into their own hands", motivated by nationalistic motives, the desire for "proof" and many worldwide unacceptable and insufficiently explained reasons.

The international community sometimes loses the connection and collaboration with the limited capabilities of government institutions, as a result of the activities of the criminal-terrorist organizations and groups [25]. In all this untimely intervention leads to the emergence of the law of force, weapons, theory of groups, social-sociological syndrome and loss of consciousness, degradation of state mechanisms, losing confidence, continuing with "business" smuggling of arms, drugs, people and alike. The wide range of current and political crises at the global level is a risk or threat to initiate a larger war. Military conflicts and crises around the world create lasting regional crises with uncertainty over the possible consequences. The new millennium is marked by bloodshed and the international community requires appropriate solutions.

3. »Critical infrastructure« in the national documents of the Republic of Macedonia

Assessments of states' national security come from various forms of threat (internal, external, armed, unarmed, and combined) and are aided by political, security, economic, social, environmental, military, educational and other reasons. Threats to critical infrastructure, impacts or consequences are derived from a position of strength, combined with other actions, potentially disturbing the peace and safety. Determining the critical infrastructure is regulated differently in different states. Republic of Macedonia in several strategic documents, laws and regulations, specifies the subjects, objects, processes and infrastructure important to national security.

The Concept of National Security and Defense of the Republic of Macedonia is a strategic document that implements the basics of the Constitution of Republic of Macedonia [26], defines the purposes of managing national security policy, and implements the provisions of the documents and settings that treat areas of security and defense [27]. Through defining the objectives of the National Security Policy, the National Concept on Security and Defense, defines interests, highlighting permanent as most important, by protecting sovereignty, territorial integrity and safeguarding the independence of the Republic of Macedonia.

The protection of "vital infrastructure" and the resources of the Republic of Macedonia are part of the vital interests that develop the security situation and create better living conditions for the citizens, the state and society. The importance of critical infrastructure protection is present through other settings of the National Concept on Security and Defense in the area of vital interests, especially in the protection and promotion of peace and security, life, health, property and personal safety of the citizens of the Republic of Macedonia.

Important interests determined in this strategic document give a clear commitment of the Republic of Macedonia to critical infrastructure protection, through the realization of security and development of the country and its neighbors, the preservation and promotion of peace and security in Southeast Europe, the prevention and building of instruments for the early warning of tensions and crises, providing conditions for internal political stability, improving security awareness, the conservation and protection of environment in cooperation with the environment.

Security features are important for the critical infrastructure of the Republic of Macedonia, defined by the concept of National Security and Defense, and are seen in increasing opportunities and capacities for prevention and crisis management, participation in the Euro-Atlantic security structures, regional cooperation in order to improve the security situation, political and economic stability and progress, promotion of scientific, scientific-technological and infrastructural base of the country, creating the conditions for use of own resources of the state for the purpose of security and defense.

Republic of Macedonia identifies risks and threats that can adversely affect the protection of critical infrastructure including: extreme nationalism, racial and religious intolerance, terrorism, organized crime, migration, trafficking in drugs, people and weapons, transition issues, activities of foreign intelligence services, the emergence of cyber-crime and abuse of information technology, degradation and destruction of the environment. Of course, the critical infrastructure in the country can be threatened by elementary and other disasters, technical and technological disasters, infectious diseases and so on.

The Defense White Paper is an overview of the strategic orientation of the Republic of Macedonia in terms of building a system for national security and defense of the Republic of Macedonia. The settings in the document define key segments in terms of performing security and defense functions that relate to demonstrating the importance of inter-institutional cooperation and coordination to achieve better security; the indication of the capacities and capabilities of the Macedonian Army (ARM); having appropriate facilities and capabilities and emphasizing the commitment of the country to undertake all obligations and responsibilities arising from membership in NATO and the EU. Regarding the protection of critical infrastructure, the Defense White Paper sets conditions for the realization of the vital interests through strengthening the internal security of the state as a precondition for sustainable political, economic and social development, and implementation of effective tools and methods for collecting data and information vital to the security; quality expert analysis of the security environment and effective international cooperation; dealing with transnational organized crime in all its forms, terrorism and corruption.

The long-term plan on development and defense is a document that traces the vision for the development of the defense policy of the Republic of Macedonia. The long-term plan defines the development goals of defense including: the modernization of defense capabilities for command, control, communications, computers and intelligence (C4I); contribution to the Common Security and Defense Policy; the adjustment and improvement of training to meet the missions, goals and objectives of the Army and improve defense infrastructure [28]. The achievement of these goals will ensure the protection of national interests.

Law on crisis management is the regulation that governs the system for crisis management in the Republic of Macedonia in the organization and functioning; decision-making and the use of resources; communication, coordination and cooperation; assessment of threats to the security of the Republic of Macedonia; planning and financing and other issue in the field of crisis management. The ssystem for crisis management is organized and performed for prevention, early warning and dealing with crisis situations and humanitarian disasters caused by hazards and risks to the security of the Republic Macedonia [29]. The law defines several terms that have a critical impact to infrastructure including "threat to the security of the Republic of Macedonia", "risks and dangers", "resources", "crisis", "crisis situation" [30].

National Platform of Republic of Macedonia to reduce the risks of accidents and disasters is a document based on the Framework for Action Hyogo 2005, which prescribes the mechanism for initial networking of subjects of importance to the prevention and dealing with accidents and disasters and it established cooperation among all stakeholders in the country of importance for crisis management. By March 2009, memorandums of cooperation were signed with all ministries, administrative bodies, local authorities, public utilities and public services, NGOs, academic institutions, universities, research centers and laboratories, the business community and religious communities. As a result, the National Network of Laboratories and the National Expert Network were established as part of National platform. In the period January-March 2010 the process of establishing seven separate platforms that make up the National platform was completed. A special part of National Platform imposes to three separate platforms (for security risks against terrorism, organized crime and proliferation, economic crises and risks and financial risks and crises).

Facilities and areas of importance to the defense are determined by ***Decision of the Government of Republic of Macedonia*** [31]. As objects of particular interest are considered facilities and zones that are specially arranged for needs of defense or requires their arrangement, the disclosure of which could have harmful consequences for the defense and security of the country and its citizens. Facilities and zones of special importance are: organs of state authority for accommodation and work in a state of war; operation of radio-television network in state of war; storage of material reserves to supply the armed forces; operations and production of weapons and military equipment; the dispersion and displacement of cultural and historical monuments and treasures, gold, money and securities; the needs of the Army of Republic of Macedonia.

4. Confronting terrorism as a threat against critical infrastructure

Republic of Macedonia in the 21st century is facing completely new challenges. The National Concept on Security and defense provides that threats to its sovereignty and integrity are mostly unconventional. In other words, terrorism is the most constant, real and serious threat that jeopardizes peace and security of the state. The current situation in the country does not indicate safety indicators for possible endangerment of individual acts of terrorism. But we must emphasize that there are still certain criminal groups operating in northern and northwestern parts of its territory. Also, we cannot forget the fact that there are certain groups with low level (for now) of religious radicalism. Despite the limited activities of these groups, they pose a potential threat to security and stability. Macedonia is a transit zone, and also an area for the possible recruitment of prospective members/members of terrorist organizations and groups. And, most important of all is that Macedonia is one of the most active members of the international anti-terrorist coalition, which makes it a possible target of radical religious groups for terrorist attacks on institutions, citizens or interests of the Republic of Macedonia, in and out of the country. Having In mind the favorable geographical position of states on the Balkan Peninsula, which make a kind crossing between three continents (Europe, Asia and Africa), they represent a kind of way in and out gate in this part of the world. That is the reason that determines our region as a natural crossroads and transit corridor where Macedonia has a strategic position.

Macedonia in combating terrorism. It is known that there is a significant relationship and interweaving of terrorist and criminal structures, especially in terms of providing funds for terrorist activities. Terrorist groups use networks and structure of organized crime to provide or fund its terrorist activities. Organized crime groups favor a state of disruption in functioning of the institutions in the system, allowing them to smoothly accomplish their goals. Realizing the danger of the symbiosis that exists between terrorism and organized crime (especially in terms of financial benefit that terrorists and criminals have), we come to a conclusion is that if we want the successful prevention against these two modern threats, it is necessary to prevent the flow of funds to terrorist activities in the country. Also, changes in the legislative regulation provided sanctions for financing of terrorism. In accordance with the legal definition, financing terrorism [32] is the provision or collection of funds in any way, directly or indirectly, unlawfully and knowingly, with the intent that they be used or in the knowledge that they will be used wholly or partly for the purpose of committing a crime hijacking an aircraft (Article 302), endangering the safety of air traffic (Article 303), terrorist threat to the constitutional order (Article 313), a terrorist organization (Article 394-a), terrorism (394-b), a crime against humanity (Article 403-a), international terrorism (Article 419), taking hostages (Article 421) and other act of homicide or serious bodily injury caused to create a sense of insecurity and fear with people. The mmultidimensional problem of terrorism and its financing necessarily presupposes multidimensional access in its address. In this sense, Republic of Macedonia directs its activity on two fronts: taking legislative measures that suit altered circumstances; measures and activities of state organs within established powers.

Legislative measures. In Republic of Macedonia there is still no specific law on terrorism. However, the existing legislation relating to this area provides sufficient basis for successful combat against terrorism. Macedonia up to now has taken actions aimed at supplementing and harmonization of legislation with the relevant regulations of the European Union. In terms of changes to the legislation, which in a certain way have impact on the further building of the legal mechanisms to combat terrorism in all its manifestations, we should indicate the adoption of some regulations. With the adoption of the amendment to the Criminal Code [33], which with the proper substitution of forms "terrorist threat to the constitutional order" in Article 313, "terrorist organization" under Article 394-A, “Terrorism “Article 394-B, and standardization of a new crime of” terrorism financing “of Article 394-B, together with the existing provisions of the Criminal Code, to provide the legal framework for sanctioning all forms of modern terrorism, and at the same time is thecompliance of national legislation with EU regulations and requirements arising from international agreements. These changes mean the harmonization of legislation of the Republic of Macedonia to the Framework Decision on combating terrorism in the Council of Europe. In this respect, the amendments made to the Criminal Code of the Republic of Macedonia with already existing regulations implement the obligations relating to the harmonization of national legislation. The new Law on the Prevention of Money Laundering and Proceeds from crime and financing terrorism [34] identifies the need for a more energetic and intensified struggle in view of preventing terrorism financing. In terms of countering terrorism as a form of threat to critical infrastructure, it is important to mention the passing of the Law on monitoring communications, which regulated the conditions and procedures for the interception of communications in order to prevent or detect a crime, for purpose of a criminal investigation or when needed for interests of security and defense [35]. This set is a very important legal mechanism in the area of prevention of terrorist activities and terrorist threats. The amendments to the Act of 2008, overcame the problems and inconsistencies that were observed during its implementation in order to facilitate effective implementation.

5. Authorities and measures to combat terrorism

Directorate for Security and Counterintelligence (UBK). UBK is one of the main leaders of the fight against terrorism and organized crime in the country. In accordance with the Law on Internal Affairs of 2009, Article 15 and Article 24, under the Ministry of Interior there is Directorate for Security and Counterintelligence (UBK), as one of the key areas of organization in the Ministry of Interior (MVR) [36]. Under that Law of Interior, UBK is responsible for research, prevention and surveillance of all violent acts aimed to undermine the constitutionally-fixed state order of the Republic of Macedonia, and especially to prevent terrorist activities and of organized crime, counterintelligence activity, and other attacks on democratic institutions of the Republic of Macedonia. UBK claims through constant activity and the building of their professional structure to raise its operational capability and also to respond to any threats regarding the security of the Republic of Macedonia, especially when it comes to the threat of terrorism. The convergence of several different aspects of confronting and combating terrorism, or operational activity and anti-terrorist protection within the UBK (as a body within the Ministry of Interior) and the ability to quickly and effectively use the capacity of special forces units of the Interior Ministry to conduct special actions in case of terrorist attacks, allows for a quick and efficient response to security authorities in countering terrorist attacks.

Intelligence Agency. The Intelligence Agency, as a specialized intelligence institution within the state administration, was established under the Law on Intelligence Agency from 1995 [37]. The Intelligence Agency works closely with the Ministry of Defense and the Ministry of Interior. In accordance with Article 2 of the Intelligence Agency, which entered into force in 1995, the Agency is authorized “to collect data and information relevant to the security and defense of the Republic of Macedonia and the economic, political and other interests of the state.” The Agency performs research and analysis of data and information referred to in paragraph 1 of this article (concerning security and defense of the state and the most important state interests, and must notify the President of the Republic of Macedonia, the Government and other public bodies on issues of importance to their scope). The aagency cooperates with the other two pillars of the security and intelligence system of the Republic of Macedonia on a daily basis, UBK in MVR and the Military Service for Security and Intelligence (VSBiR) in the Ministry of Defense. Within the Intelligence Agency, there is the Intelligence Directorate for international terrorism and organized crime. In accordance with its responsibilities, the Intelligence Agency collects, documents and analyzes intelligence information relevant to the security and defense of the Republic, as well as economic, political and other interests of the state. Terrorism and organized crime are threats (unconventional, asymmetrical), that nowadays pose serious threats to the national interests of many powerful countries as Macedonia.

Military Service for Security and Intelligence. The Military Service for Security and Intelligence (VSBiR) is one of the key organizational units within the Ministry of Defense. VSBiR unites as separate components - security (where counterintelligence is dominant activity) and intelligence. VSBiR legal competences are defined in Law on Defense, published in the Official Gazette of the Republic of Macedonia no.58/06 from 11.05.2006. These competencies are covered in detail in Chapter XI of the Law, starting with Article 133, to Article 141. Article 133 of this Law, "intelligence covers measures, procedures and activities undertaken for collection, documentation and analysis intelligence important for the defense of the Republic." Paragraph 2 of the same Article (133) states that work in the previous paragraph shall be performed by authorized officials of the Ministry of Defense designated by the Minister of Defense. Given the fact that conditions are significantly changed or rather the socio-political landscape of the region in which the Republic of Macedonia occupies a central position, gathering intelligence from the immediate environment (neighboring countries) is no longer the primary task of the intelligence services of the Republic of Macedonia, regardless of whether it is the Intelligence Agency or Military Service for Security and Intelligence. In accordance with Article 134 of the Law on Defense of the Republic of Macedonia, "counterintelligence covers measures, actions and procedures taken for the detection and prevention of all forms of terrorist activity aimed at the defense of the Republic.

Ministry of Interior. In accordance with Article 2 of the Law on Internal Affairs (Official Gazette, no. 92 from 24.07.2009), the scope of work of the Ministry of Interior includes: performing the system of public and state security; preventing undermining of democratic institutions established by the Constitution of the Republic of Macedonia; protect the life, personal safety and property of citizens; prevention of incitement to national, racial or religious hatred and intolerance and others.

Directorate for Financial Intelligence. The Financial Intelligence (formerly the Directorate for the Prevention of Money Laundering and until February 2012 the Directorate for Prevention of Money Laundering and Terrorism Financing) for the first time began to exist in March 2002. The establishment of such a specialized institution is done immediately after a legal issue was regulated to prevent money laundering by adopting the Law on the Prevention of Money Laundering in August 2001. The main objective of this institution is the financial monitoring, i.e. monitoring of money and preventing the financing of terrorism. In January 2008, the institution was granted the status of a legal entity within the Ministry of Finance of the Republic of Macedonia, and changed its name from the Directorate for Prevention of Money Laundering to Directorate for Prevention of Money Laundering and Financing terrorism. The Directorate functions as an administrative model of the Financial Intelligence Unit (FIU). This type of FIU acts as an intermediary between the private sector, on the one hand and law enforcement on the other. Simply said, it functions as a body that proves the trust upon which responsible entities submit their classified information [38].

Directorate for Financial Police. The Financial Police is a body within the Ministry of Finance of the Republic of Macedonia as a legal entity. Established on June 26, 2003 by Law on Financial Police [39]. This Directorate has its special powers according to the Criminal Procedure Code, and ensures the consistent application of regulations, particularly in the area of financial, tax and customs work [40]. The new Law on Financial Police precisely defines the responsibilities and powers of the Financial Police in the detection and prosecution of complex forms of organized financial crime in the Republic of Macedonia.

6. Cooperation at the national level

In order to be successful in combating terrorism, cooperation is required between all state organs and institutions in our country that have responsibilities in this area. In terms of cooperation between the three security-intelligence services (UBK, AR and VSBiR), it is primarily the result of »lessons learned« from the well-known events of 2001 and the events of September 11, 2001 in the United States. The good, continuous and complete cooperation among all institutions that make up the security-intelligence apparatus at the national, regional and global levels, ensure success in the fight against terrorism and organized crime. For this cooperation to be more successful, not only these three institutions (UBK, AR and VSBiR) must cooperate at the bilateral and multilateral level, but each of them is necessary to have cooperation with Customs and the Financial Intelligence in Ministry of Finance. The fruitful cooperation between the Ministry of Interior and the Ministry of Finance (in particular Customs Directorate and the Financial Intelligence) on its course finds the obligations arising from the Law on prevention of Money Laundering and Proceeds of Crime and Terrorism Financing. This cooperation was formalized with the signing of the Memorandum of Understanding and Cooperation and the Protocol on cooperation and understanding, which greatly facilitated the exchange of information and conducting joint actions between Ministry of Interior and the two mentioned Directorates of the Ministry of Finance. The Military Service for Security and Intelligence, as an organizational unit of the Ministry of Defense at national level, in 2009 signed a memorandum of cooperation with the Public Security Bureau in the Ministry of Interior, and with Directorate for Financial Intelligence (at that time Directorate for prevention of money laundering and financing of terrorism) in the Ministry of Finance. Certainly VSBiR so far had very good cooperation with these two institutions, but by signing this memorandum, the cooperation received additional quality.

The aim of the above mentioned is, by daily and regular communication of institutions that have specific responsibilities in combating terrorism and organized crime, and adequate exchange of information in this area, to act in a preventive manner in order to avoid what happened on 11 September 2001, and was a result of insufficient communication within the security and intelligence community of the United States.

7. Conclusions

Commitment to democratic development has prompted a number of newly created States to accede to the collective security systems, alliances or regional unification. The recent history of many Balkan countries shows that the cost of security depends on the importance of history and geopolitical position and without this knowledge the Balkan world cannot be understood [41]. The inevitability of the need to modernize the national security services is a result of the enhanced occurrence of terrorism and asymmetric threats, the use of outdated security techniques, global, slow and ineffective security apparatus, the incompatibility of modern challenges, slowness of scientific thought, research and research technologies, inefficient organizational and formational structure of the security and defense systems, and the world is still feeling the effects of shifting security structures [42]. Countries in transition still feel transitional problems such as corruption, urban terrorism, serious crime, blackmail, racketeering, murder, economic crimes, etc., that we can say to apply to security environment and space of the Republic of Macedonia.

Clearly determined transformed states of Central and Eastern Europe that accepted concepts of participation in collective security systems began implementation of the policy for the full Euro-Atlantic orientation of security systems. The presence and influence of NATO in the region of the "new" member states of NATO, contribute to achieving the necessary security processes. The need and essence of equal security contributes to overall stability in Europe and creating conditions for increased cooperation with other countries. Expanding cooperation between the member states of NATO contributed to stability in Europe and increased cooperation towards building a common political, economic, social and cultural destiny. The pprotection of critical infrastructure is an important segment for achieving national security, and lack of appropriate security treatment, measures and activities, could not provide the smooth functioning of government, the private and public sector and society in general. Terrorism is an act of violence which is a form of threaten to national security. The seriousness of the threat is the fact that the security institutions of the international community and collective security systems are not fully able to see, discover, hinder its implementation and threat. The mmanifestations of threats and hazards, remind us of the obligations to protect the critical infrastructure that EU countries have identified and established in national strategies, documents and laws.

Republic of Macedonia follows the efforts of the international community in combatting terrorism, but there is a need for continuous definition of critical infrastructure, according to the guidelines of the European Union in order to perceive, change and harmonize national documents regarding threat assessments, identifying threats and measures and activities for appropriate countering. In this context, we are to mention the significant efforts of the state authorities to establish a coherent system for crisis management, in which an important place and role despite the measures and activities for protection against natural disasters, accidents and catastrophes will have security challenges and especially asymmetric threats.

The contribution of the research in the paper determines threats and risks, authorities and services, documents, laws and their interaction in the process of the implementation of critical infrastructure protection and specificities in early detection, prevention and countering of terrorism in the Republic of Macedonia. Of course, there are no absolute models which can guarantee security and full realization of national interests through the protection of critical infrastructure. Pointing to the necessity of determining the next steps, the authors propose the following:

- Adoption of the Law on the protection of critical infrastructure, allowing adjustment of the national subsystem to protect and rescue the European system for the protection of critical infrastructure, and critical infrastructure protection of the European Union,
- Completion of the »National Platform of Macedonia to reduce the risks of accidents and disasters,« Document based on Framework for Action Hyogo 2005, which stipulates mechanisms for initial networking of subjects of importance to prevent and deal with disasters and catastrophes, in which cooperation was established between all stakeholders in the country of importance for crisis management. In this section there is a need to prepare sub-platforms for security risks from terrorism, organized crime and proliferation; economic crises and risks and financial risks and crises.
- Determining institution at the national level that will see the system for crisis management (including critical infrastructure protection), that will coordinately propose measures and activities to overcome the identified weaknesses and limitations, and will bring closer the model to collective security systems towards which Republic of Macedonia is aiming.

An important role in strengthening the crisis management system, especially in the area of critical infrastructure protection, will be given by the private sector (private military and security companies), who would have to participate respective capabilities, their role, importance and support of national security systems.

The accomplishments and perspectives of »critical infrastructure protection« lie in the respective development, placement and organization of state institutions responsible for the implementation of security measures and activities, as well as professional security authorities. The creation of a modern model is reduction of risks and threats and eliminating the possible in coordination at national level. Reality in Republic of Macedonia confirms that institutions can contribute to the complete elimination of possible challenges, threats and risks in the area of critical infrastructure protection, as seen in the proposals of the authors. The application of such perceptions and management in critical infrastructure protection will enable achieving European standards and norms and stepping closer to collective security systems.

References

[1] Federal Office for Information Security - Germany *“Critical Infrastructure Protection in Germany“,* (www.bsi.de/english/topics/kritis/KRITIS_in_Germany.pdf)

[2] United Kingdom Home Office Security, “*Counter Terrorism Strategy: Protecting the Critical National Infrastructure”* (www.security.homeoffice.gov.uk).

[3] Department of Homeland (2006),*“National Infrastructure Protection Plan*” (www.dhs.gov)

[4] Ministry of the Interior (September 2005), *“Report on Critical Infrastructure protection”,*

[5] Public Safety Canada, January (2008), *“About Critical Infrastructure“* (www.ps-sp.gc.ca)

[6] Australian National Security, (May 2007), *“What is critical infrastructure?”*. (www.ag.gov.au/agd)

[7] T. R. Mockaitis, (2006) “*The NewTerrorism: Myths and Reality”, Praeger Security International, Westport, Connecticut*-London,

[8] F Odzakov, (2011)*„Intelligence services in combating terrorism and organized crime“,* Solaris Print, Skopje,

[9] Moteff, J. (2005).*Risk Management and Critical Infrastructure Protection: Assesing, Integrating and Managing Threats, Vulnerabilities and Consequences, Report for Congress. Resources, Science and Industry Division,* Congressional Research Service

[10] Radvanovsky, R., (2006), *Critical Infrastructure (Homeland Security and Emergency Preparedness).* New York: Taylor & Francis Group

[11] http://en.wikipedia.org/wiki/Critical_infrastructure

[12] Thomas R. Mockaitis, (2006), "*The New" Terrorism: Myths and Reality"*, Praeger Security International, Westport, Connecticut-London,

[13] Vladimir J., Jasmina G. (2012) „*Protection of critical infrastructure in crises*", International scientific conference, „Management 2012", Mladenovac, Serbija,

[14] White House, (2003)*„National Strategy for critical infrastructure protection* "

[15] Boin, A., Rhinhard, M., Prezelj, I., *et al*., (2005), Shocks without Frontiers – Transnational Breakdowns and Critical Incidents: What Role for the EU?, *European Policy Center Issue Paper, 42,* Brussels

[16] Z. Kesetovic, N. Putnik, M. Rakic, (2013)*„Possibilites of improving critical infrastructure pretection in countries in transition",* Faculty of security studies, Belgrade,

[17] S. Mijalkovic, V. Cvetkovic, (2013)*„Vulnerability of critical infrastructure by natural disasters",* Faculty of security, Belgrade,

[18] M. Dojcinovski, D. Petreski, (2010) Security, Ecologic Security and Challenges in RM *,"Globalization Processes and security impact in SE Europe",* Ohrid,

[19] http:/www.peaceoperations.org

[20] http:/www.cdnpecekeeping.ns.ca

[21] http://www. Jura.uni-frankfurt.de/INPE/links.htm

[22] NATO, (2001), Ofice of information and Press, Brussels

[23] T. Gocevski , O. Bakreski, S. Slaveski, (2007), " *European Union through prism of European Security",* Faculty of Phylosophy, Skopje

[24] V. Vasilevski, (2002), "*International Humanitarian Law", Military Academy "General Mihajlo Apostolski* " Skopje

[25] T. Moctaitis, (2005), "Al Qaeda: A global Insurgency?, CCMR/NPS, DePaul University

[26] Assembly of RM (1991), *"Constitution of RM",* Skopje

[27] Ministry of Defense, *"White Book of Defense",* Skopje 2012

[28] Government of R.Macedonia, *(2011), "Long –term plan for development and defense"*, Skopje

[29] Assembly of RM "Law on Crisis Management", Skopje, 2005

[30] Crisis Management Center, (2010),"*National Platform of Republic of Macedonia for decreasing accidents and catastrophe",* Skopje

[31] Government of the Republic of Macedonia, (2003),*"Decision for determining facilities and zones of importance for defense",* Official Gazette of RM no. 83, Skopje,

[32] Criminal Code of the Republic of Macedonia, Official Gazette n.37/96, 80/99, 4/2002,and Decision of the Constitutional Court of the Republic of Macedonia, Official Gazette n.48/01 and Official Gazette of RM, no. 7/2008

[33] Official Gazette of RM no. 7/2008

[34] Official Gazette of RM no. 4/2008

[35] Official Gazette of RM no .121/2006

[36] Official Gazette of RM, no. 92 09

[37] Official Gazette of RM no. 19/1995

[38] www.usppft.gov.mk

[39] Official Gazette of RM PM, no.55 од 16 July 2002

[40] www.finance.gov.mk

[41] M. Kotovcevski, (2007), "*Secret Services on the Balkans",* Bomat Grafiks, Skopje

[42] M. Dojcinovski, (2009), "*Contemporary Military Intelligence"*, Solaris Print , Skopje

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015

© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-19

Corruption: From Generally Accepted Business Practice to Serious Threat to Critical Infrastructure Protection

Jaka VADNJAL[1]
GEA College – Faculty for Entrepreneurship, Ljubljana, Slovenia

Abstract. The dimeansions of global business acting together with the broad issue of cultural differentiation suggest that there may be no standardized answer as to whether corruption is necessarily bad for a national economy or if, on the contrary, it can even be found to inhibit economic growth to a certain level. However, there is no doubt it has been agreed that corruption as such is an example of unethical behavior. As such, also its impact on the possible disruption of the critical infrastructure may not be clearly identified. This paper, based on the theoretical grounds and findings of other researchers, aims to embed the question of corruptive business practices and behavior within the different frameworks and scopes of business dealing with public and critical infrastructure. Leaning on the findings from different pieces of investigation from around the world it finally concludes that there is no dichotomous solution to the dilemma whether a certain level of corruptive practices, when they are an integral part of a national business environment, would necessarily be bad for future economic growth.

Keywords. corruption, critical infrastructure, economic growth, economic development, ethical standards

Introduction

There is widespread agreement that corruption has become one of today's most pressing economic problems [1]. Corruption distorts standards of merit and erodes the respect of law, resulting in higher public spending and increased cost and a lower quality of infrastructure. Corruption is thus one aspect of governance which also relates to matters of transparency, accountability, political stability, social order, the rule of law and the like [2]. These factors are likely to be interdependent [3]. Corruption has a significant impact on the growth rate of real per capita income [4]. The most important channel through which corruption influences economic growth is political instability. Corruption reduces the level of human capital and the share of private investment [5]. It has an additional negative impact on growth independently from its impact on investment [6].

In a broad definition, managing and leading can be regarded as ethically driven tasks because every managerial decision affects either people or the natural environment and society. Those effects or impacts need to be taken into consideration when decisions are made. A narrower construction of the role of the manager is that managers should serve only the interests of the shareholder. Their only task is to maximize shareholder wealth. That point of view is increasingly accepted in some parts of the world where capitalism is accepted as the economic framework [7].

[1] Corresponding Author: Dr. Jaka Vadnjal, GEA College – Faculty of Entrepreneursip, Dunajska 156, 1000 Ljubljana, Slovenia, e-mail: jaka.vadnjal@gea-college.si

Governmental corruption is a pervasive element of the international business environment and has damaging effects on governments, companies, and the whole society where it takes place. However, the impact of governmental corruption on foreign investment has so far received limited attention both in trials of legal investigations and pieces of academic research. There has been an ongoing debate how multinational firms respond to corruption when investing in foreign markets. There are direct and indirect costs of corruption to business and there is corruption's impact on firms that invest or still are in the decision-making process for investments in foreign markets. Corruption involves costs that firms investing abroad are likely to misjudge or ignore. A clear understanding of corruption's nature creates value for decision makers and allows for a strategic analysis of responses to corruption pressures [8].

The main objective of the chapter is to compile an overview of the research which has been in progress in order to evaluate the negative impact and influence of the corruptive malpractices in the processes of designing, developing, building and maintaining critical infrastructure. The main theoretical and ideological framework for assessing the corruptive behavior of managers and other decision-makers is based on the paradigm of business ethics with its own written codes and individual human beings' standards, values and virtues. The main proposition of the present study, which is assessed mainly through the methodology of compilation and synthesis, goes as follows: Corruption which may be observed as a direct consequence of the unethical behavior of managers and other (also political) decision-makers impose a substantially direct and indirect social cost which seriously decreases the general welfare of a particular economy.

1. Decision-making frameworks of the critical infrastructure

Disruptions to critical national infrastructures (e.g., power, telecom, transportation, and emergency services) are an area of increasing national concern. Each of the infrastructures is highly dependent on telecommunications and each of the infrastructures is subject to disruptions, examples of which are shown in Table 1.

Table 1. Typical disruptions to critical infrastructure

Critical infrastructure	Typical disruptions
Telecommunications	Disruption of key communications nodes by fire, wind, water, or external sabotage
Power (electricity, gas)	Blackouts caused by insufficient generation to meet demand, transmission bottlenecks, or equipment outages
Emergency services	Demand greater than response capacity, as during a disaster
Water supply	Contamination with toxic substances
Agriculture and food	Contamination of food supply
Chemical industry	Explosions, release of toxic gas clouds
Defense industry	Supply line interruptions
Banking and finance	Disruption to electronic payment systems that cause bank liquidity problems
Public health	Infectious diseases
Government	Disruptions in operation

The critical infrastructure is a complex "system of systems." The interdependencies are generally not well understood and disruptions in one infrastructure can spread into other infrastructures. Infrastructure studies are becoming more and more prevalent. Risk-informed decisions are needed to help identify investment strategies and other options that best reduce overall risk [9]. Decisions almost always involve ethical considerations. A moral decision-making person sticks to her or his core values, tries to be objective and fair, has concerns for society and the welfare of everybody involved, and follows the rules of ethical decision-making. A manager should serve as a role model for other employees in all of his or her duties. Rewards and discipline concerning the ethical and unethical decisions made by others should be provided, so that a clear message is sent about which behaviors are and are not acceptable in the organization or in different situations [10]. Thus, it is very crucial to include the highest level of conduct in the matters connected with decision-making regarding the critical infrastructure because every other mode of behavior directly contributes to a higher level of risk.

The importance of social trust has been generally accepted in the social sciences. As surveyed on several occasions, it correlates with a number of other variables that are in most cases very much desirable. People who usually believe that most other people can be trusted are also more committed (i) to having a positive opinion about their democratic institutions, (ii) to participating more actively in politics, and (iii) to being more proactive in civic organizations. They give more attention and contribution to charity and are much more tolerant of people who think differently and are not like themselves. People who trust also tend to be more optimistic about their own ability to influence their own life chances and to be happier with their lives [11]. Thus, a well operating critical infrastructure would directly contribute to the level of social trust in a society.

Managers face difficult situations on a daily basis while doing their jobs. Since management decisions almost always involve ethical considerations, it is important that they recognize the ethical elements that are embedded in their day-to-day job functions. Many times, situations involve issues that are clearly right or wrong when judged by the managers' or organization's values or code of conduct. Furthermore, most managerial decisions and actions are legal, although there are occasions when a certain decision would clearly go beyond legal boundaries and be illegal. In these cases, making a decision to break the law or to do something that disagrees with a code of conduct or set of values is clearly unethical and increases the level of risk [7].

An example of such practice is facilitating payments. The use of facilitating payments is a very common form of corruption and an excellent example of a dilemma in ethical decision-making. These consist of small payments or gifts made to a person, in most cases paid or given to a public official or an employee of a state-owned company, to obtain a favor, such as speeding up an administrative process, obtaining a permit, license or service, or avoiding an abuse of power. Public opinion very often tends to tolerate such payments and regards it as a part of the system that somehow does function. They are assumed to be unavoidable and are excused with low wages and a lack of professionalism among public employees and a general disorder in government offices. Many companies see these payments as the grease that makes the wheels of the bureaucratic machine turn more smoothly and are even calculated in project costs. Despite this, facilitating payments have a negative effect on the working of public and private administrations. All too often they progress to more serious forms of corruption. They impose additional costs on companies and citizens and, therefore, the entire society [12].

Political competition and the achieved level of democracy have an impact on the density and intensity of corruption, which is typically lower in dictatorships than in countries that have partial democracy. But once they pass a certain threshold, democratic practices inhibit corruption. Government size does not systematically affect the corruption which is more evident in low-income countries which tend to underpay public sector employees who then take their rights in their own hands and provide their additional income through corrupt activities [13].

The most devastating forms of corruption include the diversion and outright theft of funds for public programs and the damage caused by firms and individuals that pay bribes to avoid health and safety regulations intended to benefit the public. A conservative estimate is that the former President of Zaire, Mobutu Sese Seko, looted the treasury of some $5 billion, an amount equal to the country's entire external debt at the time he was ousted in 1997. The funds allegedly embezzled by the former presidents of Indonesia and the Philippines, Mohamed Suharto and Ferdinand Marcos, are estimated to be two and seven times higher. In the Goldenberg scam in Kenya in the early 1990s, the Goldenberg firm received as much as $1 billion from the government as part of an export compensation scheme for the fictitious exports of commodities of which Kenya either produced little (gold) or nothing at all (diamonds). Nearly $1 billion of oil revenues, or $77 per capita, vanished from Angolan state coffers in 2001 alone. This amount was about three times the value of the humanitarian aid received by Angola in 2001—a country where three-quarters of the population survives on less than $1 a day and where one in three children dies before the age of five. In Turkey, the effect of the earthquake that took thousands of lives in 2004 would have been much less severe, according to the government of Turkey, if contractors had not been able to pay bribes to build homes with substandard materials. Extrapolating from firm and household survey data, the World Bank Institute estimates that total bribes in a year are about $1 trillion. While the margin of error in this estimate is large, anything of even that general magnitude ($1 trillion was about 3 percent of world GDP in 2004) would qualify as an enormous issue [14].

2. Corruption through principles of business ethics

The extent of use of the three principles of ethics: utility, morality, and justice in managerial ethical decision-making is subject to quite extensive research. Morality tends to be the most used ethical principle. Utility is the least used. There are also expected relations between personal attitudes toward the three ethical principles and the intentional behavior when faced with ethical dilemmas [15].

The very usual research question is whether corruption may be beneficial for an economy. It has not been clearly researched so far whether and to what extent the impact of regulations on entrepreneurship depends on the intensity of corruption. Regulations make firm entry into markets more difficult. If there are a larger number of procedures needed to start a business and larger minimum capital requirements, then this is detrimental to entrepreneurship. Corruption may reduce the negative impact of regulations on entrepreneurship in highly regulated economies and facilitate firm entry, which means support for the 'grease the wheels' concept [16].

There has been a widespread opinion that bribery greases the wheel of commerce, while others believe that bribery sands the wheel of growth. It has been argued that firms autonomously choose their level of bribery according to their environments and that the benefits and costs may differ for different types of bribery. Specifically, small firms are more likely to be forced to engage in bribery, while big firms may strategically engage in bribery. However, bribery hurts small- and medium-sized firm growth, but not large firms [17]. This finding turns the situation of bribery as being more against justice for smaller firms compared to larger ones.

Countries are perceived by business people and their citizens to be less corrupt if they are highly developed, long-established liberal democracies, with a free and widely read press, a high share of women in government, and a long record of openness to international trade [18]. More educated countries and, to a smaller degree, richer countries, generally have less corruption which is also correlated with the level of income and racial inequality but not correlated with the size of government. There is a weak negative relationship between corruption and economic development in a country. There is correlation between development and the fact that good political outcomes occur because education improves political institutions [19]. Growing economic prosperity in transition countries leads to lower corruption, and contrary to findings for other nations, a bigger government size seems to reduce corruption. Larger countries generally have more difficulties controlling corruption. Transition reforms might be the best solution for corruption reduction [20]. Multinational enterprises often run into government corruption when operating in different countries. Interestingly, in the international management literature, this issue is typically strictly neglected [21].

3. Direct cost of corruption

Bribes, kickbacks, "grease," and "speed" money are the most conspicuous types of corrupt activity. The direct costs of corruption are those costs that result from direct interaction between the firm and the government. Hence, bribes, bureaucratic red tape, and various categories of transaction costs are considered direct costs since they can be identified with a direct interaction or transaction between a particular firm and corrupt officials. Similarly, resources expended in an effort to avoid extortion by corrupt officials of a given firm are also a direct cost.

3.1. Bribes

Bribes cost firms and other stakeholders through monetary and non-monetary payments to those with public power. Examples of bribery are numerous. However, only a small proportion of bribes are exposed, suggesting that bribery is much more pervasive than what is revealed and reported. In September 2002, Michael Woerfel, a senior employee of the European Aeronautic Defense and Space Company (EADS), was charged with corruption in connection with a 1999 $5 billion arms deal with South Africa. EADS conceded that it had "helped" 30 South Africans with hefty discounts on luxury cars. In related developments, chief whip of the ruling African National Congress (ANC) Tony Yengeni was charged with corruption, fraud, and perjury. Also in September of 2002, a Lesotho court found Acres International, a Toronto-based firm, guilty of passing $260,000 as a bribe to the chief executive of the project. The executive was convicted of 13 counts of bribery and of accepting more than $2 million in total bribes. In July 2002, Xerox admitted in a regulatory filing that it had made improper payments of more than $500,000 “over a period of years” to government officials in India to push sales [8]. All these case studies show that the critical infrastructure, being in most cases a matter of public investment and public money spending, is very sensitive to corrupt activities which may consequently increase its vulnerability.

3.2. Red tape and bureaucratic delays

Red tape and bureaucratic delays are examples of non-monetary costs that result from dealing with corrupt officials or complying with the requirements of corrupt regimes. To avoid red tape and delays in facilitating project approvals, firms often use bribes to grease the wheels. This was the case when Robert King, a leading investor in Owl Securities (OSI), was convicted on five counts of conspiracy and for violating the Foreign Corrupt Practices Act by planning to bribe Costa Rican officials. The bribery was related to OSI’s plan to build a new Caribbean super-port and a 124-mile dry canal through Costa Rica, designed to rival the Panama Canal [22]. Lockheed Martin agreed to a consent decree (neither admitting nor denying allegations) in which it paid nearly $25 million in fines after it was accused in 1995 of paying $1 million to an Egyptian member of parliament in order to facilitate the sale of Lockheed aircraft to the Egyptian Air Force [23]. Tehelka, an Internet news portal, caught several government officials taking bribes from undercover reporters in India. The reporters were posing as arms dealers peddling “fourth-generation” thermal hand-held cameras on behalf of a British company. Again, these case studies show that the critical infrastructure is also very sensitive to corrupt activities which may consequently increase the risk of its vulnerability.

3.3. Avoidance

Firms may be forced to engage in expensive efforts to avoid and limit their exposure to extortion by corrupt officials, including hiding output and opting out of the official economy. Avoiding corruption can be costly. For example, Procter & Gamble, as part of its broader exit strategy from Nigeria, decided to close a Pampers plant rather than pay a bribe to a customs official [24], which may be a good example of ethical behavior of the corporation.

3.4. Directly unproductive behavior

Corruption may force firms to engage in a range of costly and unproductive behavior. This may include investment in channels of influence of the decision-makers and power-holders to gain advantage in dividing up the benefits of economic activity through lobbying, direct vote solicitations, and influence peddling. In China, various forms of obligatory “profit sharing” with city officials in Hainan Province have been reported. The employment of relatives, donations, and other “favors” are apparently an expected cost of doing business in that region. One private firm in Hainan Province reported having a formal profit-sharing plan with the city officials. Firms report hiring key officials or their relatives as a way of developing political or social influence. Owners of local private firms in Wenzhous in eastern China have been known to give firm shares to senior cadres in exchange for protection from government interference [6].

3.5. Foregoing market-supporting institutions and engaging in organized crime

Firms bear additional costs when, because of corruption, they are unable to use institutions such as courts for the enforcement of contracts. Costs increase when firms are willing (or unwilling) to engage in organized crime by paying for "protection" and other security services that would otherwise be unnecessary. For example, many firms doing business in Russia in the post-Soviet era have been forced to take part in the underground market for "protection" by paying high fees for "security" services because the state cannot provide adequate public protection. The Canadian International Development Agency has spent $130 million to help generate Canadian business in Russia; however, many companies have claimed that projects have been stolen out from under them because of government corruption. As a result, Canadian investment in Russia has practically stopped all together, and the CIDA has virtually nothing to show for its investment [25]. This example shows how specific acts of corruption result in multiple costs; in this case, efforts to build institutions were thwarted through organized crime, which contributed to other unproductive and costly behavior [8].

4. Indirect costs of corruption

Many of the destructive costs of corruption affect firms indirectly through public-sector failure that results from weak or non-existent institutions, government failure to effectively use public resources, and government policies that prevent the economy from growing. The indirect costs of corruption are those costs imposed on firms that cannot be specifically identified with a particular interaction between a firm and the government or its officials. These costs may result in higher prices for resources, lowered prospects for profitability, and macroeconomic instability. The indirect costs of corruption have been relatively well documented in terms of system-wide effects. However, individual firms may overlook these costs because they don't recognize how such costs affect them. These indirect costs limit investment returns because they increase operating costs and decrease growth potential. Moreover, such costs may fall more heavily on some firms than others [26].

4.1. Reduced investment and distorted public expenditures

Corruption has been proved to reduce the ratio of investment to GDP. Corruption may also reduce public expenditures because tax revenues drop when business activity goes on outside of the official economy. Moreover, the expenditures that remain are often skewed from the most pressing needs towards projects that benefit privileged insiders. Some time ago, Nicaragua resorted to a national tax audit lottery to combat the problem of low tax revenues due to rampant corruption. Each month the government chose 100 professionals at random, audited them, and publicized the results. The government estimated that 40 per cent of all professionals were tax dodgers. The inefficient and proportionally small tax collections resulted in inadequate investment in infrastructure and education [27].

4.2. Macroeconomic weakness and instability

More generally, corruption weakens institutions like courts and regulatory agencies, slowing economic growth [28]. Corruption also reduces aggregate investment through reduction in public and private investment, increasing poverty and the social ills that go along with it [29].

4.3. Weak infrastructure

Corruption weakens public infrastructure including the critical one, resulting in inadequate, expensive, and intermittently supplied services such as telephony, electricity, and transportation [30]. Weak infrastructure offers opportunities for small bribes and thereby increases the direct costs of corruption. Corruption has even been shown to increase an economy's susceptibility to financial crises, such as those that occurred in Russia in the mid-1990s, Southeast Asia and Korea during 1997–1998, and in Latin America in the early 1980s and again in the mid- and late-1990s [31].

4.4. Misdirected entrepreneurial talent

Corruption leads to squandered and misdirected entrepreneurial talent because individuals are drawn to socially unproductive avenues for advancement afforded by corrupt environments. Hence, corruption stymies the very entrepreneurial activities that could offset or mitigate some of its harshest effects [8].

4.5. Socio-economic failure

Finally, weaker economies, poor infrastructure, and squandered investment contribute to general socioeconomic misery. Results include increased poverty, income inequality and slow income growth for the poorest in society, increasing demands on already weak central governments and the retarding of developmental goals such as education, literacy, and life expectancy. This is perhaps the most tragic cost of corruption [32].

5. Conclusions

Managers use several ways of moral reasoning based on rights, justice, utility, and care when they face a moral conflict and when these different ways of reasoning conflict. They need to take several factors into consideration as they weigh decisions based on the principles of rights, justice, utility, or care. They have to consider whether there are possible overriding factors in the decision. If a decision might result in the death of a person made one way and the unemployment of a group of persons made another way, then the overriding factor might be the life-and-death decision [33].

The problem within the ethics of care is not the isolated individual act of corruption, but the systematic system of corruption that can exist across historical periods, geographic areas, and political-economic systems. It is important to first understand how corrupt and unethical subsystems operate, particularly their network nature, in order to reform and change them while not becoming what we are trying to change. A key operating feature of corruption systems is that they are relatively stable networks rather than exceptional, independent, individual events [34].

Recognizing that management is an inherently ethical task and that the practices of the company embody a set of values or ethics, there is a set of ethically-based management practices that can help managers lead their companies effectively. The ethics of effective and competitive business practices include creating a shared sense of meaning, vision, and purpose that connect the employees to the organization and are underpinned by valuing the community without subordinating the individual and seeing the community's purpose as flowing from the individuals involved. A second characteristic that ethical leadership can provide is developing in employees a systems perspective, which is linked to the post-conventional stages of cognitive and moral reasoning discussed above, so that a value of serving other community members and related entities in the broader ecosystem emerges. Another theme is that of emphasizing business processes rather than hierarchy and structure, which is based on valuing work itself intrinsically and focusing on both the ends and means in decision-making, not just the ends. Localized decision making, particularly around work processes, provides a value of responsibility for individual actions, and using information within the system is supported by the values of truth telling, integrity and honesty, the characteristics of moral persons, as well as transparency about and access to needed information [35].

Corruption is hard to study empirically. Its many likely determinants interrelate in complicated ways. Some can change quickly and may be caused by corruption as well as the opposite. As with other types of criminal activity, it is hard to observe directly, and so researchers must rely on surveys of corruption's victims, the accuracy of which is often difficult to assess. On this last score, recent years have seen some major advances. A range of different business consultancies, economic research firms, and polling organizations have surveyed domestic and expatriate business people as well as ordinary inhabitants on the degree of corruption in the countries where they live or work. The comparative evidence accumulating from these surveys is surprisingly consistent. Different ratings correlate highly. Domestic and foreign business people, country experts from consultancy firms, and residents of particular countries basically agree about which countries have more corrupt governments. Ratings prepared in the 1980s also correlate closely with those from the 1990s. At the same time, such ratings of comparative corruption correlate as one would expect with lower investment, both foreign and domestic, and lower growth [36].

Corruption has direct and indirect effects on aggregate FDI into a given economy and influences firm-level decisions about entry mode and project structure. First, the nature of corruption is not fully appreciated and incorporated in managerial decision-making. Failure to comprehend differing types of corruption may hinder the effective operation of international businesses, where resource commitments are substantial and difficult to reverse and reputation effects are long lasting. Second, while firms fully recognize the costs related to the pervasiveness of corruption, arbitrariness is often disregarded in the development of proactive strategies. Whereas firms appear to adjust their entry modes when confronted by high arbitrariness, they may forego other strategies due to a mistaken perception that arbitrariness affects all firms the same, when in fact it can have significantly disproportionate impacts on firms. Third, firms adjust and adapt their market-entry approaches to minimize exposure to partners who may attempt to exploit the corrupt environment for their own gains, yet maximize relationships with partners that can facilitate project development. Fourth, firms often don't fully recognize the range of strategic alternatives to acquiescing to corrupt pressures. These strategies can help reduce costs, and some may help in deterring corruption more broadly. Fifth, some strategies may be pursued by individual firms, collectives of companies, or in conjunction with governments. For example, a number of the companies mentioned above support broad, government- or industry-driven efforts to reduce corruption through membership in organizations such as the International Chamber of Commerce, while at the same time focusing on shorter-term and transaction-specific challenges that affect their day-to-day business opportunities. Governments, independently and through international consortia, continue to struggle in their efforts to identify effective solutions to the destructive practices of corruption. At the same time, companies seeking new markets and opportunities continue to explore options that minimize the most pronounced impacts of corruption. Both governments and companies have made important steps in their efforts to stem the spread of corruption, but much more needs to be done. We considered five strategies that show how firms can deal with corruption in a manner that preserves their strategic choices in international market entry, while protecting themselves from the costs of corruption. None of the strategies we propose comprehensively addresses corruption. At best, each reflects a partial solution. Taken together, they may provide a more comprehensive approach, particularly given the interactive and mutually reinforcing nature of firm- and government- sponsored strategies. Just as firms pursue multiple business strategies to address their objectives in international markets, so too should they consider the range of options to combat corruption. In the interim, firms should be aware—and be wary—of their dealings in countries where corrupt practices are common. Firms would be wise to work cooperatively with each other and with government organizations to realize the substantial benefits of reduced corruption: improved firm and aggregate business performance, more effective host-nation governance, and greater and more widespread social and economic development [8].

The main proposition of the present study, namely that the corruption which may be observed as a direct consequence of the unethical behavior of managers and other (also political) decision makers imposes substantial direct and indirect social costs which seriously decreases the general welfare of a particular economy, can be regarded as confirmed. Several authors proved that both the direct and indirect costs of corruption are actually nothing but an unavoidable consequence of the unethical behavior of managers and other decision-makers. As far as short-term future research is concerned, there is the urge for better quantitative estimation of the cost of corruption. It is believed that only a direct number comparison of what can be achieved with all the amounts of economic loss will start a systematic change in the cognitive frameworks and concrete activities of those who may have future influence and the power to change those corrupt systems in the direction of the standards of modern democracies.

References

[1] N. D.Johnson, C. L. La Fountain & S. Yamarik, Corruption is bad for growth (even in the United States). *Public Choice*, 147(3-4), (2011), 377-393.

[2] A. A. C. Teixeira, Sanding the Wheels of Growth: Cheating by economics and Business Students and 'Real World' Corruption, *Journal of Academic Ethics*, 11(4), (2013), 269-274.

[3] K. Blackburn, Corruption and development: explaining the evidence, *The Manchester School*, 80(4), (2012), 401-428.

[4] M. Swaleheen, Economic growth with endogenous corruption: an empirical study, *Public Choice*, 146(1), (2009), 23-41.

[5] P. H. Mo, Corruption and economic growth, *Journal of Comparative Economics*, 29(1), (2001), 66-79.

[6] D. Ahlstrom, G. D. Bruton, Learning from successful local private firms in China: Establishing legitimacy, *The Academy of Management Executive,* 15(4), (2001), 72-83.

[7] S. Waddock, Ethical Role of the Manager, *Encyclopedia of Business Ethics and Society.* Ed. Thousand Oaks, CA: SAGE, 2007. 786-91. *SAGE Reference Online*. Web. 30 Jan. 2012, (2007).

[8] J. P. Doh, P. Rodriguez, K. Uhlenbruck, J. Collins, L. Eden, Coping with corruption in foreign markets, *Academy of Management Executive*, 17(3), (2003), 114-127.

[9] S. H. Conrad, R. J. LeClaire, G. P. O'Reilly, H. Uzunalioglu, H.. Critical National Infrastructure Reliability Modeling and Analysis, *Bell Labs Technical Journal*, 11(3), (2006), 57-71.

[10] L. K. Treviño, M. Brown, Managing to be ethical: Debunking five business ethics myths, *Academy of Management Executive*, 18(4), (2004), 69-81.

[11] B. Rothstein, E. M. Uslaner, All for all: equality, corruption, and social trust, *World Politics*, 58(1), (2005), 41-72.

[12] A. Argandoña,. Coruption and Companies: The Use of Facilitating Payments, *Journal of Business Ethics*, 60(3), (2005), 251-264.

[13] G. R. Montinola, R. W. Jackson, Sources of corruption: a cross-country study, *British Journal of Political Science,* 32(1)**,** (2002), 147–170.

[14] J. Svensson, Eight questions about corruption, *Journal of Economic Perspectives*, 19(3), (2005), 19-42.

[15] P. W. Zgheib, Managerial Ethics: An empirical study of business students in the American University of Beirut, *Journal of Business Ethics*, 61(1), (2005), 69-78.

[16] A. Dreher, M. Gassebner,. Greasing the wheels? The impact of regulations and corruption on firm entry, *Public Choice*, 155(3-4), (2013), 413-432.

[17] J. Q. Zhou, M. W. Peng,. Does bribery help or hurt firm growth around the world? *Asian Pacific Journal of Management*, 29(4): (2012), 907-921.

[18] D. Treisman, What have we learned about the causes of corruption of from ten years of cross-national empirical research? *Annual Review of Political Science*, 10, (2007), 211-244.

[19] E. L. Glaeser, R. E. Saks, Corruption in America, *Journal of Public Economics*, 90(6-7), (2006), 1053-1072.

[20] R. K. Goel, J. Budak, Corruption in transition economies: effects on government size, country size and economic growth, *Journal of Economics and Finance*, 30(2), (2006), 240-250.

[21] P. Rodriguez, K. Uhlenbruck, L. Eden, Government corruption and the entry strategies of multinationals, *Academy of Management Review*, 30(2), (2005), 383-396.

[22] W. B. Cassidy, Fraud, bribery, etc. *Traffic World*, 266(29), (2002), 8-10.

[23] R. Scott, Eliminating bribery as a transnational marketing strategy, *International Journal of Commerce & Management,*12(1), (2002), 1–17.

[24] D. Yiu, & S. Makino, The choice between joint venture and wholly owned subsidiary: An institutional perspective, *Organization Science,* 13(6): (2002), 667–683.

[25] P. Webster, Ripped off in Russia. *Maclean's. www.mcleans.ca.* (2002)

[26] P. Mauro, Corruption and the composition of government expenditure, *Journal of Public Economics,* 69, (1998), 263–279.

[27] P. Mauro, Corruption and growth, *The Quarterly Journal of Economics,* 110(3), (1995), 681-712.

[28] A. Brunetti, B. Weder, Investment and institutional uncertainty: A comparative study of different uncertainty measures, *Weltwirtschaftliches Archiv,* 134, (1998), 513-533.

[29] C. Gray, D. Kaufmann, Corruption and development. *Finance and Development,* 35(1), (1998), 7-10.

[30] P. Keefer, Protection against a capricious state: French investment and Spanish railroads, 1845–1875, *The Journal of Economic History,* 56(1), (1996), 170-192.

[31] Transparency International. *2003 global corruption report.* London: Profile Books (2003).

[32] M. Johnston, Corruption et de´mocratie: Menaces pour le de´veloppement, possibilite´s de re´forme, *Revue Tiers Monde,*161: (1999), 117–142.

[33] G. F. Cavanagh, D. J. Moberg & M. Velasquez. The ethics of organizational politics*, Academy of Management Review,* 6(3), (2000), 363-374.

[34] R. P. Nielsen, Corruption networks and implications for ethical corruption reform, *Journal of Business Ethics*, 42(2), (2003), 125-149.

[35] J. M. Liedtka, Constructing an ethic for business practice: Competing effectively and doing good. *Business and Society,* 37(3), (1998), 254-280.

[36] D. Treisman, The causes of corruption: a cross-national study, *Journal of Public Economics*, 76(3), (2000), 399-457.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-30

Outsourcing as an Important Source of Risk in the Management of Terrorist Threats

Miran VRŠEC [a,1], Milan VRŠEC [a] and Vito MURGEL [a]
[a] *Institute for Corporative Security Studies, Ljubljana*

Abstract. This paper critically deals with outsourcing as a more complex source of risk in the system for ensuring corporate security, especially when talking about subjects that are part of the critical infrastructure of the country. The Republic of Slovenia has become an integral part of the global market, which is why it is essential to recognize that the outsourcing entities that work in the Slovenian market operate more and more globally, but on the other hand global corporations are entering the market. When addressing the risks of outsourcing it is therefore essential to take into account a broader global perspective, especially if these risks are discussed in terms of the risk of terrorist attacks. Globalization requires the integration and aggregation of organizations from different geographical and cultural backgrounds, which is why there is a growing openness of the labor market and an increase in the free passage of the workforce and as a result new risks are brought by outsourcing entities. Regarding this in particular I mean the risks associated with human resources and humans as individuals. In the future, a comprehensive approach to risk management outsourcing needs to provide a different perception of outsourcing and its impact on the organization's risk and social environment. Therefore in the future, corporate security mechanisms must significantly pay more attention to outsourcing risk in so far as they would like to fulfill their basic mission, which is to allow continuous operation under normal as well as emergency situations (natural disasters, accidents, large-scale, international organized crime, terrorist acts, etc.). Therefore, there is a need for a broader discussion including more scientific research dealing with the risks of outsourcing. The real world has revealed that too little attention or even no attention has been given to establishing systems of risk management and building comprehensive integrated security systems for outsourcing risk since there is a lack of awareness of what constitutes outsourcing risk for the organization and the wider local community. The purpose of this paper is to show the importance and the role of the outsourcing in ensuring corporate security at both the operational as well as the strategic level and to indicate the risks associated with the integration process of outsourcing in the provision of corporate security.

Keywords. outsourcing, corporate security, critical infrastructure, threat assessment, terrorism, security risks, integrated security system

1. Introduction

The fundamental objective of the organization's performance (of a company) is creating (maximizing) profits and increasing the value of capital in a maximum period. By realizing these fundamental objectives, management and owners also try to achieve the optimum utilization of resources and time that they have available by introducing modern managerial tools and best practices in business processes and thus achieve the maximum effects of the operation of business processes and the organization as a whole. Basically, it is therefore a realization of the basic "mini-max" principle of economics, that is, with minimum inputs to achieve maximum effects.

[1] Corresponding Author: Miran Vršec, MSc., Institute for Corporative Security Studies, Ljubljana, e-mail: miran.vrsec@ics-institut.si

When introducing outsourcing in organizations that are part of the critical infrastructure of a country it is extremely important that the owners and the management understand the risks in which the introduction of outsourcing poses to their organization. As a rule, this involves larger organizations that have mixed ownership, where the state appears as a minority or majority shareholder, directly or indirectly. Ensuring the continuous operations of organizations that are part of the critical infrastructure in all conditions is vital for the smooth functioning of the vital activities of the state as a whole, which is why the above-mentioned "mini - max" principle must get a different meaning. When introducing a system of risk management at the strategic level we must not forget about the minimum input and maximum effect, but the necessary inputs and their optimal effects - when we talk about risk management - shown through the timely detection and rejection of dangers, effective alarming, effective action and the effective elimination of the consequences resulting from an unusual event or emergency. The awareness of the risks of outsourcing is especially important because outsourcing in organizations that are part of operators of critical infrastructure, assumes all important tasks, which are often of key (strategic) importance for the functioning of organizations that are part of the critical infrastructure (security, cleaning, information security and maintenance of information systems, strategic consulting, etc.). From this perspective, outsourcing can therefore be crucial for the functioning of a company and the introduction of outsourcing is a fatally important strategic decision for the owners and management [1].

Here are some statistics from a survey of past and future development of outsourcing in the U.S. (http://jobs.lovetoknow.com/Facts_and_Figures_on_Outsourcing). Research shows that in the U.S. more than 500,000 jobs were transferred to outsourcing since 2000 and more than 250,000 jobs had been lost at the expense of outsourcing. The biggest "culprit" for this is the information technology sector. The study lists 10 companies that brought the most jobs in outsourcing, namely: IBM 63,700, EDS 22,400, Dell 17,450, Cognizant 15,000, Siemens AG 15,000, General Electric 14,250, Convergys 14,000, Accenture 13,000, Computer Sciences Corp. 10,800 and Intel 10,426. On the account of these 10 companies, more than 200,000 were transferred in outsourcing. According to the U.S. Department of Work and research carried out in the area of outsourcing, more than 3.3 million jobs were transferred in outsourcing with the most in the areas of administration IT and support services. The final establishment made by the research is interesting and it states that outsourcing brings restlessness in people especially if they do not believe in the theoretical explanations of outsourcing.

Outsourcing is becoming more actively integrated into the operations and business processes of organizations that are part of the critical infrastructure, which under certain conditions enables all the more covert and sophisticated information gathering and the infiltration of individuals or even groups to the heart of these organizations, which can quickly - because of their importance and exposure - become the subject of a terrorist act. This statement can be confirmed by the definition of terrorism given by the FBI, which states that when it comes to terrorism, it is the illegal use of force against persons or property in order to frighten or coerce the government, the civilian population or its segment, into a particular political or social objective. Terrorist activities have no borders and cover a wide range of options, with the selection of civilians and important organizations as targets. To cause widespread nervousness, objectives are to adapt to those places where people gather in masses - airports, commercial buildings, food malls, and hotels – or by carrying out a terrorist act it causes enormous material damage and the impaired functioning of local communities or even the country as a whole. The solution for managing the risk of a terrorist attack is tremendous, but the simultaneous concentration of such a huge number of potential targets is almost impossible. In even the most sophisticated security, errors are always possible and present and as a rule slight carelessness or a slight mistake may allow potential unnoticed perpetrators to carry out a terrorist act. In this context, it is important to recognize the words uttered by some terrorist leader: "It is enough that we have luck only once, you need to have it all the time".

Man is the key factor in the system of corporate security. By performing positively man can significantly contribute to controlling risk, but by having a negative attitude this alone causes risk and also implements it in practice through various forms of activity, including acts of terrorism. Outsourcing often includes service activities, in which the end providers are people, which is why the management of human resources in outsourcing and the risks arising from outsourcing is so crucial.

2. Starting points on outsourcing

In the past, owners and management shared a general belief that the effectiveness of an organization can be increased solely through the increase in the effectiveness of individual business processes within individual business functions and within the organization as a whole. Therefore, all endeavors were oriented towards the search of internal reserves and optimal combinations of available resources. When this could no longer suffice, organizations realized it was necessary to search for new markets, in particular outside the borders of home country, which resulted in the formation of the first international connections that led to the ever growing globalization of the market and the operation of organizations. Rapid growth caused more and more problems to organizations. Becoming larger, they were also becoming less flexible and slower to adapt. What is more, they were becoming less cost-effective. Ideas started to emerge on the transfer of particular segments of activities to contractors who specialized in particular activities and were highly flexible and far more cost-effective. Outsourcing was becoming a special purchasing strategy and an increasingly important strategic decision of organizations. Today, the greatest challenge for companies is the question of how to adapt as quickly as possible to changes on global and local markets and how to remain competitive in the long-run. Certainly, outsourcing makes it easier, since companies can, in a more thorough and effective manner, focus on the development of their core activity. However, in doing so, they should not neglect the fact that outsourcing brings not only benefits, but also some risks, which are to be discussed below.

2.1. Definition of outsourcing

The concept of *outsourcing* derives from the word phrase "outside resource using" and refers to the use or rental of external resources for the need of the operation of one‘s own organization. An organization entrusts particular activities or entire business functions to outside contractors that could also be provided in-house, while more or less keeping its core competencies. The English term "outsourcing" is usually translated into Slovene by experts as zunanje izvajanje dejavnosti (external service provision), zunanja oskrba (external supply) or najem storitev (service rental). Individual authors, of course, offer different definitions of this concept. Their definitions mostly depend on the type of activity and their scope. What is more of less common to all of them is that it is a transfer or an award of a contract for one or several internal activities to another organization, which thus becomes an external contractor.

2.2. Some research findings on outsourcing

A research focused on an analysis of Slovenian companies in the area of outsourcing shows data on activities that are outsourced by the companies, namely [2]:

1. **cleaning – 66 %**
2. **security – 55 %**
3. **information technology – 49 %**
4. **preparation of hot meals – 41 %**
5. **legal services – 33 %**
6. transport – 30 %
7. accounting services – 24 %
8. equipment maintenance – 23 %
9. production – 21 %
10. distribution – 8 %

11 research and development – 6%
12 after-sales services – 4 %
13 quality control – 3 %

For the purpose of comparison, results of another research [3] are presented below:

1. **cleaning – 61 %**
2. **security – 53 %**
3. **food services – 47 %**
4. **occupational health and safety – 46 %**
5. **legal advice services – 46 %**
6. production – 39 %
7. information technology – 35 %
8. accounting and financial services – 17 %
9. distribution, logistics, storage – 11 %
10. research and development – 9 %
11. other – 6 %
12. human resources – 4 %
13. after-sales services – 3 %
14. procurement – 1 %

The data obtained from both pieces of research reveal that the majority of outsourcing is used in cleaning, security and food service. It is also often used in the area of information technology and legal advice. This is a significant finding, which is interesting in terms of risk management and corporate security for the following reasons: First, organizations transfer a fairly large part of security to outside contractors of questionable (problematic) quality; second, cleaning services in larger organizations are usually performed outside working hours and by cleaning personnel which is usually coming from culturally diverse, socially disadvantaged and crime-prone environments; third, food outsourcing is subject to the HACCP food safety standard; fourth, information management outsourcing has to be updated with the ISO/IEC 27000 security standards, whereby a strict laws on the protection of personal and confidential data and business secrets are to be obeyed; fifth, there is but little quality security advice in legal counseling; and last, but not least, contracting authorities or users do not include security clauses in the outsourcing contracts (requirements for a higher security level with the introduction of security standards, bank guarantee, non-competition clause, protection of confidential information, introduction of ISO quality standards, etc.).

It can be assumed that outsourcing of security services remains an open issue. For the purposes of our discussion, this paper primarily addresses the questions of outsourcing in critical infrastructure as well as the role and risks of outsourcing in integrated security systems and the processes of providing corporate security [4][5][6]. The main problem concerning this batch of questions and dilemmas is the management of risks which come with the introduction of outsourcing.

2.3. Why outsourcing should be introduced

Outsourcing is a means or tool for the management to successfully achieve strategic business guidelines and goals of its organization, primarily associated with an increase in efficiency, adaptability to changing conditions in the internal and external environment and the reduction of its operating costs. Outsourcing is primarily used for the purpose of the management and reduction of costs of the organization, which is too often the sole purpose of an organization. In this way, different investments can be avoided in the short run (e.g. equipment acquisition, facility expansion). Instead, an organization can use its resources for the development of its core competencies, key personnel and for new knowledge acquisition. Of course, it needs to be assessed whether the short-run benefits of outsourcing can also be felt in the long run, and what the long-term influence on the long-term development and growth of the organization is. Furthermore, it has to be taken into consideration that an organization should never allow itself to be entirely dependent on outsourcing, for this could present too great a risk for the organization in the long run [7]. Along with the development of outsourcing, activities have expanded which have become the subjects of outsourcing. Recently, it can be observed that organizations have also outsourced some significant support or even core processes or activities, such as: legal affairs, accounting services, IT, parts of production processes, logistics (transport services and storage) as well as certain parts of personnel function. This makes an organization more open and flexible, but also more vulnerable. In terms of security, this presents higher and higher risks that need to be systematically managed.

The literature overview [4][1][8][7][9][10] shows that an increased emphasis has been given to the consideration of benefits that come with outsourcing, such as: cost management and reduction, influence on the reduction of investment needs, conversion of fixed costs into variable costs, higher level of quality and reliability of operation, increase in flexibility and adaptability, orientation towards the development of organization‘s core competencies and focus on key customers. However, many experts have recently warned about the dangers of outsourcing, e.g. smaller savings than planned, poor quality of performance, hidden costs, the wrong selection of an outsourcing partner, loss of expert knowledge, business partner take-over, loss of key employees, and loss of contact with key customers. It should be pointed out that these dangers usually pertain to companies associated with the early termination of outsourcing contracts and the transfer of the performance of operations to activities in the processes, while there is too little discussion about the long-term strategic aspects and guidelines for outsourcing, both in terms of benefits and risks, including those with a direct influence on the security situation in an organization. Much too often, outsourcing is considered solely in terms of the transfer of activities to outside contractors, while no consideration is given to the necessary integration of outsourcing into the organization's support processes.

3. Introduction of quality outsourcing into the critical infrastructure management system

3.1. Definition of critical infrastructure

According to the Council Directive (EU) No. 114/2008 of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection that followed the above-mentioned programme, only energetics and transport are classified as cross-sectors of European critical infrastructure that operate in two, three or more countries. Pursuant to the Directive, each EU member state shall identify which sectors to include in the national critical infrastructure.

Critical infrastructure protection and the protection of citizens are becoming a reality and one of the most important segments of the European security policy and European security system in the EU and individual EU member states. The EU and its member states have demonstrated vulnerability. Obviously, terrorism, more than all other incidents, initiated certain activities of European institutions (European Commission and others) which have started to work on specific projects to raise the level of security control in the European area. Concerning vulnerability, threats and security risks in the EU as well as the protection of vital facilities, i.e. critical infrastructure [11][12][13], it is nevertheless important to realize that threats are not posed only by terrorism [14][15] but also take various other forms which are a cruel present and future reality. These forms are natural hazards, climate change, environmental incidents, industrial accidents and crime-related threats. These are all long-term, multifaceted and complex threats that have to be addressed in terms of damage and loss prevention, and in terms of civil and professional response to incidents.

3.2. Outsourcing provider selection

Prior to the decision to outsource, an organization's management must carefully consider and decide what activities or parts of processes to transfer to outsourcing and speculate the possible implications of outsourcing on further development and growth of the organization.

In order to think about how to require and ensure the appropriate quality level of services, the following questions concerning outsourcing provider selection should be addressed:

- How and where to find an appropriate (quality) outsourcing on the market?
- What criteria should the outsourcing provider meet?
- What warranties should be required from the outsourcing provider?

- How to choose an appropriate outsourcing provider?
- What type of contract should be concluded with the outsourced entity?
- Who will be made responsible within the contracting authority and the contractors for the introduction of entire outsourcing into specific business and other processes?
- How will the contracting authority and people responsible for outsourcing supervise the performance of contractual obligations?
- How will outsourcing introduce improvements into the performance of contractual obligations?

When talking about critical infrastructure entities, it is particularly important to point out, prior to the selection of the provider, the following questions that are essential for defining the level of risk associated with outsourcing:

- How does the service provider manage risk is its organization?
- How does it manage risks in the business environment in which it operates?
- What security and other standards are introduced into its business processes?
- What business tools does it use in the implementation of its core processes?
- What is its ownership structure?
- Does it have any affiliated or partner companies?
- Who are its key customers and what are its key markets?
- What is its financial situation (capital structure, financial resources, previous financial results etc.)?
- Who are its key personnel?
- What competitive advantages can the outsourcing service provider offer?
- What is its reputation?

The service provider selection follows the management decision that the company is ready to transfer a particular service to the outsourced company after the compliance assessment has been carried out. It is important to acknowledge that the selection procedure is very demanding. It might lead to an organization‘s success or trouble. Therefore, an organization’s management needs to examine several data and elements when selecting an outsourcing service provider. Based on the above questions, it is essential that prior to selection, the following aspects are examined: experience, references, capital power, financial stability and reputation of the service provider.

The following questions are also important to consider:

- What is the price and what is the added value resulting from the invested money in respect to the quality and range of offered services?
- Who bears the risk?
- What about the access to key knowledge and resources?
- Taking into account its strategic developments, how will the service provider be able to satisfy the organization’s future needs?
- Is the outsourcing service provider willing to invest and engage in risk-taking?
- What is the common approach to current business problem solving?
- Is the provider committed to continuously improve its services?

Obviously, the outsourcing provider selection is a complex process. The approach described above ensures to the contracting entity the appropriate management of risks coming with the introduction of outsourcing into an organization‘s work processes, and a smooth operation and optimal effects of long-term cooperation. Therefore, cooperation should be based on building good partnership and pursuing the contracting authority's main development goals.

3.3. Security mechanisms for the management of risks in outsourcing

When considering the security related to the outsourcing service provider, the following questions will arise:

- Who will directly perform outsourcing services?
- How is the outsourcing personnel security cleared and what social and cultural groups do they come from?
- What security system is established by the outsourcing service provider?
- What are long-term cooperation opportunities?

The above and several other questions should be considered by both the contracting entity as well as the outsourcing service provider. Outsourcing is a marathon rather than a sprint, and it involves several intermediate stages. It is a long-term partnership, whereby outsourcing and its service become an integral and indispensable part of the business processes and operation of an organization. As a rule, an organization's success also depends on the quality of this partnership.

The outsourcing provider has to be particularly aware of the fact that service performance for the needs of critical infrastructure entities requires significantly more engagement of security mechanisms in managing business security risks emerging in the business process and environment of the outsourcing provider. In the initial phase, the outsourcing provider has to elaborate vulnerability, threat and business-related security risk assessment, on the basis of which it can identify and analyse vulnerability, the level of threat and business security risks, and develop appropriate security measures and solutions to deal with these problems in a comprehensive manner. Efforts should be clearly focused on the development of an integrated security system which ensures a comprehensive management of business security risks, both at the strategic and operational levels. In this manner, the outsourcing provider actually manages risks in all business functions and process phases.

One of the main integrated security system elements is control, by means of which we constantly check the adequacy and effectiveness of risk management mechanisms at various operating levels. With the introduction of improvements, the control enables the smooth operation of the security system in the long-run.

However, taking all this into account, the essence of cooperation between business entities – mutual trust and understanding – should not be disregarded. This is essential, no matter how good the security mechanisms might be. Along with legal and operational definitions, such partnership largely depends on business ethics and ethics of the relationship as such.

3.4. Subject of the contract with the selected outsourcing provider

After the selection of the outsourcing provider, the subject of the contract should be negotiated. Since the partners are mutually dependent, this phase is based on complete trust between both partners. Thus, a contract should not be signed in a »win-lose« manner. Rather, a contract should be developed in such a way as to enable the resolution of potential disputes. It has to be complex depending on the complexity of the outsourced service. For complex projects, contracts can be drawn up in two parts. The general part defines the legal frameworks, while the second part details the rights and obligations of both partners [16]. When drawing up a contract, the contract should also include the benefits for the contractor, following the "win-win" model.

In line with good practices, the contract should contain 7 sections [16], namely:

1. **Task specification –** partners specify the types of work for transfer, the duration of the contact and the period of work performance,
2. **Required level of service** – the required service delivery standards must be set for all the works. The standards must be measurable.
3. **The rights and obligations of both partners** – the contract should specifically define the rights and obligations of each contracting party.
4. **Transitional period** – an important aspect of the external process and concerns, inter alia, the transfer of personnel, training of outsourcing employees, transfer of means of production, and monitoring the performance of activities.
5. **Price, terms of payment and contract duration.**
6. **Contracting management** – the time schedule of reporting and the method of solving problems related to non-compliance with contractual provisions.
7. **Specific clauses** – liquidated damages, introduction of standards and business tools etc.

When signing contracts with outsourcing providers, critical infrastructure entities also need to define outsourcing commitments on the provision of risk management system within their organizations. This means that in the contract, the outsourcing providers commit to the manner of:

- managing business security risks in their organization and working environment,
- applying occupational health and safety security measures on the location of performance of contract works,
- performing fire safety measures on the location of performance of contract works,
- providing appropriate personnel that is to perform the contract works,
- protecting personal and confidential data and business secrets they can access during the performance of contract works,
- monitoring the contract work performance,
- managing security mechanisms in their organization and ensuring their proper functioning.

Given the complexity of the contents of this part of the contract resulting from the critical infrastructure entity security needs, the contents concerned can be defined in a special act which is attached to the contract and its integral and inseparable part.

The quality of contract relationship is primarily influenced by the following 10 success factors[2]:

- Understanding company goals and objectives
- Strategic vision and plan
- Selection of the right contractor
- Ongoing management of the relationships

[2] Outsourcing Consortium, www.outsourcing.com

- Proper structure of the contract
- Open communication with affected individuals/groups
- Support and involvement of senior executives
- Careful attention to personnel issues
- Short-term financial justification
- Use of external expert opinion

Past experience with tragic events (e.g. terrorist attacks in the U.S.A., Great Britain, Spain, Africa and elsewhere) shows that the area of human resources represents the greatest risks.

Perpetrators of terrorist and other criminal acts use outsourcing as a springboard for the performance of their acts. They use outsourcing to infiltrate into an organization and secretly prepare the environment for the performance of their criminal acts (gathering information, identifying process and loopholes, searching for loopholes in the security system, and searching for potential partners for performing criminal acts, etc.). Personnel-related risks are difficult to recognize and manage. Therefore, greater attention should be paid to them.

3.5. Deliberate introduction of outsourcing into the system and process of critical infrastructure management

The majority of critical infrastructure assets in Slovenia are owned by the state. This means that most services are outsourced through the public procurement system, whereby the lowest bidder is selected. Thus, the main criterion is the price rather than the quality. Naturally, good quality is expected. But how can the lowest price (which often does not even cover the costs) ensure the expected quality or the quality compliant with ISO 9001:2008 standards, safety standards and corporate social responsibility?

The following activities or parts of processes involve risk when fully outsourced:

- IT management,
- Accounting,
- Personal and confidential data management,
- Business secret management.

The appropriate selection of an outsourcing provider is therefore crucial for the successful process of introducing outsourcing into the organization of a critical infrastructure entity.

As mentioned above, the outsourcing provider is usually selected through the public procurement system. Therefore, the preparation of appropriate documentation related to the call of tenders is essential. The documentation has to include at least all the references referred to in this paper. The preparation of bidding documents is a complex and broad topic. It goes beyond this paper, and should be explored in some other paper.

4. The role of outsourcing in integrated security systems in companies and other organizations

The security of an organization is no longer a side issue. It has become an integral part of its policy, strategy, economics, business dynamics, culture, reputation, development, growth and collapse. This means that the level of security selected by the owners, management, supervisors and employees when trying to achieve positive business results is of great importance. Loss and damage event prevention is becoming crucial, and so is the belief that the security mechanisms are the elements used for professional management of vulnerability, threats and risks. Thus, security activities have been recognized as an important factor of work and business efficiency and performance, and hence one of the factors for increasing competitiveness (competitive advantage) of every organization, which is the condition for its survival in modern and crisis market conditions.

It is obvious that the new thinking related to the security of companies rests more on economic, business and ethical values and standards that apply in economy, and less on the state and its repressive institutions. The organization must be the first to respond when its assets, capital, profits, employees, intellectual and industrial property, business secrets, competitive advantage, reputation and other values are under threat. Timely and professional response requires knowledge on security, warning and protective mechanisms within an organization, as well as knowledge and information about the control system and its external dangers and threats. It is also good to know what can and should be done – in cases of deviance in the economy – by state institutions in the discharge of their official duties, what is the role of the audit and inspection system, and where the company can order high-quality physical, technical, advisory, educational and other security services. The main issue is how to build a modern, economical, professional and independent security system in an organization, which is based on the principle of optimal protection and which ensures an appropriate level of security, cost management and protection benefits (cost/benefit) and loss prevention. It concerns the establishment of an integrated security system with integrated security which consists of interconnected and interdependent areas of expertise related to security, such as: protection against natural and other disasters, occupational health and safety, fire protection, environmental protection, data protection, protection of information and business secrets, physical and technical security, civil protection, etc. The conditions for introducing integrated security are the following: compliance with regulatory requirements, introduction of security standards, quality assessment of security solutions within the quality system management, and the improvement of the level of safety culture of employees and business ethics of the management.

Discussions on organization's security issues and the role of the state, audit, private security sector and others have become topical and have taken place within parliamentary systems, entrepreneurship, supervising institutions and the mass media. This is further reinforced by crisis management situations which require a professional handling of security issues of companies and the economy as a whole [17][18]. Negligent security in organizations can be fatal. This fatality may lead to notorious and far-reaching economic, financial, business and other scandals, huge financial loss, ethical damage, economic crime and numerous audit requests in order to determine the constitutionality, legality and ethics of the ownership, organizational, financial and personnel transformation, looking for possible fraud and error. In this respect, mechanisms for the prevention and management of all possible hazards to work, business and management of organizations should be perceived as positive. Anything that brings financial, business and moral damage is detrimental to an organization. The sum of all damages and losses in a particular organization can be devastating and frightening, often leading to entropy and collapse.

Thus, most organizations face all-encompassing internal and external treats and crisis in the transformation process. It is the commercial, social and business – i.e. economic – security of organizations that is threatened. Taking into account the conditions and circumstances of organizations' crisis management and leaving most safety concerns to organizations themselves, (particularly) the actual owners, management teams and security experts will have to make many complex organizational, technical, information, educational and other interventions to establish their own warning, surveillance and protective mechanisms.

Only an organization with modern security and control mechanisms can be sound, internally solid, successful, competitive and enjoying high reputation. The umbrella management and security management should go hand in hand to define **what the organization will protect by itself and what can be outsourced** to achieve this objective [19][20]. An organization designed in this manner has a high chance of quickly breaking into the European and global market and business scene. Indeed, quality in-house security and security outsourcing are no doubt a competitive advantage.

Most security outsourcing pertains to physical and technical security and the management of security control centers, and in that regard also to alarm signal response. This is followed by the outsourcing of fire protection services, occupational safety and health and information security. A special outsourcing area refers to the insurance of various risks at insurance companies, enabling the creation of financially attractive insurance portfolios.

5. The management of outsourcing risks in corporate security management processes

In corporate management theory and practice, risk taking is a normal, logical and essential phenomenon in every corporation, affiliated group, business system and individual company. In this context, risk avoidance means that an organization's management is incompetent, ignorant and unwilling to confront the challenges, danger, changes, business opportunities and development strategy which involves many risks. An interesting idea on risk taking in the decision process was developed by the former U.S. Secretary of State Colin Powell, who recommends a 40/70 formula and advises: „Don't take action if you have only enough information to give you less than a 40 percent chance of being right, but, don't wait until you have enough facts to be 100 percent sure, because by then, it is almost always too late. Once the information is in the 40 to 70 range, go with your gut" [21][22]. Due to many changes of internal and external origin and conscious risk-taking, companies incorporate risk management into their business policy, development strategy, decision-making processes and relationships with business partners and outsourcing in order to prevent or minimize the economic, material, financial, human and moral damage and loss.

It is an extremely important business security philosophy of those owners, operators, management and supervisors who bring **incident, damage and loss prevention** in business process management to the forefront. **The same philosophy is adapted by the owners and outsourcing management** who produce particular products for or provide services to contracting authorities. Business results and profits of contracting authorities also depend on costs, quality and risks related to outsourcing.

Contracting authorities – corporations, affiliated groups, companies, public corporations, institutes, state institutions and other organizations – have to be aware that the introduction of outsourcing involves certain risk in terms of costs, quality, reliability, security, long-term operation and operation in crisis situations.

In this perspective, the following outsourcing risks should be recognized:

- Inadequately educated, unprofessional, uncommunicative or chaotic or crime-prone management,
- Intransparent or low-quality performance of contractual obligations,
- Poor internal control,
- Low motivation of workers due to low salaries and poor labour relations,
- Poor working conditions and low level of occupational health and safety,
- Removal of confidential data, information and documentation,
- Low level of responsibility,
- No security standards,
- People working at workplaces exposed to risk and with knowledge of confidential information have not been security-cleared,
- Non-compliance with security measures in the area of and at the facilities of contracting authority,
- Poor business results – insolvency and illiquidity,
- Slow response to changes and additional requests of contracting authorities,
- Ignoring of contracting authority's warnings about mistakes,
- No guarantee about the contractor's business continuity in the event of trouble or crisis,
- No priorities determined regarding the fulfillment of contractual obligations to different contracting authorities in an emergency response requiring multiple response, etc.

The above-mentioned and other outsourcing risks are an integral part of risks related to business, finance, information, communication, market, logistics and security. This fact is disregarded by many contracting authorities who are surprised to encounter problems in their outsourcing process. In order to avoid such surprise, the questions indicated above, which are related to the above-mentioned risks should be addressed prior to the selection of the best outsourcing provider. Therefore, the quality of products and services, and the reputation of contracting entity depend on the organization of outsourcing. Outsourcing risk management falls within the corporate management framework, where the project of risk management is also given priority.

To conclude, comprehensive risk management can be handled only by managers and experts who are well-educated, experienced, prudent, flexible, and who follow good practice. The owners and management of corporations, affiliated groups and business systems should be aware that a business result depends on successful risk management, and therefore invest more in respective human resources and computer technology which enables the identification, analysis and reduction of risk up to the point when a decision has to be made and that high risks (those which are difficult to manage) should be insured with an insurance company.

6. Conclusion

Organizations wishing to keep up with the competition and duly recognize the needs of the market must leave a part of their functions to outsourcing while not losing sight of the risks that this entails. This is particularly true for critical infrastructure, which also operates in the free market and must be subordinated to the laws of the market. People in these organizations who are responsible for risk management and management with an integral security system must establish an appropriate model of selection, implementation, operation and control over the operations of outsourcing because this is the only way to optimize the positive effects brought about by outsourcing and minimize and manage the risks and costs that it brings to the organization. In any case, during the first stage they must professionally judge which activities, from a security point of view, can be outsourced, and which operations despite the advantages brought on by outsourcing must be carried out on your own. Let me conclude by emphasizing once again that when introducing outsourcing, it is essential to integrate it into the business processes, the quality management system, safety standards, taking into account those business tools (such as benchmarking, business intelligence, BSC, HRM, CRM, SA 8000), which contributes to the positive business results, competitive advantage and reputation of the subscriber of the outsourcing.

References

[1] Greaver, M. F. (1999). *Strategic Outsourcing: A Structured Approach to Outsourcing Desicions and Initiatives*. New York. AMACOM.

[2] Kavčič, K. (2007). *Zunanje izvajanje dejavnosti: analiza slovenskih podjetij.* Koper. Univerza na primorskem. Management št. 4.

[3] Uršič, B. (2006). *Razvoj outsourcinga v podjetju Emo Orodjarna, d.o.o.,* diplomsko delo. Celje. Ekonomsko poslovna fakulteta Univerze v Mariboru.

[4] Stees, J. (1998). *Outsourcing Security: A Guide for Contracting Services*. Boston, Oxford. Butterwoth-Heinemann.

[5] Brown, D. (2005). *The Black Book of outsourcing: How to Manage the Changes, Challenges, and Opportunities*.

[6] Vitasek, K., Ledvard, M., Manrodt, K. B. (2010). Vested Outsourcing: Five Rules That Will Transform Outsourcing. New York, London. Palgrave Macmillan.

[7] Power, M. J., Desouza, K. C., Bonifazi, C. (2006). *The Outsourcing Handbook: How to Implement Successful Outsourcing Process.* Philadelphia, London. Kogan Page Limited.

[8] Kehal, H. S., Singh, V. P. (2006). *Outsourcing and Offshoring in the 21st Century: A Socio-Economic Perspective.* London. Idea GroupPublishing.

[9] Oshri, I., Kotlarsky, J., Willcocks, L.P. (2009). *The Handbook of Global Outsourcing and Offshoring*. New York, London. Palgrave Macmillan.

[10] Stanger, A. (2011). *One Nation Under Contract: The Outsourcing of American Power and the Future of Foreign Policy*. New Haven, London. Yale University Press.

[11] Lewis, T.G. (2006). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* Wiley InterScience.

[12] Murray, A. (2007). *Critical Infrastructure: Reliability and Vulnerability (Advances in Spatial Science)*. New York. Springer.

[13] Biringer, B.E., Matalucci, R. V., O Connor, S. L. (2007): *Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures*. New Jersey. John Wiley &Sons.

[14] Prezelj, I. (2008). Kopač, E., Svete, U., Grošelj, K., Sotlar, A., Kustec Lipicer, S., Žiberna, A.**,** Kolak, A. *(2008). Definicija in zaščita kritične infrastrukture Republike Slovenije: raziskovalni projekt: končno raziskovalno poročilo*. Ljubljana: Fakulteta za družbene vede, Obramboslovni raziskovalni center, okt. 2008. 526 str.

[15] Čaleta, D. (2010). *Oborožene sile in terorizem v luči konfliktov 21. stoletja*. Ljubljana. Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje Ministrstva za obrambo in Inštitut za korporativne varnostne študije.

[16] Bongard, S. (1994). *Outsourcing - Entscheidungen in der Informationsverarbeitung. Entwicklung eines computergestützten Portfolio-Instrumentariums*. Wiesbaden: Deutscher Universität Verlag.

[17] Borodzicz, E. (2005). *Risk, Crisis and Security Management*. New York. John Wiley&Sons.

[18] Vršec, M. (2011). *Pomen neprekinjenega poslovanja za poslovno učinkovitost organizacije s poudarkom na kritični infrastrukturi*. International Conference on Days of Corporate Security, Ljubljana. March 23-24th 2011. Ljubljana: Institute for Corporate Security Studies, 9–40.

[19] Vršec, M., Vršec Mir. (2009). *Obvladovanje hudih motenj poslovanja z načrtom neprekinjenega poslovanja in s kriznim načrtom*. Mednarodna konferenca Nove tehnologije, novi izzivi, Portorož, 25.–27. 3. 2009. Fakulteta za organizacijske vede, CD 1575–1587.

[20] Vršec, M., Vršec, Mir. *(2009) Sistemi in trgi poslovne varnosti.* Študijsko gradivo. Ljubljana. Fakulteta za varnostne vede, str. 311.

[21] Berk, A./Peterlin,J/Ribarič, P. (2005). *Obvladovanje tveganj – skrivnosti celovitega pristopa*. Ljubljana. GV Založba, Založniško podjetje, d.o.o., Zbirka Manager.

[22] Broder, J.F. (2006). *Risk Analysis and the Security Survey*. Boston, Oxford. Butterworth-Heinemann.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-45

Towards a Resilient Critical Infrastructure System against the Risk of Terrorism

Zoran KEKOVIĆ [a,1] and Vladimir NINKOVIĆ [b]
[a] *Faculty of Security Studies, Belgrade*
[b] *Transconflict Serbia*

Abstract. Terrorism is one of many sources of risk which may reduce the capacity of critical infrastructure organizations to deliver against their objectives. However, unlike more frequent and more predictable incidents like criminal offenses or natural hazards, terrorist acts are non-routine risks and therefore difficult to anticipate. Typically, non routine risks have low probability, that is, they occur rarely or in some instances have never occurred but have very high consequences for the organisation. The attack on CI can be particularly attractive for a terrorist organization or an individual due to its highly interdependent infrastructures and its often high symbolic value. Critical infrastructure resilience (CIR) is an integrating objective designed to foster system-level investment strategies. Three resilience capacities are used to define, quantify, and ultimately design for a better resilience of the particular system: (1) *absorptive capacities,* or the ability of the system to absorb the disruptive event; (2) *adaptive capacities,* or the ability to adapt to the event; and (3) *restorative capacities,* or the ability of the system to recover. Occasionally the magnitude of a crisis exceeds an organization's own ability to respond. At such times the intervention and assistance of external groups (including government, other businesses, and the public) can be decisive.

Keywords. resilient, terrorist threats, critical infrastructure, risk, capacity

Introduction

Critical infrastructure organizations operate within the environment of new and rapidly changing technologies, while also facing contemporary challenges, such as being placed under increasing pressure to manage risks to their operations while at the same time continuing to create shareholder value and deliver essential services to their customers. Some elements of critical infrastructure are not only fixed assets, but are, in fact, networks or supply chains with very complex interdependencies, due to which they have also become more vulnerable to disruption.

It has only been over the last few decades that organizations have invested heavily in risk management as a way of coping with complexity and uncertainty in an organizations' operating environment. Traditional approaches are sufficient for high levels of reliable performance in relatively stable, predictable and low threat environments characterized by reasonably foreseeable risk. While traditional planning provides a solid foundation for dealing with routine risks and uncertainty, organizations that rely excessively on it can find themselves underprepared for unpredicted, non-routine, disruptive and sometimes catastrophic events, including terrorist attacks. Terrorism is one of many sources of risk which may reduce the capacity of critical infrastructure organizations to deliver against their objectives. However, unlike more

[1] Corresponding Author: Dr. Zoran Keković, Faculty of Security Studies, Belgrade, e-mail: zorankekovic@yahoo.com

frequent and more predictable incidents like criminal offenses or natural hazards, terrorist acts are difficult to anticipate. Typically, non routine risks have low probability, that is, they occur rarely or in some instances have never occurred but may carry very high consequences for the organisation.

It is important to stress that for the purpose of this paper we define risk in line with the ISO 31000, i.e. we are interested in successful achievement of organization's objectives and goals: *"Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is "risk"* [1].

The scope of this paper encompasses organizational performance and building organizational resilience against non-routine risks, terrorist acts in particular. It does not address engineering challenges for designing infrastructure to achieve the outcomes of reliability, redundancy and robustness which are vitally important and addressed elsewhere in the literature.

Taking into account their rare occurrence, occasionally it seems too time and resource consuming, as well as economically unjustified to focus on the protection from some non-routine risks. Therefore, instead of a threat based approach, our hypothesis is that for non-routine risks, in this case – terrorism, the asset based approach with focus on a system's resilience may be a more viable option. However, as it is frequently the case in social sciences, the term 'resilience' is not easily defined. Numerous resilience definitions and evaluation approaches have been developed, many of them being domain-specific and, thus, not broadly applicable. The most convenient definition, in our opinion, is the one given by the Sandia laboratories which states that: "Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels" [2].

Furthermore, we suggest the framework of so-called 'resilience capacities' for the establishment of a methodology for measuring system performance level and recovery efforts, thereby determining and measuring system properties or capacities. Three such capacities are used to define, quantify, and ultimately design for better resilience of the particular system: (1) *absorptive capacities,* or the ability of the system to absorb the disruptive event; (2) *adaptive capacities,* or the ability to adapt to the event; and (3) *restorative capacities* or the ability of the system to recover. It is important to stress that this paradigm takes into account interconnectedness in networks of systems in the contemporary business and institutional environment, as, for instance, restorative capacities would be virtually non-existent, or at least far less efficient, without exogenous entities – for instance, emergency services.

We applied this framework to the analysis of resilience capacities of the London Underground and the London Emergency Services during and after the terrorist attack on the London Underground in 2005, using the data from the report written by the Greater London Assembly's Committee on the 7th of July Events. We also propose that this framework is used for analysis of system resilience to other non-routine risks, stemming from other threats, not only terrorism.

This paper consists of several key parts: a consideration of terrorism as non-routine risk and critical infrastructure system as target in which we will define non-routine risks, explain why we consider terrorism to be such risk, and give some reflections on why CI may be the preferred target for terrorist organizations and individual terrorists; in the second part of the paper we will deal with organizational response to a non- routine risk, explaining why in such cases 'business-as-usual' is not a viable option; in the third part we introduce the concept of 'resilience' and a paradigm of Critical Infrastructure Resilience as an integrating objective to the Critical Infrastructure Protection designed to foster system-level investment strategies and a qualitative analysis approach for evaluating resilience affecting system characteristics; finally, in the fourth part of the paper we will discuss three abovementioned resilience capacities – absorptive, adaptive and restorative, the application of this framework to the terrorist attack scenarios and its significance in the assessment of organizational networks, which are the key component in the organization's preparedness to a crisis.

1. Terrorism as a non-routine risk

1.1. Probability of a terrorist event

Unlike more frequent and more predictable incidents like criminal offenses or natural hazards, terrorist acts are difficult to anticipate. For criminal incident estimates we can use either criminal statistics or/and asset target value estimates. On the other hand, factors impacting the probability of a terrorist event are not constant in time, especially because the frugal world or regional politics are an inspiration for such incidents. Although some rough approximations can be made for specific regions, states, and even cities or their neighborhoods, it is almost impossible to specify the likelihood that a terrorist attack will occur with any definite statistical confidence at a particular time in the particular location. Historical data on previous occurrences are not the most reliable source in estimating terrorism risk, as the conditions driving terrorists may change over relatively short timescales. Even if the conditions remain stable, there is often very limited amount of historical data from which the probability or likelihood of a terrorist attack can be estimated. In statistics, this condition is called small sample space, and in such instances giving phony and misleading quantitative results should be avoided [3].

According to the last published EUROPOL report, there were in total 219 terrorist attacks carried out in EU member states [4]. Of these numbers, 125 attacks occurred in France and 54 in Spain, and are mostly related to separatist groups and individuals.[2] However, most of these attacks were small scale incidents, as in 167 separatist attacks in which a total of 2 persons were killed, whilst in 6 religiously inspired attacks 8 people died (7 during the assumed Al-Qaeda attack at the airport in Burgas). More than 40% of attacks in 2012 targeted private properties. Business targets have remained stable at 25%, whilst the proportion of attacks against government facilities slightly decreased compared with 2011 [4].

Given their relatively rare occurrence, there are no useful sources for estimating the probability or likelihood of the facility in question to be a potential target to a terrorist. Therefore, the key question is not how likely a terrorist event is to happen, but rather whether a specific facility is likely to be of interest to a terrorist organization or an individual. Again, due to the low number of these events, quantitative methods can be misleading and the scenario planning remains the best bet.

[2] Unfortunately, the report does not present data from the non-EU Balkan countries.

1.2. Planning for a terrorism event

Security managers and decision makers regard terrorism as a high-risk, low-probability concern that needs to be addressed on an irregular basis. This means that once the contingency plans, emergency procedures and business continuity plans are established, they can turn their attention back to the 'everyday crimes' and other day-to-day issues that threaten the organization's assets. However, situation is different in critical infrastructure assets, such as chemical plants, oil refineries, airports and maritime ports, where terrorist threat is considered to be significantly higher. Certainly, like other 'normal criminals' the terrorist will select the most vulnerable target and the one that will generate the highest 'yield' to their objective.

What we can sometimes predict are methods and tactics of the attacker, as most organized groups tend to maintain the same modus operandi throughout their existence. Particularly because attacks can be implemented in various ways and for different reasons, it will significantly affect the likelihood and the vulnerability components of risk. In devising scenarios, we must also think about what is and what is not technically possible, but we must always bear in mind that terrorists can occasionally find their way around technical difficulties or to get lucky only once.

Even though threat assessments are critical for security decision makers, not even the best assessment can anticipate every possible scenario, as terrorists always **adapt to the countermeasures** [5]. Hence, the scenario development of terrorist incidents requires the ability to walk in the terrorist's shoes. What we need to do is to try to put ourselves in the place of the terrorist and devise possible methods and targets, which would then serve us to prevent their occurrence or to mitigate their effects. It is more difficult to do with terrorists, than with, say, 'normal criminals' as we must place their way of thinking into ours, regardless of how far different from ours it may be. The goals and objectives of adversaries, i.e. terrorists, should continually be studied and their **motivation** and intent must be evaluated.

The motivation of terrorists is political, or more broadly speaking – ideological. Therefore, their targets are often landmark buildings or institutions that symbolize the object of their hatred. For instance, environmentalist groups attacked car dealerships that sold high-fuel-consumption sport utility vehicles or chemical factories and laboratories that experiment on animals, far right activists attacked gynecological clinics where abortions were performed. The biggest global terrorist organization, Al Qaeda, in particular targeted objects with high symbolic value – the World Trade Center, the Pentagon and the Twin Towers in New York City.

However, targets may not be of the same value to the owner and to the adversary. Usually, when evaluating **target values** the following factors should be taken into account: casualty and injury rates; asset potential for loss, damage or destruction; damage to the political landscape; disruption to operations; disruption to the economy; media attention; impact on the organization's reputation; impact to employees' morale; fear.

Another variable that can and should be assessed is the capability of the terrorist group in question. Terrorist capabilities may include highly trained and skilled military units, armed with explosives, even with unsophisticated nuclear weapons – 'dirty bombs'. They can also be trained in sabotage, hostage taking, assassinations, identity frauds – such as providing fake passports and driver's licenses, etc. **The capability of the adversary** will greatly influence the threat dimension of risk.

According to some authors, in the struggle against terrorism it is necessary to switch the focus from the 'causes' to background environmental factors that lead to radicalization [6]. For instance, the armed combat experience in the Middle East can be one of the main predictors of terrorist activity [7].

Also, in order to achieve its global goals, the international terrorist network very skilfully exploits local political and economic problems that burden the Balkan states. Therefore, a huge discontent with the factual situation on the ground, poor economic and social conditions, the actions of religious and other extreme groups, the existence of the infrastructure for the taking of terrorist actions and the lack of efficient legal institutions create an ideal environment for terrorist groups' activities. Another problem in this region is the strong presence of organized crime which is more often than not linked with terrorist and extremist cells.[3]

Last, but not least, opportunities can impact the threat level more than other factors, but the good side is, certainly, the possibility to **control the opportunities through careful monitoring of asset vulnerabilities**.

As we previously stated, it is difficult and almost impossible to quantify non-routine, extremely rare events such as terrorism. The threat level can be expressed in qualitative terms, which would depend on 'educated guesses' of experts. The most common way of expressing the risk level of terrorism is through threat-rating scales, of which, perhaps, the best known is the Homeland Security Advisory System with five color-coded levels indicating the risk level (from green to red). However, as we can see from these several paragraphs, thorough and detailed terrorist threat assessment is time and effort consuming with, more often than not, questionable results, and may not be economically viable and a justifiable option for many organizations, including those that are part of the critical infrastructure, at least on the local, regional and national levels.

1.3. Critical infrastructure system as a target

One of the most significant dilemmas that any management has is the prediction of targets for a terrorist attack. Where will the attack take place? Will the target be human or simply physical objects? Will the targets include buildings or people associated with foreign countries, foreign investments, or simply because they are representative units of a larger group defined as enemies by the terrorists?

Terrorist groups are rational in their choice of targets; they evaluate strengths and weaknesses, costs and benefits [8]. Some targeted buildings could have a symbolic value, and their damage or destruction would indicate that any part of a society is vulnerable. In that sense, critical infrastructure buildings as targets represent the government's inability to effectively protect obvious targets, from which it results that it does not seem likely that it will be able to guard the less obvious ones.

An attack on CI can be particularly attractive for a terrorist organization or an individual due to its highly interdependent infrastructures. It is almost impossible to find self-sufficient individual infrastructures, as they normally exist together as a subsystems or "systems of systems", in which two or more infrastructures interact with one another and are connected via physical, cyber, and logical interdependencies. "Systems of

[3] Arguably, in this region, the terrorism threat mainly comes from the Islamist, secessionist (Kosovo and the surrounding areas) and far right extremist milieu. For more detailed discussion see [7].

systems" are defined as sets of multiple, but independently operational systems that must interact effectively with one another to meet specific needs.

Identifying and quantifying the different types of interdependencies, such as intra-regional, inter-sectoral, and public-private interactions was emphasized after the terrorist bombing of the World Trade Center in New York City and the federal building in Oklahoma City in the mid-1990s. Recognizing the possible threats to the national infrastructures and security of the United States, President Clinton established the President's Commission on critical infrastructure protection (PCCIP) in 1996 represented by both federal departments and private sector agencies. Because of the increasing dependence of CI and an increased vulnerability to physical disruption and cyber threats, the commission focused on threats and vulnerabilities in five sectors: Information and Communications, Banking and Finance, Energy, Physical Distribution, and Vital Human Services.

Interdependencies increase complexity and vulnerability and consequently the physical disruption effects caused by terrorism. A simple example of this would be the interdependency between the transportation and energy systems. These two systems interact mainly at two different stages: operation and investment. At the operational level each system needs to satisfy its demand with the existing capacity: while the transportation sector demands energy in the form of fuel, the energy sector requires the movement of raw bulk energy source (e.g. coal or natural gas for thermal power plants). Due to reciprocal demands, the interruption of operation each of these sectors has an impact on the energy-transportation supply chain. Given the potential for increased performing together between energy and transportation, the attractiveness of both of these infrastructures as potential terrorist targets is evident. Even the effects of such physical disruptions can be maximized if the terrorist scenario is designed to exploit coupling interdependencies.

2. Organizational response to a non-routine risk

There has been a growing interest in the organisational response to non-routine risk. Whether it is risk, business continuity or crisis management, the emergence of interest in these fields is a good measure of increasing concerns in this area. The governance challenge is how to reconcile the divergence or lack of coherence between the fields that have evolved to deal with organisational response to risk of shocks. There appears to be little research about how these various perspectives can be integrated within an effective governance framework. This issue is rarely addressed in the organisational literature so carrying out research in this area will be very important.

The OECD defines governance as *"the system by which entities are directed and controlled"*....and goes on to state *"the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined"* Risk Management is a fundamental element of governance, that is the achievement of objectives. "*Risk management should ensure that organizations have an appropriate response to the risks affecting them. Risk management should thus help avoid ineffective and inefficient responses to risk that can unnecessarily prevent legitimate activities and/or distort resource allocation"* [1].

When it comes to planning and organizing the protection of critical infrastructure, it is crucial to understand that the protection is not an end by itself, but a means of ensuring the conditions for the prevention of undesirable events and for keeping business continuity in case such events occur. Thus, instead of putting infrastructure itself as a physical entity as an object of protection, the supreme goal should be the protection of services they provide [9].

One way to understand non-routine risks is to deconstruct the problem into two separate parts: the strategic environment and the capacities of the organization. An environment that emphasizes terrorism as a non-routine risk requires the warning “capacities” that deal with the inside of the organization - its ability to collect, process and distribute warning. Figure 1 can be used as a starting point for discussion among senior management and their staff about what it is they want from warning of whether they find themselves in a stable or unstable strategic environment.

Organization’s warning capacities	Strategic environment	
	Stable	Unstable
Increasing		
Decreasing		

Figure 1. A framework for warning [10].

However there is a fundamental challenge that organisations have been conceived primarily as devices for reducing uncertainty [11]. According to Boisot: “They achieve this by creating zones of stability, structures that can maintain their identity over time in the face of external variations” [12]. However, if the external variation is a shock, then expecting organisations to seamlessly shift from one state to another is problematic, at best. If organisational survival depends on the rate of learning being greater than the rate of change in the environment, then a crisis or disaster with a very rapid rate of change and a very compressed time frame can be very challenging [13].

Non-routine risks generate conditions where numbers of people and organisations (sometimes large) have to work together in a non-routine way. They may not have even met each other before, much less be experienced in working together [14]. The range of tasks, objectives and working environment may be substantially different from their normal workplace. “It is vital that the people involved in the response have received sufficient opportunity beforehand in the planning stage to form effective relationships with those people that the emergency will thrust together intra-and inter-organisationally” [15].

The challenge is what organisational structures or system would be appropriate for an organisation that has to make significant changes in the way it utilizes assets, people and other resources. The work by Kreps and Bosworth on organisational adaptation to disasters in a community context is a valuable source of understanding the reorganisation process inside entities [16].

3. Organisational resilience and the new challenges of managing risks

The concept of critical infrastructure resilience has become a key component of the nation’s CIP policies for decades. Largely due to the terrorist acts of September 11, 2001, governments are now concerned about how these systems perform during and after natural and manmade disruptive events, such as hurricanes (e.g., Katrina, Ike) pandemic influenzas (e.g., H5N1, H1N1), chem.-bio attacks, and many others. Following 9/11, the U.S. Department of Homeland Security explicitly focused its efforts on protecting CI from acts of terrorism by stating Presidential directives and charging the Homeland Security Advisory Council to ensure recommendations for the optimal delivery of CI service in the post-9/11 "all hazard" environment. "We cannot protect every potential target against every conceivable attack; we will never eliminate all vulnerabilities. Furthermore, it is virtually impossible to define a desired end state – to quantify how much protection is enough – when the goal is to reduce vulnerabilities. Critical infrastructure resilience (CIR) is not a replacement for CIP, but rather an integrating objective designed to foster system-level investment strategies. It is businesses that must bear the costs of resilience, which must make cost/benefit decisions in a changing, competitive environment" [17].

The overarching goal of the Department of Homeland Security National Infrastructure Protection Plan is to: [...] build a safer, more secure and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CI and key resources (CIKR) and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of attack, natural disaster, or other emergency [18].

The resilience framework formulated by Sandia National Laboratories includes a definition of resilience and system performance metrics and measurement methodology which can be applied to studies of natural and man-made disruptive events. The proposed definition of system resilience is: "Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels." [2]

However, it must be stated that there is no 'one-size fits all' template for organizational resilience – this would fail to address the complexities of different corporate environments and characteristics, regulatory environments, stakeholder expectations and organizational obligations. It is for this very reason that resilience is different for each organization.

Taking all of this into account, we can ask the following question: What are the opportunities to enhance organisational performance and improve the potential for an organisation to survive a shock while continuing to achieve its aims and objectives whether in the public, private or not for profit sectors?

The following question then arises: Can all risks be managed through the normal processes of the organisation? The vast majority of risks have consequences which can and should be managed through routine processes in an organisation. However there are risks that cannot be managed in this way, the consequences are so great that business as usual is not a viable option. What approaches, structures and systems are needed to manage this group or family of risks?

As we have pointed out, non-routine risks have low probability, that is, they occur rarely or, in some instances, have never occurred but have very high consequences for the organisation. This can be represented graphically using a risk spectrum shown in Figure 2. At one end there are minor risks easily managed through routine processes often described as incidents; at the other end of the spectrum there are catastrophic risks and there is a threshold along the spectrum between routine and non-routine risk. The threshold is defined by changes in the organisation's or system's performance, not on absolute values. A situation in an isolated small organisation may force it into non-routine activity whereas the same event might be a minor incident in a large organisation and easily handled through routine processes.

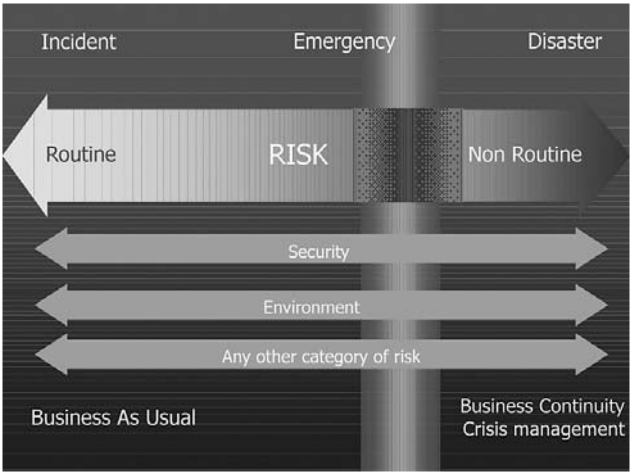


Figure 2. Risk Spectrum [19].

4. Absorbent, Adaptive and Restorative resilience capacities against terrorism

The above proposed resilience framework creates a methodology for measuring system performance level and recovery efforts, thereby achieving the overarching goal of more resilient CI systems, determining and measuring system properties or capacities. Three such capacities are used to define, quantify, and ultimately design for better resilience of the particular system: (1) *absorbent capacities,* or the ability of the system to absorb the disruptive event; (2) *adaptive capacities,* or the ability to adapt to the event; and (3) *restorative capacities,* or the ability of the system to recover.

The absorbent and adaptive capacities are probably the most important in the initial stages of large, widespread disruptions, where repair of the system might be impossible in the short term.

The **absorbent capacity** is the degree to which a system can automatically absorb the impact of system perturbations and minimize consequences with little effort. The absorbent capacity is an endogenous feature of the system. For example, a storage can enhance the absorbent capacity; if a chemical plant is disabled but a large amount of collocated storage of its product is undamaged, customers can continue to be supplied by the stored quantities, with little cost to the producer or customer, while the plant is repaired." [2]. Examples of resilience enhancement features that can increase the absorbent capacity include system robustness and system redundancy.[4]

Adaptive capacity is the degree to which the system is capable of self-organization for recovery of system performance levels. It reflects a dynamic ability of the system to change endogenously throughout the recovery period. Consider the scenario in which terrorist act destroys high voltage power lines, leaving many customers without electricity. Having customers with emergency generator enhances system adaptive capacity because the system can be changed (customers adapt to the disruptive event by generating power

[4] System robustness decreases system impact through the strength of individual connections in the system, whilst system redundancy decreases system impact through providing alternate pathways for the system mechanics to operate.

from a fuel source like gasoline rather than connecting to the electric grid) so that some portion of system performance is regained at a relatively low amount of effort [2].

Adaptive capacity from the emergency services should be also considered, as the structure of these services can radically be changed during a disruptive event.

The **restorative capacity** is the ability of a system to be repaired easily. These repairs are performed by entities exogenous to the system (e.g. emergency services). These repairs usually restore the system to near its original, pre-event state, but can also restore the system to a completely new state of regime that anticipates future system requirements. For example, the electric power grid has monitoring systems that can automatically detect when and where a break in the grid emerges. Such technologies enhance the restorative capacity of the power grid because repair crews can be sent to the location of the break. These technologies result in a shorter disruption that is easier to repair (in terms of cost and time) then it would be if crews had to search large portions of the grid to find the break before repairing it [2].

As the restorative capacities reflect the ability to be repaired exogenously, in the event of a crisis, emergency responders must determine what has happened and where it has occurred.

4.1. The importance of networks for organizational resilience

In today's interconnected and complex business environment, organizations depend heavily on business partners, supply chains, and distribution networks for the continued achievement of their goals. Whenever the magnitude of a crisis exceeds an organization's own ability to respond, the intervention and assistance of external groups (including government, other businesses, and the public) can be decisive.

During unforeseen events (and especially high impact events) the ability to rely upon these networks becomes even more important in enabling the rapid adaption to and recovery from disruptive circumstances. Organizations develop resilience networks by cultivating trusted relationships with business partners to strengthen their entire value chain including upstream and downstream dependencies.

Frequently, there is very little time during the onset of a disaster to finalize the type of commercial and legal arrangements that normally precede this type of collaboration. Trusted partners can often be called upon to 'go the extra mile' during crisis circumstances to provide critical inputs and assistance.

The system interdependences can affect resilience capacities. We can explain that with the following example that represents the system interdependencies between the two CI systems: Energy sector (A) and Bridge building sector (B).

- **Absorbent capacities**: If system B is dependent upon system A (producing fuel oil as a component for bridge building) to operate, then this relationship will lower system A
- **Adaptive capacities:** System A may have adaptive capacities (which alter the existing supply chain of oil derivates) that allow the system to reorganize to reduce its dependency upon system B
- **Restorative capacities:** The operation of system A may not depend upon the functionality of system B, but the repair of the components of the sector may require system B to be operational. In such cases, the restorative capacity of system A is diminished. Additionally, the repair of multiple sectors must

often be coordinated (for example, where infrastructures are collocated in urban areas), which further reduces institutional capacity by increasing the complexity of repair.

4.2. Applying the assessment resilience framework to a possible terrorism scenario

Capacities can be identified for classes of disruptive events. The example of the London bombing can be used as a catastrophic scenario to describe resilience capacities within each system, as well as system dependences across systems that can affect resilience capacities.

The London bombing on 7th July 2005 caught the British authorities completely by surprise. The terrorist struck the center of London on four different lines at the height of rush hour at a symbolic moment.[5] The incident took place at multiple locations throughout a vast urban subway system, making the spatial determination a real challenge. If the incident occurs in a tunnel between stops, both station will report that something has happened, creating the mistaken impression that one incident is in fact two. Once the authorities determine that the incident is terrorist attack, they face additional questions. They must first determine the nature of the attack. A bomb blast is certainly an explosion, but it may also be the means of dispersing chemical, biological or radiological agents. Next, they need to find out if the attack is over or still unfolding. Terrorists have frequently used a secondary device to kill emergency workers responding to the initial attacks. Answering the questions, “what, when, and how” will determine which resources responders send to the site of an attack and which they hold in a reserve [20].

Figure 3 contains the results of the ex-post resilience assessment for the two systems: urban subway system and emergency services. The objective of this resilience assessment is to provide a qualitative evaluation of the resilience of the systems to a terrorist attack. To achieve this objective, the researchers need to perform the following steps by interviewing subject matter experts:

- *Identify system and subsystem(s) of interest:* Systems are often composed of subsystems that would be best analyzed separately.
- *Identify system performance metric(s):* The most purposeful system performance metrics, from the perspective of the relevant stakeholders, should be chosen. For example, for the purposes of the NISAC study in 2009, the percentage of customers with working electric power was more relevant to the Department for Homeland Security than the profitability of power companies [21].
- *Assess or simulate the recovery effort:* Because the recovery path is a function of the recovery effort, identifying both will likely follow similar qualitative or quantitative methods.
- *Identify resilience enhancement features of the systems and assess resilience capacities*

The evaluation and results for the resilience capacities of each system could be qualitative assessments (high, medium, or low) gathered in a single resilience matrix as described in the Figure 3.

[5] The leaders of the G-8 countries were meeting in Scotland on the day of the bombings.

<table>
<tr><th colspan="4">Resiliency Matrix: Terrorism Scenario Analysis Example
- Assessment of the response --</th></tr>
<tr><th>System</th><th>Absorptive capacities</th><th>Adaptive capacities</th><th>Restorative capacities</th></tr>
<tr><td>Urban Subway System</td><td>LOW</td><td>LOW</td><td>MEDIUM</td></tr>
<tr><td>Emergency services</td><td>MEDIUM</td><td>HIGH</td><td>MEDIUM</td></tr>
</table>

Figure 3. Resiliency Matrix [22].

Urban Subway System:

- Absorptive capacities: *Low.* The terrorism damaged underground facilities, thus having a large initial systemic impact.
- Adaptive capacities: *Low*. Since mobile phones do not work underground, people closest to the incident sites could not report what had happened. Passengers and train drivers could not communicate with one another, and train drivers could not communicate with the Network Control Center. The lack of basic first aid equipment of any of the trains. A number of passengers had varying degrees of first aid training, including formal military and medical training, enabling essential treatment to be provided (such as applying improvised tourniquets and makeshift bandages) and to remain calm and collected in the face of potential panic, chaos and desperation.
- Restorative capacities: *Medium*. There were no monitoring systems that could automatically detect what and where had occurred (the location of the explosions in the tunnel). Strategic oversight of the emergency worked reasonably well. The authorities took steps to evacuate the subway system, and less than hour after the incidents had begun they determined that they were the result of a terrorist attack on multiple targets, but had no way of knowing whether the attack was over. The first emergency responders had no way to verify whether chemical, biological, or radiological weapons had been used in conjunction with the conventional bombs. The London Ambulance Service put hospitals on "major incident standby" to create "rendezvous points" in case there was CBRN risk. Deployment of fire engines and ambulances to the bomb sites occurred at a very high rate. Too many ambulances were sent to that scene, compromising the ability to evacuate the wounded at other sites. The responders failed to distribute the wounded evenly throughout the London hospital system, and did not notify some of the hospitals closest to the incident sites.

Emergency services:

- Absorptive capacities: *Medium*. Emergency services facilities were not destroyed. Uncertainty about the possible presence of CBRN made entering the Underground tunnels potentially more hazardous. The responders could not have been certain that there was no radioactive material. Delaying until the proper equipment arrived (hazard suits, etc.) might have cost of those seriously wounded.
- Adaptive capacities: *High*. Emergency responders were numbered and equal to the task, regardless of their experience, whether probationers or seasoned professionals, whether fire-fighters, paramedics, or policemen, off duty or on. Some emergency services functions such as search and rescue were supported by community members.

- Restorative capacities: *Medium.* The lack of communication among different emergency responders. The Metropolitan Police Service, The London Fire Brigade, and the London Ambulance Service each made their own determination at each site and often at different times as to when a major incident should be declared. The emergency responders did not follow procedures for handing uninjured persons over to the Police for collation of details and witness statement specified in their own guidelines.

Modeling the likely outcomes of different terrorism attacks allows one to estimate the effectiveness of resilience capacities and, accordingly, different defensive responses. Modeling efforts over the past decades have tended to emphasize worst-case scenarios. While such scenarios may be possible under the right circumstances, they are probably less likely than localized threats, which is the most important for immediate response to a terrorist attacks, assessing and addressing restorative capacities to this attack. For instance, a chemical attack might destroy multiple hospital emergency departments or contaminate them to such extent that they could no longer be used. The biological attack could quickly spread to medical personal, thereby effectively destroying their capacity to respond [23].

5. Conclusion

Continuous, reliable operation and resilience of critical infrastructures is crucial for maintaining national security, economic prosperity, and quality of people's life. The trends are clear, turbulence, complexity and uncertainty in our environment are only going to grow. Rather than eliminating all threats or hardening all assets, it may be desirable to bolster resilience in CI systems so that the functions of those systems can be maintained during and after disruptions – both natural and manmade.

At the heart of the problem is the organisation; the building blocks of our society and economy. How can sufficient learning and capacity building keep up with change? How can effective transformational and adaptive capacity become institutionalised and a core part of good governance of organisations [24]? *" Taking this broader view which sees learning as a cultural activity of organisations helps us explore a less instrumental more reflexive aspect of institutional resilience in the face of the future."* [25]. Learning and capability development are key themes that emerge from researchers and thinkers across this incredibility broad and diverse field, whether at individual, team or organisational levels and across networks.

As non-routine risks are rare and unpredictable, the improvement of absorbing, adaptive and restorative resilience capacities seems like a viable option to preparing and protecting against all potential threats. It should not be over stressed that terrorism is only one among the vast array of non-routine risks to which this assessment framework can be used. This method we applied in the case study of the unfortunate London Bombings of 7th July 2005, by assessing the three resilience capacities of the London Underground and the emergency services. The case study not only showed the importance of functional and operational resilience capacities of the system under attack, but also the importance of the organizational networks and the resilience capacities of the organizations and systems encompassed in that network.

References

[1] *ISO 31000:2009,* Risk management – Principles and guidelines,

[2] E.D. Vugrin, *A framework for assessing the Resilience of Infrastructure and Economic Systems.* In: Sustainable and Resilient Critical Infrastructure Systems, Springer, 2010, p.83.

[3] C.S. Young, *Metrics and Methods for Security Risk Management*, Burlington, MA, Syngress-Elsevier 2010.

[4] *TE-SAT – EU Terrorism Situation and Trend Report*, Deventer, European Police Office, 2013.

[5] T. Norman, *Risk Analysis and Security Countermeasure Selection*, Boca Raton: CRC Press, 2010.

[6] R. Korteveg, et al (2010) – *Understanding Violent Radicalization: Terrorist and Jihadist Movements in Europe*, London ; New York : Routledge, 2010.

[7] V. Ninković, Z. Keković, I. Vasović, *On-lajn poziv u D*žihad – radikalizacija putem Interneta,u: Savremene politike i sistemi kriznog upravljanja, 7th International Conference, University of Applied Sciences Velika Gorica, 2014.

[8] David Long. *The Anatomy of Terrorism,* New York: Free Press, 1990, p.139.

[9] Z. Kekovic, S. Vučić, R. Despotovic, N. Komazec, Compliance of education programs with the need of protection national critical infrastructure, In: Z. Keković, D. Čaleta, Ž. Kešetović, Z. Jeftić, *National Critical Infrastructure Protection,* Faculty of Security Studies, Belgrade, Institute for Corporative Security Studies, Ljubljana, 2013, pp. 201-217

[10] P. Bracken, How to build a warning system*, Managing strategic surprise*, Cambridge, 2008, 16-43

[11] H. Simon, *Administrative Behaviour*, New York, Macmillan, 1961.

[12] M. Boisot, *Preparing for Turbulence:* in Garratt, B. (Ed) Developing Strategic Thought. London, Profile Books, 2003, p.54.

[13] W.R. Ashby, *Self regulation and Requisite variety in Introduction to Cybernetics* Wiley London, 1958.

[14] E. Borodzicz, *Risk, Crisis and Security Management,* Chichester, Wiley, 2005.

[15] M. Crichton, C. Ramsay, and T. Kelly, Enhancing Organisational Resilience Through Emergency Planning, *Journal of Contingencies and Crisis Management* Vol 17 (1), 2009, p.33.

[16] G. Kreps, and S. Bosworth, Organisational Adaptation to Disaster in H. Rodriguez, E.L. Quarrantelli, and R.R. Dynes (Eds) *Handbook of Disaster Research*, Springer, New York, 2006, pp 295-315

[17] Homeland Security Advisory Council, *Report of the Critical Infrastructure Task Force*, US Department of Homeland Security, Washington DC2006.

[18] *National Infrastructure Protection Plan*, US Department of Homeland Security, Washington DC, 2009.

[19] M. Tarrant, The organization: Risk, Resilience and Governance, *The Australian Journal of Emergency Management* Volume 25, No. 02, 2010

[20] T.R. Mockaitis, *The London bombings: A case study in effective consequence management.* In: Managing the Consequences of Terrorist Acts – Efficiency and Coordination Challenges, Institute for Corporative Security Studies, Ljubljana, and Center for Civil-Military Relation, Naval Postgraduate School Monterey, USA, 2012, p.42.

[21] The DHS National Infrastructure Simulation and Analysis Center. As a part of NISAC program, a multi-year project to evaluate the potential impacts resulting from a large earthquake was performed. Source: http:/earthquake.usgs.gov/regional/ceus/products

[22] *Report of the 7th July Review Committee* , London: Greater London Assembly, 2006, 12

[23] D.Nikolić, A.Kovačević, S.Stanković, *Comprehensive approach to tactical response in case of terrorist acts involving WMD,* In: Managing the Consequences of Terrorist Acts – Efficiency and Coordination Challenges, Institute for Corporative Security Studies, Ljubljana, and Center for Civil-Military Relation, Naval Postgraduate School Monterey, USA , 2012, p.106.

[24] A. Podger, Innovation with integrity – the public sector leadership imperative to 2020, *Australian Journal of public administration* 63 (1). 2004; F. Kettl, The Future of Public Administration *Report of the Special NASPAA/American Political Science Association Task Force,* 2003; G. Hamel, L.Valikangas, The Quest for Resilience *Harvard Business Review* Sept 2003; B. Garratt, (Ed) *Developing strategic thought*, London, Profile Books, 2003.

[25] B. Turner, and N. Pidgeon, *Manmade disasters*. London, Wykeham, 1997 p.195.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-59

The Risk of Terrorist and Violent Extremist Attacks against Schools

Petra VEJVODOVÁ [a,1] and Miroslav MAREŠ [a]
[a] *Department of Political Science, Faculty of Social Studies, Masaryk University, Brno*

Abstract. The contribution focuses on terrorist and violent extremist attacks against schools and pupils in Europe. Discussed are the reasons why schools can serve as targets, what kind of danger is represented, in which context of political extremism and terrorism, and what consequences and challenges it brings in the issue of managing terrorist threats (the possibility of early warning mechanisms, prevention and preparedness). The emergency plans of American schools are considered as good practice.[2]

Keywords. schools, violent extremism, terrorism, civilian threat, prevention

Introduction

In recent years countries and societies have been dealing with mass casualty events resulting from terrorism. Mainly due to September 11, 2001 terrorism has become a phenomenon, which in the last few years the media have paid attention to on a daily basis. Terrorist acts are happening with alarming frequency, with escalating intensity and with a lot of, in many cases, innocent victims. Death, fear, anxiety and uncertainty spreading through the media affect the psyche of hundreds of thousands of people and influence public opinion [1][2][3].

Although acts of terror affect all age groups of the civilian population, some of them focus only on harming children. Children are the casualties in many of these events. Schools are the ideal place for terrorist attacks because of the large number of people concentrated in one place for many hours on a daily basis. They are among the so-called 'symbolic targets' of terrorists and extremists. In addition, they require consideration as such attacks typically afford their perpetrators significant media attention. And more, they serve as 'easy / soft targets', as they are relatively easy to assault.

The probability of attacks on educational institutions has been demonstrated several times worldwide. In 1974 terrorists killed 21 school pupils and many others injured in the Israeli town of Ma`alot. The largest event in recent years took place in the year 2004 in the Russian city Beslan, where terrorist attacked the school of 7- to 18-year old pupils and took them hostage. When the first plane hit the northern tower of the World Trade Center in New York on September 11, 2001, there were four elementary schools and six high schools several blocks away [4].

[1] Corresponding Author: Dr. Petra Vejvodová, Department of Political Science, Faculty of Social Studies, Masaryk University, Brno, e-mail: vejvodov@fss.muni.cz

[2] This contribution was prepared as part of the research project "Methods of Predicting Long-term Geopolitical Development in Central Europe" (VF20102015005), financed by the Ministry of the Interior of the Czech Republic.

However, in the history of terrorism, acts of terrorism and violent extremism targeting schools or facilities and individuals associated with schools have not been a common occurrence. Nonetheless, due to the horrific nature of such acts, most of which are against innocent children, they deserve our attention. The terrorist attacks have had a serious negative long-term impact on children physically, mentally, and socially. It is accepted that disasters and emergencies can have devastating effects on children and families. Studies over the past few decades have documented the prevalence of a variety of post-trauma psychological reactions among children and adolescents after mass violence that occurs immediately or some time after the experience. As a group, traumatized children manifest significantly higher rates of behavioural and emotional problems than non-traumatized children. Common problems include complicated bereavement, somatization, depression, anxiety, aggression, eating disorders, diminishing self-efficacy and self-esteem, learning problems, disturbances in moral development and conscience functioning and many others [5].

The frequency of terrorist acts is high worldwide and this is a fact that forces preparation for the difficult tasks of coping with them. This contribution reflects the issue of terrorist attacks against schools and in the first part brings the overview of the main types of attacks known from recent histor y to show what kind of threats can be aimed at schools and children. What kind of attacks we should be aware of. It means that the first part is based on empirical findings. The second part introduces the possibilities of prevention and preparedness based on the American experience. Many American schools are let to prepare emergency plans covering terrorist attacks. Non-governmental organizations focusing on school safety help them. The second part is meant as an overview of some basic safety rules and recommendations.

1. Types of attacks

1.1. Attacks on school buildings

The Israeli nation has had substantial experience with terrorism targeting schoolchildren, primarily committed by Muslim radicals. Between 1968 and 2004, fifteen such terrorist acts were committed in Israel, killing 92 and injuring 21 children. All these acts were either directed towards the school itself or a school bus [6].

Among the most tragic was the 1974 Ma'alot school massacre, when Arab terrorists dressed as Israeli soldiers killed 21 children. Since then, the state of Israel has placed armed security staff in every school, armed guards attend every school trip or sports event, and armed security forces are present on buses [6]. In the 1990s, however, the terrorists' tactics changed and they began increasingly to target school buses. Although the buses were escorted by the armed forces, they were an easier target than school buildings themselves. From March 1997 to June 2004, ten of the twelve recorded terrorist attacks on schoolchildren were direct towards a school bus [6].

In April 2003, an explosion took place at a high school in the city of Jenin on the West Bank, and almost 30 students were injured. Responsibility for the attack was claimed by the Jewish radical organisation Nikmat Olelim (Revenge of the Infants). The attack was allegedly a revenge attack in retaliation for the Jewish children killed by Palestinian terrorists [7].

In December 2004, a bomb damaged a Muslim elementary school in Eindhoven in the Netherlands. On this occasion no-one was killed or injured. At the time the police linked the attack with the recent killing of the filmmaker Theo van Gogh, who was a harsh critic of Muslims [8].

More recent was the June 2013 attack on a school in the city of Maiduguri in north-eastern Nigeria. The attack was preceded two days earlier by another targeting of a high school in the city of Damaturu, also in the north-east, in which seven students, two teachers and two attackers perished. In Maidiguri, members of the Boko Haram sect entered the hall in which final exams were being held and opened fire in all directions. Nine pupils died. The members of Boko Haram committed the attacks in revenge for the youth's cooperation with the army, which had previously launched a large-scale offensive against Boko Haram. In certain regions, young people had also signed up for voluntary patrols informing the army of individuals suspected of belonging to the rebels [9].

1.2. Attacks on schoolchildren in the vicinity of a school

A case dating from 2001 can also be classified into the category of terrorism aimed at schoolchildren. In September 2001, violence was committed against the pupils of a Catholic girls' school and their parents in the northern part of Belfast in Northern Ireland. The main entrance to the Catholic school was located in the Protestant section of the city. Parents and pupils, therefore, used a side entrance, which did not exit into the Protestant sector. On the first day of school, some parents and children decided to access the school using the main entrance. A group of Protestants blocked their way, throwing stones and bottles at them and injuring two women. The tension then escalated further and a bomb was detonated near the school. Fortunately, no children were injured, yet the experience was a traumatic one. Responsibility for the incident was claimed by the organisation Red Hand Defenders, which is a name used as cover by the extremists of the Ulster Defence Association, Ulster Freedom Fighters and Loyalist Volunteer Force [10][11][12].

1.3. Attacks on school buses

According to data provided in 2007 by the organisation Safe Havens International, terrorists commonly attack transport, and attacks against them comprise 42% of such targets worldwide. Attacks on buses account for 40% of cases. Moreover, globally, 37% of attacks on schools targeted transportation [13]. The reason why buses are chosen is simple. First, they make easy targets as they are mostly unprotected, and as such are not costly for the terrorists to attack. Second, the drivers are usually not trained specifically on how to respond to the eventuality of a terrorist attack. Third, they provide a symbolic target.

In May 1994, four Chechens armed with grenades and firearms hijacked a bus filled with teachers, parents and children in Southern Russia. The hostages were later released after a multi-million dollar ransom was paid [7]. In November 2000 a bomb targeting a school bus exploded in the Gaza Strip settlement of Kfar Darom, killing two passengers and wounding twelve others; including five school children [7]. In March 2002, a terrorist suicide bomber killed seven and wounded a dozen more when he blew himself up on a bus frequently used by Arab and Jewish school children, many of whom were injured [7]. And, in June 2002 two students were murdered and fifteen wounded by a gunman believed to be from an ethnic minority Karen rebel group, in an attack on a school bus in Thailand [7].

1.4. Hostages

The occupation of a school in Beslan provides a typical example of this type of terrorist attack. On 1 September 2004, Chechen Islamist separatists seized a school in the South Ossetian city of Beslan in the south of the Russian Federation. As this was the first day of school, there were more people in the school than usual. The terrorists captured about 1200 hostages (children, teachers and parents) and held them in the school's gymnasium. On 3 September, a bomb exploded at the school, killing at least 330 civilians, 10 members of special units and 31 terrorists. 186 of the victims were children, and 783 were injured. Responsibility was claimed by the Chechen leader Shamil Basayev [14][15].

1.5. Kidnappings of schoolchildren

A very recent case falls into this category: on 14 April 2014 the organisation Boko Haram abducted more than 200 girls from a boarding school in Chibok, Nigeria [16]. The Islamist militants have claimed responsibility for the abduction, and their leader has threatened to 'sell them in the market' [17].

1.6. Patrolling

This type of aggression against schools is associated with the activities of violent extremists only, who by their paramilitary actions are seeking to challenge the security forces of the state. In Europe, an instance of such patrols in schools was recorded in the Czech Republic. In June 2008, the paramilitary unit, the National Guard, created by the extreme right National Party, announced its intention to patrol in front of elementary schools in the city of Karlovy Vary. The task of the National Guard was to watch over 'white' children and 'protect' them from the children of Romani families. Fearful of the National Guard, several Romani pupils then left the schools patrolled [18]. The National Guard ceased its patrols at the end of the school year, and there is no doubt that its presence heightened inter-ethnic tension.

1.7. Other: Poisoning of food and water

In April 2012, water was poisoned at a Girls School in Rustaq district, Takhar province in Afghanistan. 150 students and 21 teachers were injured, although there were no casualties. In May of the same year, water was poisoned in another girls' school, at Bibi Jajera High School, in Taloqan, also in Takhar province, Afghanistan. 80 students, three teachers and one member of staff were hospitalised. Four days later the attack was repeated, at this time 40 students were affected; again, fortunately there were no casualties [19].

2. Possibilities of prevention and preparedness

Although one hundred percent protection against terrorist attacks is not possible in any area and at any potential target, schools do have means at their disposal to, at least partially, reduce the possibility of, and the damages caused by, such an attack.

Chris Dorn has emphasised that schools should first implement 'Emergency Operation Plans', developed based on 'Emergency Management' and 'First Responder Input' scenarios. Such plans should cover as many potential variants as is feasible, and be repeatedly tested for reliability; staff obviously also need to be familiar with possible approaches [13]. Naturally, this does not solve the problem of terrorist attacks on schools; it is merely a tool that might reduce their impact.

Dorn also presented the 'All-Hazards Four Phase Model', dealing with various possible scenarios by employing the following four phases:

- Prevention/Mitigation
- Preparedness
- Response
- Recovery [13]

This is a cyclical process involving planning and testing, where on the completion of a cycle results are evaluated and the process involved is adjusted accordingly. The model deals with potential incidents, such as armed assault, hostage-taking, an explosion or the threat of a bomb attack, a natural disaster and fire.

In the **Prevention/Mitigation phase**, Dorn referenced areas such as good physical security, increased surveillance, school safety zone enforcement measures, visual/mechanical weapons screening and good computer/information/route security. When ensuring **Preparedness**, communication with other stakeholders (emergency management, law enforcement agencies, fire and medical services, mental health support, local business) are of key importance, as are communication plans and strategies. Schools must be equipped to make a response to an attack and overcome its effects. Maps of buildings and information provision are also important.

Dorn focused on measures that can be implemented by schools themselves. Baray [6] identified external areas, which need to be considered in connection with those counter-terrorist measures, which seek to prevent attacks on schools and schoolchildren. These need to be advanced by the security forces themselves, and according to Baray should encompass the following:

- The development of police department employees to be the agency's subject matter experts regarding school terrorism (Terrorist Liaison Officer);
- Collaborative partnerships with the school district and community stakeholders;
- A successful school resource officer program;
- A comprehensive prevention and emergency response plan; and
- Anti-terrorism tactical training for patrol level and SWAT personnel.

The procedures and recommendations developed in the US are inspirational. These have been developed in response to the nation's fairly significant experience with terrorist-motivated and other violent attacks on schools. In particular, US experts have experiences to draw on from a number of incidents of school shootings. Various US organisations specialise in providing security to schools and can help individual schools to establish security and prevention plans so that the threat of violence at their institutions can be minimised.

According to the National School Safety and Security Services [20], several basic recommendations concerning terrorist attacks and the provision of security in schools can be identified. Obviously every school has unique needs, stemming from its location, environment, etc. The first rule says that schools and official representatives should not be afraid to speak about this type of risk, and to prepare for it. Although by discussing the possibility of a terrorist attack, they might cause fear and panic among some parents, in general awareness eliminates fear. Thus, if parents are well informed, the effect should be positive. Fear must be overcome with education, communication and awareness.

Communication with pupils and students should also be open. Obviously, any discussions must be set up to be appropriate to the age of the children. Pupils and students should also understand that any potential reaction to an abnormal situation is in fact normal. Discussions should focus on facts and pupils must be reassured that the measures taken increase their safety.

It is further recommended that schools check, and if necessary put in place, emergency guidelines, and implement the necessary procedures relevant to the conditions in which the school is operating.

Crucially, a certain level of awareness must be achieved amongst the members of the school community; i.e. teachers and staff. It is recommended that both teachers and other staff be trained and informed of emergency plans, for which they should also be drilled. In an emergency, everyone must understand what exactly his or her role is. Staff should report suspect vehicles, individuals and items noted around the school premises. They should also be able to respond to suspicious information-gathering attempts.

Physical security is also essential. Schools need to revise the access routes to their buildings and be aware of them. Their number might need to be reduced so they can be easily monitored. It is also recommended that schools install physical access barriers such as fences, gates, etc. Janitors and staff responsible for access to the school need to be sensitive about the presence of suspicious persons, vehicles and items in the vicinity of the school. Access to technical facilities at a school (i.e. areas where heating, cooling and ventilation systems are located) should also be limited.

If the school provides transportation to children, it should be aware of the possible risks of this, and attempt to reduce them. Emergency plans should be drawn up concerning school bus transport, and drivers need to acquaint themselves with these.

Security is equally important in terms of where schools store and prepare food. Emergency plans should be in place to determine where pupils and staff are forced to remain in the school: access to a sufficient amount of water and provisions needs to be guaranteed. Furthermore, there is the question of medical supplies – in particular if schools are adequately prepared in this area. It is recommended to have enough medication for pupils for at least three days.

Communications with other key actors also needs to be established. These include mental support services for pupils, parents and staff, but also involving the police and fire services. Parents, pupils and staff should know with whom to communicate if necessary, who should be called if something suspicious is noted, etc. The school should have a crisis communication plan in place, and parents need to be aware of the methods the school would use to contact them in an emergency. The technical side of communication also demands attention, including the provision of a backup power supply.

Finally, one recommendation suggests that schools should also identify buildings, organisations, etc. in their vicinity, which are also under a potential threat of a terrorist attack, such as military installations, government facilities, power plants, airports, railways, chemical factories, etc. School should draw up crises plans in consideration of this contextual data.

3. Conclusion

In contemporary Europe the issue of terrorist attacks against schools and pupils is not as reflected as, for example, in the United States of America, where mass casualty events in school environments unfortunately have happened more frequently. To a large extent they can be called terrorist attacks of so-called insane shooters or lone wolves. Terrorist attacks are also more common due to the significantly multicultural society and foreign policy of the United States that are significantly involved in the affairs of states with different culture, politics and religion. The prevention and preparedness is thus reflected in the American environment significantly and schools are encouraged and trained in creating emergency plans that cover also the possibility of a terrorist attack. In the United States a number of organizations have been also created that specialize in school safety and help prepare these emergency plans. In many American states, the issue is also reflected by legislation.

However, although the European continent is less affected by the issue of terrorist attacks against schools and students, this does not mean that we should overlook this issue. Cultural, ethnic and religious disputes have escalated in last few years into violent clashes, in a few cases also pupils were used as targets. Europeans should be aware of this possible threat and deal with it with full responsibility. Emergency plans of American schools can be a good practice and experience that can be transferred to Europe.

References

[1] M. Mareš, *Terorismus v ČR*. Centrum strategických studií, Brno, 2005.

[2] W. Laqueur, *Poslední dny Evropy…Humanistická Evropa, nebo islamistická Eurábie? Analýza – perspektiva – prognóza – řešení*, Nakladatelství Lidové noviny, Praha, 2006.

[3] J. Eichler, *Mezinárodní bezpečnost v době globalizace*, Portál, Praha, 2009.

[4] M. Rassin et al., Emergency Department Staff Preparedness for Mass Casualty Events Involving Children, *Disaster Management & Response*, 2 (2007), 36 – 44.

[5] V.F. Balaban, et al., Screening and Assessment for Children`s Psychosocial Needs Following War and Terrorism. In Friedman J. Matthew, Mikus-Kos, Anica, eds., *Promoting the Psychological Well Being of Children Following War and Terrorism*, IOS Press, Amsterdam, 2005, 121 – 162.

[6] M. D. Baray, *The Threat of Terrorism to U.S. Schools…Fact or Fiction?,* http://lib.post.ca.gov/lib- documents/cc/41-Baray.pdf, 2007.

[7] Safe Havens International, School Terrorism Timeline, http://www.safehavensinternational.org/category/school-terrorism-timeline/.

[8] C.S. Smith, *Dutch Muslim School Bombed; Link to Killing Suspected*, http://www.nytimes.com/2004/11/09/international/europe/09dutch.html, 2004.

[9] Lidovky.cz, *Teroristé zaútočili na školu. Zabili devět dětí*, http://www.lidovky.cz/teroriste-zautocili-na-skolu-zanechali-devet-mrtvych-pfr-/zpravy-svet.aspx?c=A130619_074149_ln_zahranici_vs, 2013.

[10] D. Brown, *Children on the Front Line*, http://www.theguardian.com/uk/2001/sep/03/northernireland.derekbrown, 2001.

[11] J. Hyland, *Northern Ireland: Catholic girl school becomes focus for sectarian violence*, http://www.wsws.org/en/articles/2001/09/ire-s05.html, 2001.
[12] T. Oliver, *Loyalist shame at school bombers; Fury over attack on children*, http://www.highbeam.com/doc/1G1-77859197.html, 2001.
[13] Safe Havens International, *Innocent Targets. When Terrorism Comes to School*, https://smartech.gatech.edu/bitstream/handle/1853/13237/slides.pdf?sequence=4, 2007.
[14] ČT24, *Beslan si připomněl oběti masakru z roku 2004*, http://www.ceskatelevize.cz/ct24/svet/65575-beslan-si-pripomnel-obeti-masakru-z-roku-2004/, 2009.
[15] U. Klussmann, The Beslan Aftermath: New Papers Critical of Russian Security Forces., *Spiegel,* 2005, http://www.spiegel.de/international/spiegel/the-beslan-aftermath-new-papers-critical-of-russian-security-forces-a-363934.html.
[16] Aljazeera America, *Nigerian Government says most kidnapped girl rescued*, http://america.aljazeera.com/articles/2014/4/16/nigeria-kidnap-rescue.html, 2014.
[17] The Guardian, *Missing Nigerian schoolgirls: Boko Haram claims responsibility for kidnapping.*, http://www.theguardian.com/world/2014/may/05/boko-haram-claims-responsibility-kidnapping-nigeria-schoolgirls, 2004.
[18] ČT24, *Národní garda u školy v Karlových varech situaci spíše zkomplikovala***,** http://www.ceskatelevize.cz/ct24/regiony/20705-narodni-garda-u-skoly-v-karlovych-varech-situaci-spise-zkomplikovala/, 2008.
[19] R. Johnston, *Terrorist and criminal attacks targeting children*, http://johnstonsrchive.net/terrorism/wrjp39ch.html, 2013.
[20] National school safety and security services, *Schools & Terrorism: School Terrorism Preparedness*, http://www.schoolsecurity.org/terrorist_response.html.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-67

Use of the Enhanced Structural Model for Attack Analysis and Education

Blaž IVANC [a,b,1] and Tomaž KLOBUČAR [a]
[a] *Jožef Stefan Institute*
[b] *ICS Center for Information Security*

Abstract. Ensuring cyber security is a dynamic, demanding, and complex task. Due to the pace of development in this area, cyber security experts are forced to engage in constant education and have access to test environments and develop both offensive and defensive cyber techniques. The qualitative analyses of past attacks and other security incidents can present a significant contribution to the development of knowledge. In an effort to improve the attack modeling in critical infrastructure and remedy certain weaknesses of the existing models, we have developed a model called the Enhanced Structural Model. The purpose of this paper is to present both the possibilities of the attack modeling and our model for the analysis of past incidents and for educational purposes. The model is suitable for presenting the knowledge in the form of an analytical presentation of the attacks as well as for performing laboratory work and the examination of students.

Keywords. attack, cyber security, cyber warfare, incident, attack model, education

Introduction

Ensuring cyber security is a dynamic, demanding, and complex task. Cyber security can be divided into many sub-areas, such as cryptography, database security, malware analyses, intrusion detection etc., and it is impossible to expect that one person could cover all of them. At the same time, new forms of cyber attacks are constantly on the rise, modern information systems and networks are becoming increasingly complex and more and more security technologies are available in response to the new attacks. Due to the pace of development in this area, cyber security experts are forced to engage in constant education and have access to test environments and develop both offensive and defensive information techniques.

The qualitative analyses of past attacks and other security incidents can present a significant contribution to the development of knowledge. By using different models and techniques the expert can model past and future cyber attacks and thus develop a sense for the manner of the attack implementation and improve the ability of countermeasure management. The modeling of potential attacks facilitates the selection of appropriate security technologies and is preferable already at the design of the information systems.

In literature and in practice many models with their advantages and disadvantages can be found [1][2][3]. In an effort to improve the attack modeling in critical infrastructure and remedy certain weaknesses of the existing models, we have developed a model called the Enhanced structural model [4].

The purpose of this paper is to present both the possibilities of the attack modeling and our model for the analysis of past incidents and for educational purposes.

[1] Corresponding Author: Blaž Ivanc, MSc, ICS Center for Information Security, Cesta Andreja Bitenca 68, Ljubljana, e-mail: blaz.ivanc@ics-institut.si

This paper is organized as follows: Chapter 2 includes the presentation of both the attack modeling method and the Enhanced structural model used as a technique of attack modeling. In Chapter 3 the applicability of our model for attack analysis and educational purposes is demonstrated. The fourth chapter includes the conclusion and future work.

1. Background

This chapter briefly presents the attack modeling and the Enhanced structural model. In the attack modeling we first introduce the importance of modeling and the categorization of models. This is followed by a presentation of our model.

1.1. Attack Modeling Method

Attack modeling is one of the most important methods for detecting the weak points of information systems and networks. It raises security awareness and helps us to prepare for possible scenarios which we would like to avoid in practice. If we prepare ourselves for potential security incidents, we can adequately protect the corporate environment and make sure the incidents do not occur.

1.1.1. Attack Model

The attack model is a fundamental tool for the development of attack scenarios. The skills of analysts – the subject-matter experts who model the attacks – are of key importance in attack modeling. Therefore constant work on the following inter-related points is important:

- Consideration of security issues from the threat agent's point of view.
- Monitoring new attack techniques.
- Analysis of the attack methods.

In the process of the attack modeling various models, which can be divided into static and dynamic or structural and behavioral models, are used [2]. Graph-based models can be more directly divided into attack trees and Petri nets [3]. The attack tree model is one of the structural techniques, while the Petri nets are a dynamic technique, characterized by the presence of the time dimension. Structural models can quickly become excessive. Due to their static nature and step-by-step treatment of the attack, they are also difficult to demonstrate the coordinated attacks with [5]. Nevertheless, the structural techniques have their advantages, such as the modular construction of the model, production speed, and intuitiveness.

1.1.2. Attack Tree

The attack tree is one of the static or structural model types, like Bayesian networks. The origin of the attack tree is in the fault tree, but holds a different role and purpose. Therefore, it is wrong to classify the fault tree and similar tree-based models in the attack modelling category. A standard attack tree is often referred to as AND / OR tree. The model has been the subject of derivatives, such as adding countermeasures to the end nodes etc., and thus been given new related names. What most of the presentations of the extended models have in common is that they are based on nodes, which require the implementation of one of the sub-nodes (OR-condition) or all of the sub-nodes (AND-condition). The main goal of attack is represented in the root of the tree, while the intermediate nodes present the obligatory or non-obligatory sub-goals that must be reached on the way to the main goal. The end nodes or leaves of the tree represent actions. After setting up the model, the nodes can be assigned quantitative or qualitative values. In the qualitative approach, the analysts often use scenario analysis, whereas the attack trees are often used for implementation. The quantitative approach means that resources are evaluated numerically, while threats, vulnerabilities and countermeasures can be regarded as a necessary upgrade of the attack tree for designing a high-quality strategy for reducing risks.

1.1.3. Variations of the Attack Tree

There are different versions of attack trees, such as protection tree and defence tree [6] [7]. The featured version of the attack tree model, presented by Ivanc and Klobučar [8] and based on the analysis of the Stuxnet computer network operation, not only incorporates labels for exploiting vulnerability, which have an additional message value in the presentation of the target systems, planning, and implementation of the attacks, but also includes additional nodes: the conditional subordination node, the housing node, and the initiator node. These are some of the additional nodes proposed by Khand [9]. Additional nodes enable the simulation of various operating situations and consequences of attacks and capture a wider source of attackers in the implementation of a certain attack.

1.2. Enhanced Structural Model

Models, such as the Enhanced structural model (ESM), are based on a modular approach which allows the expert analysts of different disciplines to work on the development of the model at the same time. The development of the model is relatively fast; however, reading can be more transparent than with some other models. The ESM was basically developed for the attack modeling in the critical infrastructure.

The attack modeling using the ESM enables a better understanding of the implementation of the attacks, the identification of security weaknesses and an analysis of the existing security policy. The model eliminates certain limitations that are present in the attack modeling. These are: high abstract demonstration of the attacks and low flexibility of the course of the operation to a particular target.

The attack modeling is most recommended in the design phase of the system or operations. In this way it can provide better operational safety. The attack modeling is also useful when an incident has already happened. It enables better assessment and decision-making in relation to the handling in the next hours and days and also a subsequent analysis of the events.

1.2.1. Overview of the Characteristics of the Enhanced Structural Model

This chapter presents the characteristics of the Enhanced structural model. Figure 1 displays an example of the Enhanced structural model. The main characteristics of the model are:

- **Use of two additional nodes of Khand to illustrate the course of the attacks**
  - Using Khand's conditional subordination node, the internal enemy can be considered as a threat agent during the course of the attack. Use of the housing node allows us to demonstrate different time stages of the attack execution.
- **Use of labels for exploitable vulnerabilities**
  - Vulnerability labels help us recognize the vulnerable target computer systems or software. In addition to describing the software, which is the target of exploiting vulnerabilities, the labels provide information on the complexity of a given set of attack. Subject to the expected result of the exploited vulnerability, they also give a sense of the position for each part of the attack within the framework of the entire operation.
- **Use of labels for attack vectors**
  - The attack vector indicates a particular method or a path for the compromising of the computer systems.
- **Demonstration of countermeasures**
  - Countermeasures in the Enhanced structural model appear as a set of countermeasures, the elements of which are individual security countermeasures. The aim of a set of security countermeasures in the Enhanced structural model is to demonstrate what types of countermeasures are encountered in the implementation of the attack.
- **Segmental distribution of the model structure**
  - A segment is a logically labelled collection of nodes that form a certain comprehensively completed sub-tree structure. Each analyst involved in assembling the model can use the dotted lines to isolate a specific part of the model and thus indicate a certain characteristic of this segment.

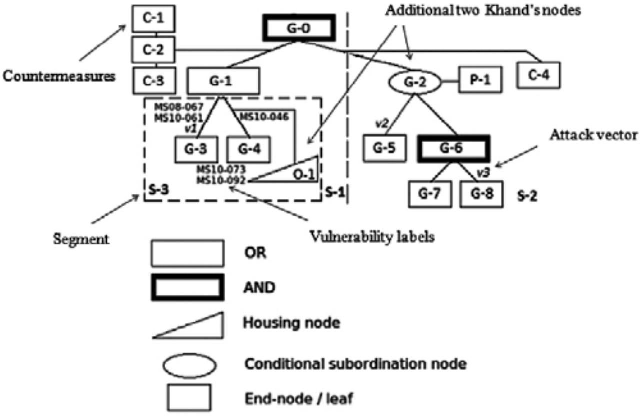


Figure 1. Example of the Enhanced structural model intended for information attack modeling [4].

2. Use of our Model for Attack Analysis and Education

Both in terms of the analysis of the previous attacks and education, it is important that the model can be developed by several specialists at the same time and that the work is carried out quickly and comprehensively. This is especially important for the participants to whom the information and knowledge of the model are being presented. The mentioned features correspond to the structural techniques of the attack modeling.

Based on the previous work and the evaluation of our own model [10][8], we believe that the Enhanced structural model is a suitable tool for attack analysis. Therefore, in this chapter we first demonstrate the use of the model for the attack analysis and later its use for educational purposes.

2.1. Analyses of Attacks

In recent years we have used the attack modeling method in connection with the attacks and security of the critical infrastructure. Before designing our own model we used a partially improved attack tree [4] to present the importance of the attack modeling in the critical infrastructure. A similar model was used for a snapshot of the situation and the development of attacks on the computer-aided water supply of the population. The Enhanced structural model has been introduced to remove some of the weaknesses of those models.

Figure 2 illustrates that the high-quality attack modeling first requires the knowledge about the weaknesses of the target systems. At the same time it is necessary to know and master the offensive techniques, tactics, and procedures in practice. This is followed by the application of the model and the generation of the attack scenarios.

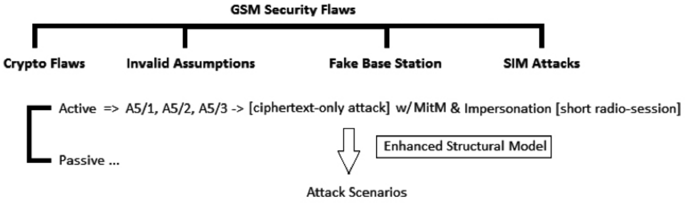

GSM Security Flaws
Crypto Flaws
Invalid Assumptions
Fake Base Station
SIM Attacks
Active => A5/1, A5/2, A5/3 -> [ciphertext-only attack] w/ MitM & Impersonation [short radio-session]
Passive ...
Enhanced Structural Model
Attack Scenarios

Figure 2. Placement of the model in the process of developing attack scenarios.

Figure 3 reveals an example of the Enhanced structural model and the reading of the course of the attack. Names of the tree nodes, attack vectors, countermeasures and segments are given in Tables 1-4. The model is presented based on the attacks introduced in [11]. In the paper, the authors describe the attacks in their test environment dedicated to the treatment of internal attacks in industrial control systems. There are two target elements in their test environment: programmable logical controller (PLC) and human-machine interface (HMI). There are four identical attacks presented for both elements. We will focus on the two: Replay attack and denial of service (DoS). Four different implementation options are proposed for the latter. Within the context of DoS we will choose two options. Primarily we will choose a set of Netwox tools which allow the selection of tools depending on the attack technique. The second option, the selection of the LOIC tool, will be demonstrated in the model as an alternative for the implementation of the attack with the aim of causing the denial of service.

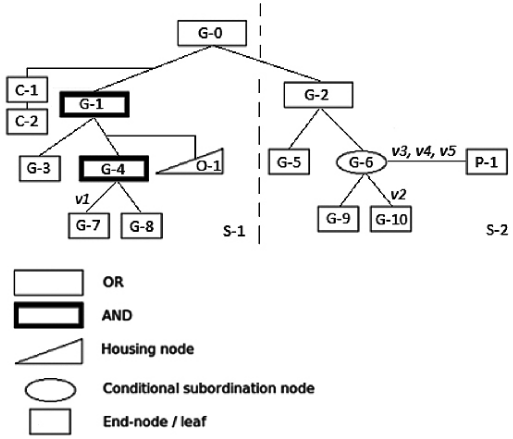


Figure 3. Enhanced structural model based on the attacks in the test environment.

Table 1. Description of the attack nodes.

Node	Description
G-0	Attack on PLC
G-1	Exploiting the vulnerability of the FINS protocol
G-2	Executing the Denial of Service attack (DoS)
G-3	Eavesdropping the data stream
G-4	Replay attack
G-5	Sending the IP packages that exceed the permissible length
G-6	Generating attacks using the research tool
G-7	Authentication of the malicious component
G-8	Executing Write Request
G-9	Selection of tools from Netwox
G-10	Implement the attack
O-1	Access to servers
P-1	Use of LOIC tool

Table 2. Description of the attack vectors.

Vector	Description
v1	Brute force
v2	Sending random IP packets
v3	Sending UDP packets
v4	Sending TCP packets
v5	Sending HTTP packets

Table 3. Segment label.

Segment	Description
S-1	The segment deals with attacks that can lead to control reprogramming
S-2	The segment deals with attacks aimed at causing non-availability

Table 4. Description of security countermeasures.

Countermeasure	Description
C-1	Write protection
C-2	Read protection

Model reading

The main goal of the attack is represented by the G-0 node “Attack on PLC”. The legend in the figure reveals that the node requires a logical OR operation. In this way we can carry out the attacks that exploit the vulnerabilities of the FINS protocol (G-1) or DoS attacks (G-2). The first procedure in exploiting the vulnerability of the FINS protocol is eavesdropping the data stream (G-3). The mentioned protocol is sending data in cleartext to the test environment, which allows the attacker to become familiar with passwords and other information necessary for the subsequent authentication of malicious components. The G-1 node requires a logical AND operation and with that the continuation on the G-4 node. This node is related to the implementation of the replay attack and requires the implementation of nodes G-7 and G-8. In order to achieve the authentication of the malicious component, we must bypass the security countermeasure of the write protection. This is achieved by generating the requests with all the possible parameter values, the correct value of which will authenticate the component. However, we can become familiar with the selection of the correct values already during the eavesdropping of the data stream. The O-1 node is a housing-node and provides for a logical XOR operation between the node itself and the G-4 node. Node O-1 provides for the attacker’s access to the servers using a password obtained through the eavesdropping, i.e. the implementation of the G-3 node. In this case, the attacker does not implement the replay attack (G-4), since the effect of such attack is less significant in comparison to the malicious consequences arising from the O-1 node.

In the previous paragraph we described the S-1 segment, which deals with the attacks that may lead to control reprogramming. This is followed by the segment S-2 which provides for the execution of DoS attacks with the sub-goal G-2. Thus, the G-5 node may be used for sending IP packages exceeding the permissible length. We can also use dedicated research tools, which provide for the conditional subordination node G-6. This node in the first place requires the selection of the appropriate tool from the Netwox toolbox (G-9) and the implementation of the attack (G-10). Vector v2 shows that we decide for overflowing with random IP packets. The P-1 node provides for an alternative implementation of the attack using the LOIC tool, while vectors v3, v4, and v5 provide for the sending of the UDP, TCP and HTTP packets.

The Enhanced structural model also provides for an indication of the exploited vulnerabilities. The illustrated vulnerability case is considered in terms of security weaknesses and deficiencies. It fails to provide for the generally recognized indication of vulnerability which would indicate other circumstances, such as the effect of the exploited vulnerabilities, the complexity of the affected systems, and others.

2.2. The Use of the Model for Educational Purposes

For the purposes of the Enhanced structural model evaluation, structured interviews were conducted with experts from the field of modeling and critical infrastructure in Slovenia [4]. The heads of the information security and defense studies post-graduate programs participated in the interviews. Based on the interviews we discovered that the model can be widely used also for educational purposes. In Slovenia, until now academic professors have been explaining the functioning and courses of the attacks to students in different ways. However, they did not use the attack modeling method to demonstrate attacks to ensure a more comprehensible and detailed presentation.

As told in [12], students are well familiar with security incidents, but they lack the basic skills and background knowledge to be able to understand the technical aspects. Therefore the authors proposed a basic attack tree model as a tool that could efficiently contribute to the management of information security related aspects.

Academic professors can use the Enhanced structural model for the following:

- More detailed presentations of cyber attacks to students.
- Distribution of the laboratory tasks to students depending on the structure of the model.
- As a tool for the better preparation for delivering the study subjects in relation to the computer network operations.

The model is also interesting for students. The use of this model enables the students to better understand the implementation of the attacks. In a transparent manner they can see where in the course of the attack a certain attack technique is being used. The use of the model helps develop the security awareness and the analytical abilities of the students. In order to be used, it is recommended that students are already familiar with the more advanced material in the field of information security. Prior technical knowledge and specific specialties mostly depend on the level or the complexity of the attacks that are to be modeled.

The more detailed are the presentations of the attacks and more complex is the implementation, the greater are the technical knowledge and a variety of specialties of the students. This is reflected in the knowledge and the implementation of offensive and defensive information techniques, tactics and procedures. Our model can be used for various tasks:

- Designing the model according to the attack scenario and reading the scenario with regards to the model.
- Management of information attacks: Assigning the tasks and assembly of the individual parts of the model into a final and completed whole.
- Complementing the model: The model displays only the main goal of the attack and the intermediate nodes representing the partial goals of the attack. Final attack nodes, exploited vulnerabilities and the use of attack vectors should be demonstrated by students independently.

Attack modelling is an excellent educational tool. The Enhanced structural model is a suitable tool for both professors and post-graduate students.

3. Conclusion and Future Work

The evaluation of our model revealed the potentials of use for the analysis of past attacks and in education. The model is suitable for both presenting the knowledge in the form of an analytical presentation of the attacks as well as for performing laboratory work and the examination of students. The model can be developed by individuals or groups with different levels of knowledge. An additional advantage of using the model in education is a debate following the comparison of different models.

In the future, we would like to develop a curriculum for the training of experts dealing with the information attack modeling. At the moment, the Slovenian students come across the attack modeling method only through invited guest lecturers. It should be noted that, in contrast to other countries, none of the Slovenian organizations at the state level dealing with classified information use the attack modeling method.

The current software support for attack modeling is based on the attack tree model. Thus, it does not support the integration of the characteristics of our model. In the future, we should consider designing a software framework for attack modeling based on the Enhanced structural model.

References

[1] Y.H. Chang, P. Jirutitijaroen, C.W. Ten, A Simulation Model of Cyber Threats for Energy Metering Devices in a Secondary Distribution Network, *5th International Conference on Critical Infrastructure* (2010), 1-7.

[2] P.C. Ludovic, M. Bouissou, Beyond attack trees: dynamic security modelling with Boolean logic Driven Markov Processes (BDMP), *European Dependable Computing Conference* (2010), 199-208.

[3] I. N. Fovino, M. Masera, A. De Cian, Integrating cyber attacks within fault trees, *Reliability Engineering & System Safety* 9 (2009), 1394-1402.

[4] B. Ivanc, *Modelling of Information Attacks on Critical Infrastructure by Using the Enhanced Structural Model*, Jožef Stefan IPS, Ljubljana, M.Sc, thesis (2013).

[5] T.M. Chen, J.C. Sanchez-Aarnoutse, J. Buford, Petri Net Modelling of Cyber-Physical Attacks on Smart Grid, *IEEE Transactions on SmartGrid* 2(4) (2011), 741-749.

[6] K. Edge, The Use of Attack and Protection Trees to Analyse Security for an Online Banking System, *Proceedings of the 40th Hawaii International Conference on System Sciences* (2007), 144b-144b.

[7] S. Bistarelli, F. Fioravanti, P. Peretti, Defense trees for economic evaluation of security investments, *The First InternationalConference on Availability, Reliability and Security* (2006), 416-423.

[8] B. Ivanc, T. Klobučar, Critical Infrastructure Attack Modelling, *Elektrotehniški vestnik* 79 (4) (2012), 193-196.

[9] P. A. Khand, System Level Security Modelling Using Attack Trees, *2nd International Conference on Computer, Control and Communication* (2009), 1-7.

[10] B. Ivanc, Techniques and procedures of cyber attacks on critical infrastructure, *Management of corporate security: new approaches and future challenges* (2013), 161–171.

[11] N. Sayegh, A. Chehab, I.H. Elhajj, A. Kayssi, Internal Security Attacks on SCADA Systems, *Third International Conference on Communications and Information Technology (ICCIT)* (2013), 22-27.

[12] V. Saini, Q. Duan, V. Paruchuri, Threat Modeling Using Attack Tree, *Journal of Computing Sciences in Colleges* 23(4) (2008), 124-131.

This page intentionally left blank

Section 2:
Information Security and Counter Terrorism Considerations

This page intentionally left blank

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015

© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-79

Improving Critical Infrastructure Protection and Resilience against Terrorism Cyber Threats

Sandro BOLOGNA [a,1], Alessandro LAZARI [b] and Stefano MELE [c]
[a] *Italian Association of Critical Infrastructures Experts, Rome, Italy*
[b] *School of Law, University of Salento, Italy*
[c] *Italian Institute of Strategic Studies 'Niccolò Machiavelli', Rome, Italy*

Abstract. Nowadays business continuity and disaster management procedures and policies are increasingly based on the notion of resilience. This relatively young topic is gaining increasing importance now that more recent experiences have shown that not all the attacks or accidents to critical information infrastructures (CIIs) can be avoided even if protection measures are correctly implemented. Such a circumstance implies that the response to 'protection' needs, which has mainly shown the use of technology as a possible solution to all of the issues, is not sufficient in covering the entire lifecycle of modern information infrastructures which requires instead the implementation of redundancy measures together with specific procedures that are designed and implemented in view to facilitate a faster recovery of an asset that has suffered an unavoidable accident. The aforementioned scenario is somehow confirmed by the reorientation of the EU policies in the field and, more specifically, by the 2014-2020 European Programme for Critical Infrastructure Protection (EPCIP) which now mainly rotates around key resilience concepts like prevention, preparedness and response. This paper, after a short description of the most significant vectors of attacks directed towards CIIs, offers a review of the main principles of resilience and a basic scheme that should guide those stakeholders that are in the phase of studying how to effectively implement those measures in the management lifecycle of technology driven infrastructures.

Keywords. critical infrastructures, resilience, cyber attack, cyber security, cyber strategy

Introduction

A critical infrastructure is a tempting target for an enemy, be it a terrorist organization or a hostile country. With the development of the so-called cyberspace, for the first time in the history, it is possible to attack strategic targets, like vital infrastructures, without physically being in the place where they are located and avoiding the risk of being caught during the attack [1].

The first response against cyber threats has been focused on their technical side, investing in security measures such as firewalls, antivirus and other software/hardware intrusion-detection solutions. However, there is a growing understanding that this problem cannot be dealt on a technical and operational level only, as, nowadays, many of the aforementioned technical solutions have proven to be ineffective or insufficient

[1] Corresponding Author: Dr. Sandro Bologna, Italian Association of Critical Infrastructures Experts, Rome, Italy, e-mail: s.bologna@infrastrutturecritiche.it

if not integrated with redundancy-oriented solution. Resilience, commonly intended as the capability of the infrastructures or service to rapidly "bounce back" after an attack or to absorb and frustrate its potential, is now deemed an economically justified policy in complement of existing prevention and protection policies that stand as the pillars of current Critical Infrastructure Protection programs. Such a new approach is increasingly important especially since cyber attacks have multiplied in recent years, increasing the fear of global digital-breakdowns, the deviation of use and general distrust of many services essential to the modern society. Resilience is an engineered aptitude, embedded in the infrastructures' protection and management lifecycle, that allows complex systems to survive different kind of attacks or to diminish their impacts, and consequently incidents occur despite defense barriers crafted into those systems. One of the sources of increasing cyber attacks is coming from terrorism cyber threats [2].

Much has been written about cyber terrorism and terrorists' capability to affect cyber security. Although this phenomenon existed well before 9/11[2], cyber terrorism has emerged as a great security concern in the last decade, thanks to the dizzying growth in the use of digital technologies. Up to now, even if cyber terrorism is widely perceived as a high priority source of threats to infrastructures and orderly societal life, there is no case or known evidence that it might bring the same level of casualties and severe damages as caused by "conventional" attacks.

This paper, after a review of some recent examples of cyber attacks against critical infrastructures, the most common vulnerabilities and analyses of sectors targeted by cyber attacks, illustrate the increasing necessity to move from protection toward resilience. An acceptable level of cyber security will not be achieved if we do not consider the necessary efforts to improve critical infrastructure resilience, circumstance that should not ever imply a blind reorientation of focus that puts physical security in the background. These efforts should include, but shouldn't be limited to, employment of a strong security policy and working with law enforcement if necessary (also for forensics purposes), awareness in the application of the latest security technologies, conducting regular security audits, the implementation of a suitable disaster recovery plan. The paper will also include a human-centric perspective, as it is the authors' opinion that cyber security is not achievable without a human-in-the-loop vision that spans from training to management and include delicate aspect as preparedness and aware decision-making. For achieving the paper's outcomes and in view to indicate clearly where security manager or liaison officers should intervene, a basic scheme including 'lines of defense' will be proposed so as to create awareness on which areas of the short-mid-long term of the infrastructure's overall lifecycle should be amended or improved.

1. Some Recent Example of Cyber Attacks against Critical Infrastructures

Producing comprehensive lists of cyber attacks is not an easy task because, usually, government agencies, national critical infrastructures, large-scale laboratories and other major actors do not tend to disclose whether a cyber attack has taken place nor reveal its

[2] One of the very first example of legislation promulgated in view of preventing cyber attacks can be dated back to 1987 and to the US' Computer Security Law. Such law was mainly focused on the security and privacy of sensitive information stored in federal systems and aimed at establishing some security best practices. Among the requirements, it is worth mentioning the appearance of "security plans" and the introduction of the training courses for the users of such systems.

details. In the following some of the most recent and well known attacks will be taken into account:

- "Stuxnet", which became known to the public in 2010, is believed to be the first malware specifically designed for targeting a critical infrastructure's systems. Computer analysts have confirmed that it has been deployed in order to shut down the centrifuges at Natanz's (Iran) uranium enrichment plant, where stoppages and other issues reportedly occurred around that time. The sophisticated worm spreads via USB drives and makes the attack possible by exploiting four previously unknown bugs (0-day vulnerability) of the operative system.
- In February 2013, a critical vulnerability in the Industrial Control Systems called "Tridium Niagara AX Framework" – widely used by the military and hospitals - was found. After a complete set on analysis and test, the system has been found vulnerable to a specific zero-day vulnerability that permits to gain complete control of the machinery.
- In August 2013, more than 30,000 computers were compromised and destroyed by the Shamoon virus a "spear-phishing" attack at Saudi Aramco. All it took to affect the network was one employee opening an infected email containing malware called Shamoon - and 75 percent of the company's workstations were infected/compromised.

Attackers can find connected and vulnerable systems through simple internet searches through search engines like Shodan[3]. Moreover, here is where ultimately, the problem lies - attackers know about vulnerabilities and continually exploit privileged accounts in almost every attack while the vast majority of organizations do not even know that they exist. In January 2013, the United States' Department of Homeland Security released a map that pinpoints the locations of 7,200 Critical Infrastructures with Industrial Control Systems that appear to be directly linked to the Internet and potentially vulnerable to cyber attacks.

As cyber attackers continue to become more and more sophisticated, and the benefits of interconnecting corporate ICT systems with IACS systems becomes more attractive to companies that operate critical infrastructure, every organization will have to face these evolving security challenges [3][4].

2. Common Vulnerabilities and Methods of Attack

The reason why the operators of cyber infrastructures – or infrastructures that rely on IT systems – should increase their focus on resilience is quickly explained if considering all of the "known" vulnerabilities and methods of attack that can negatively affect the lifecycle of cyber systems (and services depending on those systems).

The recurring vulnerabilities and attacks can be briefly summarized in the following lists:

Vulnerabilities

- Intrinsic software/hardware vulnerability (by design);
- Lack of (physical and logical) protection measures;
- 0-day vulnerabilities;
- Misconfiguration/incompatibility of the components of a system;

[3] The search engine is available at: http://www.shodanhq.com.

- Lack of software/hardware updates or updates not properly tested before installation/implementation;
- Unpreparedness of the system administrators;
- Lack of training of the users of the system;
- Obsolescence of the infrastructure or of part of the systems;
- Flaws in the corporate IT policy (credentials still active even after the retirement/resignation/dismissal of employees);
- Underestimation of risks deriving from physical vulnerabilities of facilities that hosts cyber systems (e.g. exposed to flooding, willful acts, etc.).

Attacks

- Distributed denial-of-service;
- Network intrusions;
- Malware, Trojan horse, backdoors;
- Targeting of specific users (administrators – key position's operator);
- Targeting of specific equipment/devices (e.g. Programmable logic controller - PLC);
- Total or partial destruction of the systems (e.g. fire, explosion, etc.);
- Social engineering;
- Insiders.

Both the aforementioned categories have increased in importance (and capability to harm cyber systems) due to the massive adoption of technologies in all of the corporate and public sectors and due to the light-speed evolution of the market competition – circumstance that in some case is forcing the technology vendors to sell "not-fully-tested" equipment.

It can be affirmed that the adoption of resilience measures seems to be justified by the same variables that a long time ago have suggested the adoption of protection measures and from the awareness that there is no resilience without protection and vice-versa.

At the same time, it's necessary to highlight that the adoption of resilience measures shouldn't in any case divert or reduce the focus from protection, as these approaches are complementary and cannot be equally missing from the management and security lifecycle of modern infrastructures.

The need to put the same emphasis on protection and resilience of cyber infrastructures should be a lesson learned from the unbalanced approach to the protection of "physical versus logical" assets that the governments, the security agencies, the operators and the technology vendors have had in the past. Such an unbalanced approach, enacted through an unjustified reorientation of the focus from the physical to the logical protection of critical assets and infrastructures, has created the premises for the deep underestimation and missing perception of risks, behavior that has often exposed infrastructures to new risks and vulnerabilities, instead of reducing them.

Another review and analysis of the lists proposed above also shows the dominating importance of the "human factor", as most recurring variable that may assume a negative role in the protection and resilience of critical infrastructures. From the design to the implementation and use of technologies (as well as measures, best practices, standards and protocols) – passing by testing, certification, preparedness and training – the human being finds himself in a delicate role, whose mission to secure the orderly societal life imply the necessary adoption of smooth, comprehensive and effective models in order to break-down and simplify the governance and management of every day more complex, interdependent and vital infrastructures.

3. Analysis of Sectors Targeted by Cyber Attacks

In order to acquire full awareness on how many sectors are (or can be) affected by cyber attacks, it should be sufficient to say that there is a potential risk lurking in each of the nodes that are part of the global network of assets and related services provided to the modern society. For this reason, it should not be a surprise if among all the sectors the energy one appears to be the most targeted from cyber attackers. Such an assumption is clearly explained by the fact that the intention to disrupt most of the services available nowadays can be enacted through taking down the power infrastructures.

Such dramatic circumstance is confirmed by a recent study issued by Symantec[4]. The security company affirms that attacks have been successfully conducted not only targeting internet-connected systems but also isolated ones.

The reasons behind such attacks, apart from the source or the profile of the attacker, are the same: the destruction or disruption of the infrastructure with consequent loss of service.

Another element that seems worth analyzing, if considering the most recurrent profile of the attackers, is the one that shows that cyber terrorists aren't considered as the top threat to energy infrastructures as they share the top ranking with operator's competitors (mainly interested in espionage), state sponsored attacks (e.g. Stuxnet), activists and – as previously mentioned – insiders (e.g. dissatisfied employees).

According to the aforementioned study, "*during the monitoring period from July 2012 to June 2013, we observed an average of 74 targeted attacks per day globally. Of these, nine attacks per day targeted the energy sector. Accounting for 16.3 percent of all attacks, the energy sector was the second most targeted vertical in the last six months of 2012, with only the government/public sector exceeding it with 25.4 percent of all attacks. The high ranking was mainly due to a major attack against a global oil company, which we observed in September 2012. However, in the first half of 2013 the energy sector continued to attract a high proportion of attacks, ranking in fifth place with 7.6 percent of targeted attacks*".

Also the U.S. government's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has confirmed its engagement in responding to more than 200 incidents between Oct. 2012 and May 2013, with 53% of them aimed at the energy sector.

Nevertheless, Symantec highlighted that most of the attacks to the energy infrastructures "*could have been prevented by following best practice guidelines for protecting the IT infrastructure and the industrial components, indicating that despite high revenues and strategic importance, many energy sector companies are not prioritizing cybersecurity*".

Such a last sentence gives another perspective on the real state of play of the security of Critical Information Infrastructures, or the fact that many of them couldn't have yet started to implement adequate protection measures and might be more than far from implementing resilient ones.

The horizon seems even cloudier when considering that the number of Industrial Control Systems is likely to increase in the future with the consequent increase of the

[4] Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf.

number of potential targets in the energy sector as well as in other vital infrastructures. For these reason, energy companies should invest more efforts in implementing efficient and consistent measures for reducing the impacts of cyber attacks in order to avoid extended loss of services with all kind of catastrophic effects that can cripple many other sectors (e.g. transport, communications, healthcare, financial transactions, governmental operations, etc.).

Up to now, most of the time, the attacks to the energy sector have been "categorized" as local ones – and also between those ones that aren't unlikely to cause fatalities. The debate is still open around the possibility that a single well-planned cyber attack could cause the shutdown of an entire national or regional grid (intended in its largest extension – e.g. the European grid). Even if such risk has been evaluated as low, such an evaluation should not reduce the efforts in implementing resilience measures with the establishment of trans-boundary cooperation in view to strengthen and further develop the security of such delicate and important infrastructures. It's the authors' opinion that one of the main principles that drove the promulgation of the US Presidential Decision Directive NCS/63 – back in 1998 – has still to be considered as the main mission: "*Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare* [of the United States]".

The same approach should also be applied to all of the sectors that are most likely to be targeted by cyber attacks. Among those, the transport and financial ones, that, together with the public administration continuity, stand at the base of the orderly societal lifecycle.

Particularly in the financial sector, the real risk is constituted by the fact that cyber criminals are constantly increasing their capabilities in exploiting the usage of modern technologies for illicit/catastrophic purposes, circumstance that strongly suggest to avoid "defensive" maneuvers only, but specific plans in order to minimize the impact of potential attacks through the establishment of what can be defined as a "resilient society".

4. From Protection to Resilience

In order to decide what to protect and how to protect it, a set of preliminary activities, normally comprehended in the concept of "risk analysis", has to be conducted. These activities include: hazard identification and analysis, risk assessment, risk reduction aimed to reduce the severity of risks through the definition of an adequate protection policy. Any cyber protection policy, in order to be effective, has to cover at least all the following aspects: use of the best (up to date and tested) policies and procedures to prevent cyber attacks, use of the best available techniques and technologies to detect cyber attacks, use of the most advanced technologies in order to grant adequate redundancy of critical data and services, use of well-designed plans in view of gaining the capabilities to quickly recover after a cyber attack.

Past and recent experiences have shown how likely it is that protection policies, sooner or later, may fail. For this reason, and being aware of the fact that the efforts put in place for protection of CIIs can be easily bypassed, all of the stakeholders involved in the security of such delicate and vital infrastructure are strongly suggested to put more emphasis on critical infrastructure resilience.

The US Presidential Policy Directive on Critical Infrastructure Security and Resilience[5] defines resilience as "the ability to prepare for and adapt to changing

[5] *Cfr.* Presidential Policy Directive (PPD- 8): "National Preparedness" promulgated on the 30th of March 2011.

conditions, and withstand and recover rapidly from disruptions due to emergencies." The need for resilience comes from how the threat of a cyber attack is perceived by the apical management of an infrastructure or a governmental agency. The paradigm of cyber security for critical infrastructures, from 2010 and onward, shifted from the concern of the sole risk of attacks coming from outside of the network, to the fact that the attacks can also be generated from the inside, through an infected pen drive, for example, as the "Stuxnet" has clearly shown.

With the clear intention of proposing an embryonic approach for establishing a cyber resilience policy, it can be said that such policy should be based on four lines of defense.

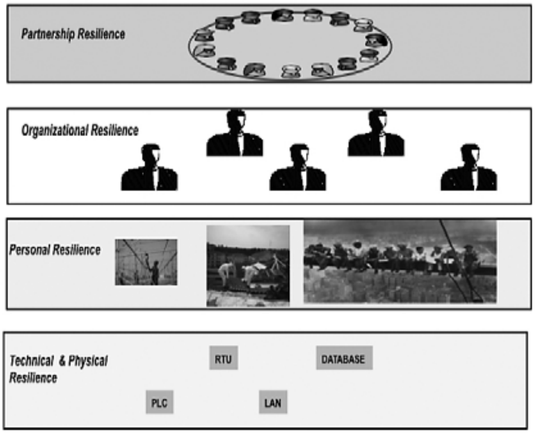


Figure 1. Short caption.

The first line of defense is at the technical and physical level. Physical and technical resilience describes what the Critical Infrastructure has, in terms of implemented tangible safeguards to deter or slow down an adversary (fences, locks, bars, etc.), detect an attack (guards, sensors, electronic access control systems, etc.), and/or to mitigate vulnerabilities (shortcomings or weaknesses in the security posture). Traditional network security controls like firewall, intrusion prevention system, and anti-virus are widely deployed and adequate to keep known threats at bay, but are insufficient to mitigate the risk that is unknown (e.g. 0-day vulnerabilities), unperceived (e.g. lack of training or the presence of insiders) or that can be properly addressed (e.g. software/hardware limits or the infrastructure's obsolescence). These legacy controls are often the key line in defense against these evolved threat actors, many of whom have access to sophisticated R&D resources. While the adversary innovates, in fact, the majority of security infrastructures continue to use dated technology as their primary defense [5].

The second line of defense is at the personal level. Personal resilience is a critical component of systems' resilience. The personal resilience gap of greatest concern is not in defining employer-specific roles and responsibilities an employee has in an emergency. It lies in the employees' own personal preparedness so the employees are available more quickly and with better focus to the organization that relies on them to carry out their emergency roles and responsibilities when emergencies occur. Creating a company's culture of resilience it is already an urgent need that will require to change the way companies perceive themselves in relation to a disaster or an emergency. In an increasingly volatile and uncertain world, one of the greatest assets an organization can have is the agility to survive unexpected emergency situations [6].

The third line of defense is at the organizational level. It is suggested that organizational resilience is best achieved through a systematic decomposition of its elements, based on discernible criteria. This breakdown isolates each of the components and facilitates the identification of key attributes or characteristics. The major pillars of organizational resilience are technical resilience and personal resilience, as described above, and functional resilience intended as a clear responsibility and definition of what to do and who does it [7].

The fourth line of defense is the establishment of collaboration and partnership among different stakeholders. In Europe, the European Public Private Partnership for Resilience (EP3R) was established as a follow-up to the policy initiative on Critical Information Infrastructure Protection (CIIP) adopted by the European Commission on 30 March 2009. The objectives of EP3R are to support Information sharing and stock taking of good policy and industrial practices, and foster common understanding, discuss public policy priorities, objectives and measures, improve the coherence and coordination of policies for security and resilience in Europe and identify and promote the adoption of good baseline practices for security and resilience[6].

In the US, the NIPP 2013[7], Partnering for Critical Infrastructure Security and Resilience, with the view to achieve enhanced security and resilience solutions, embraces a collaborative partnership based on comparative advantage and reinforces the importance of efficient and qualified information sharing. The government, for example, can provide the private sector with access to timely and actionable information in response to developing threats and crises. In addition, the government can help private sector's partners gain a more thorough understanding of the entire risk landscape, enhancing their ability to make informed and efficient security and resilience investments. Finally, industry participants gain an ability to help government planners make better decisions on government security and resilience initiatives, with benefits accruing across critical industry sectors and to the nation as a whole. As the nation's critical infrastructure is largely owned by the private sector, managing risk to enhance security and resilience is a shared priority for industry and government.

5. International Initiatives on Cyber Security

On February 7th 2013, the "Cyber security Strategy of the European Union: an Open, Safe, and Secure Cyberspace"[8] was presented through a press conference with the important remarks of Catherine Ashton (EU high representative), Neelie Kroes (Vice-President of the European Commission responsible for the Digital Agenda) and Cecilia Malmström (EU Commissioner for Home Affairs).

The remarks revolve around the fact that we rely on cyberspace in almost every sector of our lives, and thus the importance of defending it from cyber attacks. Neelie Kroes has underlined one of the critical points of the EU Strategy, that is to say cyber resilience: "*We need to protect our networks and systems, and make them resilient. That*

[6] https://resilience.enisa.europa.eu/ep3r.

[7] http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20 Infrastructure%20Security%20and%20Resilience_508_0.pdf.

[8] http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf.

can only happen when all actors play their part and take up their responsibilities. Cyber threats are not contained to national borders: nor should cyber security be. So our strategy is accompanied by a proposed Directive to strengthen cyber-resilience within our single market. It will ensure companies take the measures needed for safe, stable networks. […] *Europe needs resilient systems and networks. Failing to act would impose significant costs: on consumers, on businesses, on society. A single cyber incident can cost from tens of thousands of euros for a small business — to millions for a large-scale data breach. Yet the majority of them could be prevented just by users taking simple and cheap measures*."

In the aforementioned report, the achievement of cyber resilience is the first of five strategic priorities of the EU in order to efficiently tackle cyber threats. The pivotal factor for achieving a status of resilience for critical infrastructure is promoting Public-Private Partnership and collaboration. An additional factor is that the EU could permit further security, in cases of threats with transnational characteristics, also coordinating a collective response. For these reasons, the mandate of the European Network and Information Security Agency (ENISA) was strengthened and modernized. In order to try and close the security-gap among Member States, the strategy of the European Union was associated with a proposal of legislation, that aims at setting for example "common minimum requirements for Network and Information Security (NIS) at national level which would oblige Member States to: designate national competent authorities for NIS and set up a well-functioning Computer Emergency Response Team [that would coordinate with the] Computer Emergency Response Team responsible for the security of the IT systems of the EU institutions, agencies and bodies ("CERT-EU") [that] was permanently established in 2012".

The strategy stresses the importance of the public-private engagement as a paramount step, given the fact that most of the infrastructures are property of, and operated by, private bodies. On the other hand, from the private point of view, it is necessary to raise awareness on the risks of cyber threats and establishing a risk management culture, in order to make the network and the information systems of a given infrastructure resilient.

The infrastructures' owners should also share information with the national NIS authorities and report any incident, in the same way that US infrastructures report to the US-CERT. One means to foster the Public-Private Partnership could be the European Public-Private Partnership for Resilience (EP3R), that is a platform for public-private cooperation "on the identification of key assets, resources, functions and baseline requirements for resilience as well as cooperation needs and mechanisms to respond to large-scale disruptions affecting electronic communications". The last two aspects that the strategy takes into count are the financial support for critical infrastructures that would come from the Connecting Europe Facility (CEF) and the organization of cyber incident exercises at EU level. After the Cyber Europe 2010 and 2012, the second one included also the private sector, a set of nations have now publically developed and published their National Cyber Security Strategy (NCSS) or, alternatively named, a National Information Security Strategy. Due to the global nature of cyberspace, international collaboration could be expected to be one of the highest priorities of each of the NCSS.

Given the enhanced and more focused European approach, a specific Critical Information Infrastructure Protection and Resilience Unit have been established at ENISA[9]. The Unit is responsible for assisting competent national EU agencies, the private

[9] http://www.enisa.europa.eu/activities/Resilience-and-CIIP.

sector and the EU Commission to develop sound and implementable preparedness, response and recovery strategies, policies and measures that fully meet the emerging threats critical information infrastructures face today.

On 12th February 2013, the president of the United States Barack Obama issued an Executive Order entitled "Improving Critical Infrastructure Cyber security", which has similar principles and measures to those included in the Cyber security strategy of the European Union.

Undoubtedly, this is a sign of how an important challenge the cyber security of Critical Infrastructures – and of their Industrial Control Systems – is becoming in different international contexts.

6. Italian Initiatives on Cyber Security

On March 19th, 2013 the much awaited and coveted Cyber security Decree[10] (DPCM January 24th, 2013) was published in the Italian Official Gazette. The Decree sets forth the new government architecture that is entrusted with the task of facing potential cyber security threats in Italy.

The Prime Minister is at the top of the organizational structure established by the Decree along with the "Committee for the Security of the Italian Republic" (CISR), which has the task of defining the national security strategy (the so-called "National Cyber Security Strategy"). A "collegial co-ordination body" supports the first level of such an organizational structure. The collegial co-ordination body is chaired by the Director General of the Department for Information Security (DIS). The Military Adviser assisting the Prime Minister also attends the meetings of the collegial co-ordination body.

On December 9th, 2013, the Italian Cyber Security Report 2013[11] was released from the Cyber Intelligence and Information Security Center of Sapienza University of Rome. The Report gives a breakdown of the Italian standpoint in the context of the protection of national critical infrastructure and other sectors from cyber attacks from the legal and technological viewpoints.

The Research Center of Cyber Intelligence and Information Security (CIS) is a multidisciplinary centre developing new knowledge and operational methodologies to gather relevant information from cyber and physical environments and to transform it through intelligence processes in enriched information that can be used to prevent incidents that can harm the society by creating at the same time smarter complex systems.

On February 2014, the Italian Presidency of Council of Ministers publically released the "National Strategic Framework for Cyberspace Security"[12] and the "National Plan for Cyberspace Protection and ICT Security"[13].

The National Cyber security Strategic Framework sets out the strategic guidelines that must be pursued through a joint effort and a coordinated approach of all key stakeholders of the national cyber security architecture identified by the Prime Minister's

[10] Available at: http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2013-03-19&atto.codiceRedazionale=13A02504&elenco30giorni=true.

[11] Available at: http://www.uniroma1.it/sites/default/files/2013CIS-Report.pdf.

[12] Available at: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.

[13] Available at: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf.

Decree of the 24th January 2013, under the coordination and guidance of the Committee for the Security of the Republic.

These guidelines include:

- The enhancement of the technical, operational and analytic expertise of all institutions concerned with cyber security;
- The strengthening of the cyber protection of ICT networks and computer systems supporting our critical and strategic infrastructure;
- The facilitation of public-private partnerships; the promotion of a Culture of Security and of cyber hygiene; the improvement of our skills to effectively contrast online criminal activities;
- The reinforcement of the capability to effectively contrast online criminal activities;
- The full support to international cooperation initiatives in the field of cyber security.

In accordance with these six strategic guidelines, eleven operational guidelines have been identified:

- Enhance the expertise of the intelligence community;
- Identify the Network and Information Security (NIS) Authority that will engage at the European level;
- Develop a widely shared cyber taxonomy and promote a common understanding of cyber security terms and concepts;
- Foster Italy's participation in international initiatives to enhance cyber security;
- Attaining the full operational capability of the National Computer Emergency Response Team;
- Compliance with international obligations;
- Compliance with standards and security protocols;
- Support for the industrial and technological development;
- Strategic communication;
- Allocation of adequate human, financial, technological and logistic resources to the strategic sectors of the Public Administration;
- Implementation of a national system of information risk management.

The National Plan (NP) identifies the operational guidelines, the goals to pursue and the lines of actions to be carried out in order to give full implementation to the National Strategic Framework for Cyberspace Security (NSF), in line with what is outlined by the Prime Minister's Decree of 24th January 2013 setting out "Strategic Guidelines for the National Cyberspace Protection and ICT security".

7. Conclusions

There is clear evidence of the fact that cyber attacks to critical infrastructures and, above all, to energy and transport infrastructures are constantly increasing. The difficulties intertwined with the events that are characterizing these assets that are vital for the orderly societal living and for the economy, demand that top managements, policy makers, technology/education/training and certification providers to rethink their operative models so as to include and start spreading, in their respective area of influence, the principles of resilience. Examples of initiatives on cyber security have been briefly reviewed in the paper and the feeling is that such initiatives should be initialized at all of the levels of the "security pyramid" so as the principles of resilience can begin to 'break in' and be hardcoded in the business and management strategies, regulation, policies, under/postgraduate courses, measures, protocols and technologies to be established and implemented for facilitating the prompt recovery of an infrastructure and the prompt reestablishment of a service that has suffered a disruption.

At the same time, it's opinion of the authors that such initiatives should be somehow coordinated around clear objectives and long-term achievement. The risk is, in fact, that the lack of consensus around the most urgent matters and the lack of vision of the future of cyber security will reduce the impact of harmonization with the consequence of very fragmented and less effective approaches.

From the experiences gained up today, we may suggest the following initiatives:

- Strengthen management, skills and capacity within risk analysis, security evaluation and resilience by design;
- Closer integration of topics related to physical, personnel and IT security;
- More training and increased standardization within emergency preparedness;
- Strengthened cooperation within public–private, and in the industry's own networks and organizations within areas such as intelligence, safety and security analysis;
- Development of a holistic, coherent and synergic approach, at national level, so as to enhance the country's preparedness, resilience and reaction capabilities;
- Enhance education skills and develop a multicultural approach to cyber security in university and research centers;
- Promote dissemination activities and increase awareness among the population;
- Cyber threats are not contained to national borders: nor should cyber security be.

References

[1] L. Tabanski, Critical Infrastructure Protection against Cyber Threats, *Military and Strategic Affairs*, Vol. 3, No. 2, (2011).

[2] P. Theron, S. Bologna, Critical Information Infrastructure Protection and Resilience in the ICT Sector, IGI Global, Hershey PA, 2013.

[3] Y. Lenchner, *The Rise of Critical Infrastructure Attacks: Understanding the Privileged Connection and Common Thread*, IntelligentUtility, 2013.

[4] S. Bologna, A. Fasani, M. Martellini, *Cyber Security. Deterrence and IT Protection for Critical Infrastructures*, Springer, 2013, 57-72.

[5] General Dynamics, *Defending against cyber attacks with session-level network security*, 2010.

[6] A. Coos, R. Bearse, *Strengthening Resilience of the Nation's Most Important Asset: People*, The CIP Report, 2013.

[7] W. Boone, 2014, *Functional Resilience: The "Business End" of Organizational Resilience*, The CIP Report, 2014.

[8] C. Wueest, *Targeted attacks Agains Energy Sector*, Symantec, 2014.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-91

Protecting Critical Information Infrastructure from Terrorist Attacks in South East Europe: How Real is the Threat?

Metodi HADJI-JANEV[1]
Military Academy "Genral Mihailo Apostolski", Skopje; Associated member of the University "Goce Delcev"-Stip, Republic of Macedonia

Abstract. The process of globalization and the rise of information and telecommunication technology have significantly affected global and South Eastern -SEE security. On one hand, thanks to the development of these technologies and geopolitical dynamics, the region of SEE is becoming more interconnected, interrelated and shaped by modern infrastructures that enable respective SEE countries' commodities, prosperity and competitiveness. On the other hand, like in the rest of the world, these processes and dynamics have increased unpredictability, complexity and threats to the SEE security in the context of modern terrorism. At the same time, the recent history of violent conflicts, social stability challenges, Euro-Atlantic ambitions, support to the "global war on terror" and the increased presence of radical religious groups and individuals in the region of SEE are variables that further affect its security. Today, modern terrorist groups and individuals exploit cyberspace to achieve strategic advantages against the mightier enemies. Given that their agenda is violent, abstract and apocalyptic protection of the critical information infrastructure has become one of the main concerns for NATO and its allies. Therefore the article explores how and in which way terrorists' use of cyberspace could affect critical information infrastructure in the region of SEE. To achieve this, the article first explains contemporary terrorists' objectives around the globe and compares them with the objectives that these actors have in the region of SEE. In this context the article briefly explains the development and achievements of the ICT sector in the region of SEE and analyzes them into the context of cyber-based threats posed by modern terrorism. Then the article provides an assessment of how the terrorists' use of a cyberspace affects critical information infrastructures in the region of SEE.

Keywords. Critical information infrastructure protection, Modern terrorism, South East Europe, cyber-attack

"The Internet is a prime example of how terrorists can behave in a truly transnational way"; Ban Ki-moon, Secretary-General of the United Nations

[1] Corresponding Author: Dr. Metodi Hadji-Janev, Military Academy "Genral Mihailo Apostolski", Skopje; Associated member of the University "Goce Delcev"-Stip, Republic of Macedoni; e-mail: hadzijanev@yahoo.com

Introduction

Information and communication technology (ICT) and the use of cyberspace play crucial roles in the region of South East Europe (SEE). Cyberspace is the dominant place for social, economic and political activities in all SEE countries. Economic and management efficiency among others urge SEE countries to follow the best practices around the globe of connecting supervisory controlled and data acquisition systems (known as SCADA) that run critical infrastructure to the internet. Nevertheless, the growing dependence on cyberspace in SEE has not been matched by a parallel focus on security.

Parallel to these trends and dynamics, the threat from global terrorism also gravitates over SEE. Recent practices show that the cyber - world has become both a battle-space for modern terrorists' ideological and information warfare and a medium for global radicalization. Thus, many states have seriously considered measures and mechanisms to improve critical information infrastructure protection. As for the rest of the World, terrorists' use of a cyberspace represents a significant threat vector that underpins SEE's security. This undoubtedly urges the SEE government to: identify, assess, mitigate, and develop mechanisms to counter terrorist threats from cyberspace. Pundits, academics and intelligence officers disagree over the terrorists' ability to affect our security through attacking critical information infrastructure. Furthermore, while some countries nest critical information infrastructures protection under general critical infrastructure protection policies and strategies others make distinctions between the two. Giving that these trends in the region of SEE are new and in the process of development, after explaining terrorist threats in the context of cyberspace, one has to understand how the concept of critical information infrastructure protection works. Hence, after accomplishing this, this article will assess whether or not the threat of terrorists' use of cyberspace to the CII in the region of SEE is real or not. If yes, to what level, and if not, why is this so?

The article accomplishes this through several assumptions and facts. First, the region of SEE consists of Albania, Bulgaria, Bosnia, Croatia, Greece, Macedonia, Montenegro, Romania, Serbia and Slovenia. Second, although some of the SEE countries are NATO and EU members, Albania is only NATO, and others are PfP countries. The article takes the NATO-based policy approach in the process of CII, i.e. that although there is in general NATO's guidance about cyber security, all of the SEE countries are responsible for developing cyber security policies.

1. Modern Terrorism and South East European Cyberspace

Modern terrorism is a serious threat to global peace and security [1]. Both academics' and pundits' communities generally agree that groups and individuals with violent, religious, global and abstract agendas comprise what we called modern terrorism. These groups and individuals are usually affiliated with Al Qaeda and are known as Al Qaeda and its Associated Movements (AQAM) [2]. A study on Al Qaeda lasting more than ten years conducted by Jytte Klausen shows that these franchise-types of organizations (meaning AQAM) have centralized planning and decentralized execution [3]. Usually a small group of people orchestrates and plans the operations. Later these operations are delivered by local cells that may, but usually do not have connections with the planners.

Some of these groups have real ties to Al-Qaeda and share its goals. In politically fragile societies there are those who hide behind the cause to cover their criminal activities. Others, like the ones in Africa, look like local warlords using the label to burnish their brand [4]. In all cases, some really understand the goal and the cause they serve, but some are only angry and the victims of radicalization [5]. Hence, modern terrorism is a hybrid threat composed of terrorists, criminals, insurgents and religious extremists.

Several studies have shown that to achieve strategic advantage and gain global support while confronting mightier adversaries the core cadre of AQAM heavily abuse modern information and communication technology (ICT). According to a recently published UN study (further the UN study), terrorists are using the internet to promote and support terrorist activities through six different and overlapping categories [6]. The UN study explains that the terrorists use the internet for: propaganda (including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyber attacks. Other independent studies point that the decentralized nature of the Internet as a medium and the associated difficulty in responding to emerging threats match the franchised nature of terrorist organizations and operations [7]. Some reports emphasize the learning opportunities that the Internet offers to terrorists. In his in-depth analyses of how terrorists use the internet, Gabriel Wimann explains how different websites provide advice and has manuals on how to build and operate weapons and how to pass through border checkpoints [8]. The London Bombing attacks are a clear example of how powerful this can be [9]. Committing cybercrime activities to fund their decentralized terrorist operations is another abuse of the internet. According to press reports, Indonesian police officials believe the 2002 terrorist bombings in Bali were partially financed through online credit card fraud [10]. Additionally during the 2007 UK trial for the 2005 London terrorists' bombing, the accused revealed that 72 stolen credit cards were used to register over 180 Internet web domains at 95 different web hosting companies [11]. Other well supported evidence about the modern terrorists' intent to use the internet for direct attacks of critical infrastructures and cause severe consequences clearly attests about the danger that modern terrorism poses to our security.

Current security dynamics related to modern terrorism have also affected the region of SEE. The complex history of religious and ethnic conflicts so far seems that it serves as a perfect match for AQAM. In this context, the rising influence of radical and violent Islam is a new and dangerous trend in the region that holds potential for destabilization beyond its borders.

The ICT and the use of a cyberspace play crucial roles in the region of SEE. The pursuit of modernization, the Euro-Atlantic integration and the necessity of foreign investments among others have urged SEE countries to invest in the development of ICT and cyberspace. Thus, virtual cyberspace has become the dominant place for social, economic and political activities in the region of SEE. The growing dependence of cyberspace in the SEE however, has not been matched by a parallel focus on security.

During the Kosovo campaign, for example, NATO arguably experienced the first ever organized cyber-attacks [12]. According to the local SEE and world news, recent reports, and studies, many SEE countries are facing experienced cyber activists but the awareness of these threats is not promising. The news reports, back in May of 2013, informed that three Romanian nationals were caught taking part in a multimillion dollar cyber fraud ring that specifically targeted U.S. consumers and the trio ended up making off with more than $2 million [13]. Although not a regional trend *per se*, the mysterious disappearing of a cyber crime writer in Bulgaria in 2010 and 2011 speaks that actions in SEE cyberspace has significant influence on security [14]. Although reports misinterpreted the information, a young hacker from Macedonia back in 2012 was detained due to cybercrime allegations (i.e. attempting to illegally penetrate several security websites in the US) [15]. Reports about working in a network with hackers from different countries also indicate the threat in SEE Cyberspace. Individuals from Britain, the US, Bosnia and Herzegovina, Croatia, Macedonia, New Zealand and Peru were arrested in an operation carried out with the assistance of Facebook and international law enforcement agencies [16]. Although the threat is present, some of the plot researches in the region show alarming results when it comes to awareness level. The pilot research conducted in Slovenia displayed a serious lack of awareness regarding different forms of cybercrime among the general public, as well as the members of law enforcement agencies, and consequently also a poor understanding of legislation pertinent to cybercrime [17].

The former analysis is especially important if one puts it into the context of current events in the Islamic community and terrorists' use of cyberspace in SEE. In fact, it could be argued that SEE cyberspace has become a platform for committing various types of illegal activities including terrorist activities through cyberspace. At the same time, on several occasions, (NATO Parliamentary Assembly in 173 DSCFC 09 E BIS - NATO and cyber defense, NATO's New Strategic Concept - 2010; The 2012 Chicago declaration, etc.) NATO has emphasized that threats from cyberspace to NATO countries and Partners are real. Given that some of the SEE countries (Albania, Bulgaria, Croatia, Greece, Romania and Slovenia) are NATO members and some (Bosnia, Macedonia, Monte Negro and Serbia) are Partner nations- (PfP countries) addressing the issue of terrorists' use of cyberspace in the current security environment is more than urgent. This is especially true in the light of the recent trend to connect control systems that run critical infrastructure to the internet.

Energy experts David Kennedy and John Besant-Jones in their study on South East Europe Regional Energy Market (SEEREM) argued that establishing such a market among the SEE countries is a major development for this region. One of the arguments that they made is the urgent need to implement the so called Supervisory Control and Data Acquisition-SCADA. Calling upon similar experience around the Globe, they argued that implementing SCADA will help to improve system reliability, and therefore support integrated system operation, reducing potential negative spillover effects between countries [18]. Similar independent-country-based studies confirm these findings [19]. Nonetheless, despite the fact that these initiatives are highly welcomed among the SEE political elites, SCADA systems are rare in SEE. Even if there are some SCADA systems, these systems are not connected to the internet and are just partially promising projects. Thus, the global security trend in the context of potential SCADA cyber attacks that drives western based academic and security experts' considerations over the threat from the so called "cyber terrorism" at least for now, seems to have little relevance for SEE cyberspace. This arguably raises the question of how and in what way terrorists' use of cyber space could threaten the critical information infrastructure in SEE.

2. The Terrorists' Threat to the Critical Information Infrastructure in the Region of SEE

2.1. The concept of Critical Information Infrastructure Protection and Security Trends in SEE

Much has been written about the critical information infrastructure protection (CIIP). However, there is no generally accepted definition of what constitutes critical information infrastructure. While some countries and organization distinguish between critical infrastructure and critical information infrastructures, others integrate both as essential elements of national crisis management, homeland security or overall defense systems. The OECD report on development of policies for protection of CII explains that in Australia, Canada, Korea, The Netherlands, The United States and the United Kingdom the concept of the critical information infrastructure is captured within the context of the critical infrastructure [20]. According to the report, South Korea is the only country participating in the study to make an explicit reference to critical information infrastructure. The EU and NATO have the same approach of distinguishing between CI and CII. Nevertheless, the Member States remain ultimately responsible for defining CI and CII-related policies [21].

Entities that make a distinction between CI and CII approach generally define CI as "The Critical infrastructures (CI) are those systems that provide the resources upon which all functions of society depend" [22]. Examples are telecommunications, transportation, energy, water supply, health care, emergency services, manufacturing and financial services. When these entities define CII they focus on "communications or information service[s] whose availability, reliability and resilience are essential to the functioning of a modern [national] economy, security, and other essential social values" [23].

Bringing the discussion into the context of an SEE approach to CIIP at first glance might look confusing for several reasons. The complexity with this approach begins with the fact that not all of the SEE countries are EU and NATO members. Second, not all EU and NATO members have identified critical information infrastructures. This is especially relevant for the SEE countries. Third, although due to their Euro-Atlantic aspirations almost all SEE countries follow EU guidance on CI identification, there are no EU or NATO guarding standards for these infrastructures. The protection itself depends on the Member State's capabilities.

When it comes to the SEE countries' legacy in a defense and security context, it could be argued that in general SEE countries share the same legacy and challenges. Almost all of the SEE countries (except for Greece) transitioned from a socialist system to democracies (although with a different tempo). In all SEE countries protection concepts for strategically important infrastructures and objects have been part of the national defense planning systems for decades. The processes of globalization and technological development have imposed almost the same if not equal challenges to all SEE countries. Contemporary security dynamics created hybrid and asymmetric threats which in the region of SEE are usually posed by non-state actors (groups and individuals with terrorist or criminal affiliation). At the same time the trend of modernization has imposed new types of vulnerabilities due to modern society's dependence on inherently insecure information systems.

Today it is more than clear that the modern terrorism practiced by AQAM among other works is under a critical infrastructure- and critical information infrastructure-oriented agenda. After the 9/11 attacks, attacks in Bali, Madrid, London and similar alike confirm these views. Although terrorists' capability to affect cyber security as a mere trend has existed in the past, security experts have begun to address these issues more closely after 9/11 and the so called 2000 Bali attacks. A 2003 private study found that during the latter half of 2002, the highest rates for global cyber-attack activities were directed against critical infrastructure industry companies [24]. Another report on industrial cyber-security problems using data from as far back as 1981, has reportedly found a 10-fold increase in the number of successful cyber-attacks on infrastructure Supervisory Control and Data Acquisition-SCADA systems since 2000 [25]. Recent reports also indicate the growing threat perception from modern terrorism practiced by AQAM [26]**.** Although until today we haven't witnessed a successful large-scale terrorist cyber-attack that has caused casualties, the treats from AQAM to SEE CII remain important. On the other hand, focus on the concept of protecting critical information infrastructure is important to SEE for several reasons.

First, development of the ICT sector and the subsequent modernization of the SEE societies like in the rest of the world have created a highly interdependent software-based network of networks. Urged by the global trends of modernization, interest to attract foreign investor and the Euro-Atlantic integration processes almost all SEE governments have focused on building the so called e-governance. This undisputedly means that the risks to affect the SEE countries' security have significantly grown. In fact, the urgent need for greater connectivity under the pressure of the highly competitive market logic always affects security.

Second, in 2004 The Secretary-General's High-level Panel Report on Threats, Challenges and Change, recognized that security has dramatically evolved [27]. In this changed security environment Dave Clemente carefully observes that "There is no avoiding the security implications emerging at the intersection of cyberspace and critical infrastructure" [28]. Similarly the EU and NATO have recognized on several occasions that ICT systems, services, networks and infrastructures form a vital part of our economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. These infrastructures, according to the EU and NATO, are typically regarded as critical information infrastructures (CIIs) as their disruption or destruction would have a serious impact on vital societal functions. Connecting the large-scale cyber-attacks targeting Estonia in 2007 and the breaks of transcontinental cables in 2008 clearly attest that analyzing CIIP does not have to include terrorist attacks on the SEE SCADA systems.

Third, along with NATO's and the EU's approach, many leading states in the field of CIIP have recognized that threats from non-state actors depending on their motivation or their targets could come either from "cybercriminals" or from "cyber terrorists". Although some may view a huge distinction here, the current trend in many countries' security documents discussing CIIP is that economic well-being and national security are closely interconnected. For Estonia, for example, the purpose to protect CII is related to proper functioning of the country during emergencies [29]. Similarly for the United States, terrorists could incapacitate or destruct CII which would have a negative or a debilitating impact on national security, national economic security, national public health or safety, or any combination of those [30]. The German federal Biro for information security also considers that current threats and vulnerabilities of the critical infrastructure require joint efforts from government and economy [31].

Fourth, threats to CII do not exclusively come from cyberspace. The Stuxnet attack on the Iranian Nuclear power plant will definitely rewrite the cyber terrorism playbook [32]. In this context David Geer earlier this year offered statistical arguments clearly speaking of the increased physical danger risks of cyber terrorism [33]. Even more, if the Spiegel's story about the so called "Operation Orchard" by Erich Follath and Holger Stark, published back in 2009, is true, then it would be clear why the denying the terrorist threat to the SEE cyberspace or CII in the region of SEE will not make any sense [34].

Finally, it is well established among the academic, pundit and intelligence community that SEE have emerged as a battleground for radical militant Islamism. Although there are those who deny these views, many provide credible anecdotal evidences about the dangers that modern terrorism poses to the security of SEE. Early researches and writings about this region's connectivity to Al Qaeda, for example, can be found in Yossef Bodansky's book from 2001 [35]. Others have written more specifically about the connectivity between Al Qaeda and the SEE. In 2004, Kohlman has tried to explain the Afghan-Bosnian modus operandi and the network [36]. Citing figures like Abu Jandal (the suspected bodyguard of Osama Bin Laden), after interviewing him, Fawaz Gerges explains how radical Islam came and started to change the landscape of the Muslim Community in the region [37]. What is particularly interesting is that the interview explains that the reason of being here for these militants is not just to support the fight against the Serbs or the Croats, but much broader and with a different goal. Recalling of his journey to Bosnia, Abu Jandal claimed that (according to him): …"*They (*Bosnian youth*) were completely ignorant of Islam… Therefore, we saw that the responsibility we shouldered in Bosnia was broader and more comprehensive than the mission of combat, for which we had come. So we found that we became bearers of weapons and at the same time bearers of a call, a book, a message…"*[38]. Similar writings about the region (including Albania, Kosovo, Macedonia Serbia etc.) can also be found in Deliso's 2007 book [39] or in the Spanish researcher Juan Carlos' 2008 research [40]. Although one could find these researches as subjective, the UN studies dedicated to this problem seem to confirm most of the findings of the above mentioned writings. The recently published UN Study report about the connection of individuals, groups, undertakings and other entities associated with Al-Qaida puts Bosnia among the top countries that serve as sanctuary for AQAM [41]. According to this UN report, Bosnia has the same number of organizations (five according to the report) linked to Al Qaeda as Pakistan and is just behind Afghanistan, which is on the top of the list. More interestingly, the report identifies such groups and individuals in Albania and Kosovo too. Al-Haramain, an organization that operates in Afghanistan is mentioned in the report as an Albania branch [42]. "Al Rasheed Trust", a similar path, has connections to Chechnya, which according to the report from 2014, operates in Kosovo [43]. If one puts these findings into the context of Jytte Klausen's conclusions (mentioned earlier) about the franchise mode of operation, it would be more than clear that individuals and groups that identify themselves with the violent and radical Al Qaeda's agenda are present in the region of SEE.

Nevertheless, parallel to these written evidences, based on research or analyses, considerable empirical evidence stems from the recent events. These events confirm that individuals and organizations linked to Al Qaeda are not using the region just for sanctuary but also for targeting. The June 2010 bomb attack on a police station in the central Bosnian town of Bugojno [44]; the 2011 attack on the US Embassy in Bosnia

[45]; the 2012 attack and murder of 5 civilians in Macedonia [46] and the 2012 attack on Israeli tourists in Bulgaria [47]; along with numerous reports about prevented attacks or arrests (ex. Bosnia, Serbia, Croatia, Kosovo, or Cyprus) [48] confirmed that the threat from these adversaries is real. Furthermore, recent trends in active support of radical Islamic groups in Syrian resistance and growing numbers of internet based recruitments for these supports, along with the alleged on-line radicalization before, the above mentioned attacks and attacks around the globe connected with the region, raise serious concerns over the terrorist use of cyberspace in the region of SEE. This poses the question of how the terrorists' use of a cyberspace could be a threat to SEE CII.

2.2. Assessing the Threat: Terrorists' use of South Eastern European Cyberspace in the context of Critical Information Infrastructure Protection

During 2002 the US Navy War College conducted a war game called "Digital Pearl Harbor". One of the purposes of this activity was to assess the threat and consequences of a potential terrorist cyber-attack [49]. The result from the exercise was positive for the U.S. at that time, i.e., the exercise proved that attempts to cripple the U.S. telecommunications infrastructure would be unsuccessful because system redundancy would prevent damage from becoming too widespread. Nevertheless, the simulated scenario revealed that the most vulnerable information infrastructure was the Internet itself. The former is especially important in the context of SEE cyberspace and threats from modern terrorism.

A direct threat to SEE critical information infrastructure in terms of causing an attack that could result in the loss of lives and material cost is almost impossible. Therefore the main focus of further analysis would be on the indirect threat that modern terrorism could cause through abusing the most vulnerable information infrastructure in the SEE i.e. the "Internet itself". The following debate will use current findings and explain how terrorists' use of cyberspace could cause serious threats to the security of SEE.

2.2.1. The Terrorists' use of SEE Cyberspace for the Dissemination of Propaganda

Many analyses show that one of the primary uses of cyberspace by terrorists is for the dissemination of propaganda. According to the official UN Study on the Use of the Internet for Terrorist purposes "*…propaganda generally takes the form of multimedia communications, providing ideological or practical instruction, explanations, justifications or the promotion of terrorist activities*". Practice shows that designing the propaganda materials is a carefully prepared process that articulates the existing challenges that creates a burden to the all societies. In the region of SEE these materials also attack fragile ethnic relations. First, there is a misinterpretation of the general social challenges (unemployment or severe social conditions). Then they bring these challenges in the context of ethnic challenges. Inconsistencies and social inequalities in the SEE societies are usually emphasized with specific graphic material acceptable to the target audience and always with a religious prefix. The religion is offered as relief and hope. So far, however, it could be argued that there is nothing wrong with what they do. Thus, the final product is ideological material ready to be shared online or through SEE cyberspace [50].

Later, specific events which are usually linked to ethnic issues or negative images that are still fresh from past conflicts are usually used as vectors that instigate propaganda. Events in Kosovo in 2011 after the decision to construct a Catholic Church to honor

Mather Teresa represent an example of such practice. A similar example represents the aftermath of events such as the designation of Florim Neziraj and Sadullah Bajrami as a supreme religious officials in the Kacanik region of the trends and dynamics in this direction [51].

The dissemination of the propaganda material usually includes messages, opinions, presentations, magazines and periodicals, audio and video files, and even video games developed by terrorist organizations or sympathizers [52]. Existing YouTube spots and websites could also link to other sites from different regions in order to amplify the effect and present the global movement. For example, the Facebook page called "Islamic Pride" has several posts against voting, including a video in which bearded men call on Muslims to boycott elections, arguing that true Muslims may not vote. In other posts and pictures, Islamic Pride attacks moderate Islamic leaders in Albania and Kosovo especially those who favor the West.

Several sites, however, are well known for spreading religious intolerance and violence, including suicide attacks and anti-democratic messages. In this context Facebook, Twitter and other online social media have become a serious problem too. According to some estimates over the last year, dozens of videos and Facebook pages advocating extremism have appeared on the SEE cyberspace [53].

According to Balkan Insight news, in a video message shot in Syria and posted on YouTube, a person called Lavderim Muhaxheri called on Muslims to join the fight to establish an Islamic state based on *Sharia law*. According to the same report, one picture posted on the page, seen by Balkan Insight, shows about a dozen armed men, wearing black masks, with the title, "Albanian Mujahedeen of the Islamic State of Iraq and Syria, with their battalion leader". The same person has also tried to convince others indirectly with posts like this "We thank Allah for allowing us to join these lions from all over the world to protect here the honor of our Muslim sisters" [54].

What is significant though is that this process is a growing trend in the SEE cyberspace. Recent studies on Balkan extremists' use of the internet and social media has shown alarming results. These results are surprising if one considers that Islam in this region has always been with a moderate prefix [55]. The number of those who are 'liking,' making comments and sharing the content of these pages, especially when it comes to religious leaders, extreme Islamists and Wahhabists, is rising on a daily basis [56].

AQAM's indirect threat to SEE CII – i.e. the internet itself, however does not stop here. Many materials and methods of propaganda aimed at potential or actual supporters also focus on recruitment, radicalization and incitement to terrorism. This usually is achieved through messages conveying pride, accomplishment and dedication to an extremist goal.

2.2.2. Challenges from the Terrorists' use of SEE Cyberspace for Instigation, Recruitment, Radicalization and Communication

According to the above mentioned UN Study on the Use of the Internet on Terrorist purposes, "*recruitment, radicalization and incitement to terrorism may be viewed as points along a continuum*". This study stipulates that "radicalization" refers primarily to the process of indoctrination that often accompanies the transformation of recruits into individuals determined to act with violence based on extremist ideologies. The process of radicalization, according to the Study involves "*the use of propaganda, whether communicated in person or via the Internet, over time*". The length of time and the effectiveness of the propaganda and other persuasive means employed vary depending on individual circumstances and relationships. These circumstances are specific to the region of SEE.

In this light the wave of modernization and increased ability to ITC access have positive and negative aspects to SEE. SEE governments' efforts to modernize the respected societies have brought increased efforts to reduce ICT cost and to introduce cyberspace into everyday life for its citizens. On the other hand, as in the rest of the World, the reach of the Internet provides terrorist organizations and sympathizers with a global pool of potential recruits.

The Internet may be used not only as a means to publish extremist rhetoric and videos, but also as a way to develop relationships with, and solicit support from, those most responsive to targeted propaganda. Scott Gerwehr and Sarah Daly argue that terrorist organizations increasingly use propaganda distributed via platforms such as password-protected websites and restricted access Internet chat groups as a means of clandestine recruitment [57].

General trends in the instigation, radicalization and recruitment process show that those who radicalize and spread the agenda are very adaptive to different environments. They skillfully abuse modern technology and employ very persuasive methods of spinning Islam while attacking fragile groups or individuals from society. So far they have been very successful in radicalization and gaining followers in problematic societies (failed states and rogue states). However, building their argument on the challenges of the very society they live in, these groups and individuals are also present in stable and democratic societies.

Usually like the propaganda activities, online instigation, recruitment, radicalization and communication processes in the SEE are adapted to account for demographic factors such as age or gender, as well as social or economic circumstances. The Internet therefore is a particularly effective medium for the recruitment of minors, who comprise a high proportion of users. The process of online instigation, recruitment and radicalization in the region of SEE commonly capitalizes on an individual sentiment of injustice, exclusion or humiliation [58].

The case of Arid Uka, a young Kosovo Albanian who committed a terrorist attack on US Airmen in Germany during 2010 is a clear example and product of such radicalization. According to his lawyer, Uka had watched a video the night before the attack purporting to show American soldiers raping a teenage Muslim girl. It turned out to be a scene from the 2007 anti-war movie "Redacted," which had been taken out of context. Thus, Uka was a victim of an online recruitment and radicalization process (conducted in a decentralized way-as a lone wolf, self radicalized terrorist) from sites that popularize radical ideas through youth culture, song and video. Uka confessed that he listened to Islamic music on his iPod while nursing doubts that would be able to follow through with his plan [59].

An additional problem for the SEE government in this context is the ability to find the right balance between public safety and individual human rights. Some intergovernmental and human rights organizations have expressed doubt that the concept of "glorification" of terrorism is sufficiently narrow to be criminalized. Basic concerns often are connected to potential violation of the human rights (precisely permissible limitations of the right to freedom of expression, as enshrined in articles 15 and 19 of the International Covenant on Civil and Political Rights).

It is true that there is legal ground for SEE governments to prevent incitement of terrorism. The problem with this legal framework is that it has a limitation. For example, while article 19, paragraph 3, of the International Covenant on Civil and Political Rights allowed public authorities to limit freedom of speech, article 20 paragraph 2, requires States to prohibit any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. This, nevertheless, is possible only if the required restrictions are necessary and proportional to the threat.

Both, "proportionality" and "necessity" are hard to prove for three reasons. First, the technical reason, the internet is a platform that allows users to hide their IP addresses. Second, the problem with attribution and third, the so called *Lex loci* challenge, i.e. that the user or particular website may communicate and influence the web from around the globe [60]. In this context the recent European Court of Justice's decision from April 8 2014 that the Data Retention Directive is invalid is yet another example that confirms this view.

Efforts to sanction online instigations, nonetheless, remain in the vacuum in most of the SEE countries. Propaganda designed to recruit minors takes the form of cartoons, popular music videos or computer games. Tactics employed by websites maintained by terrorist organizations or their affiliates to target minors have included mixing cartoons and children's stories with messages promoting and glorifying acts of terrorism, such as suicide attacks.

These examples along with the recent history of violent conflicts, social stability challenges (challenges of transition and corruption, unemployment inexperience in practicing functional democracies, etc.) and global trends (support for the global war on terror and the effects of global terrorism) have turned the SEE region in a perfect environment for recruitment and radicalization.

Although this trend creates a burden for many countries around the globe, the past history of embedded repressive regimes' approaches in dealing with extremism is a specific issue intrinsic for the SEE Region. The way that a negative image of security services (inherited from former Yugoslav conflicts or authoritarian regimes) enables instigation without proper response is well described by Deliso [61]. He claims that in Kosovo, where a UN administration replaced the Yugoslav rule following the 1999 NATO bombing, the need to placate the province's mafia-connected men of strength manifested acutely in the UN's "don't-rock-the-boat" policy. Kohlmann provides similar support arguing that "the UN and the West knew about this and did nothing", implying that the history of repressive regimes inhibited the legitimacy to act [62].

Cyber forums offer a venue for recruits to learn about, and provide support to, terrorist organizations and to engage in direct initiatives in the propagation of terrorist objectives [63]. Nevertheless, access to these sites is usually restricted. The use of technological barriers to entry to recruitment platforms increases the complexity of tracking terrorism-related activity by SEE intelligence and law enforcement personnel [64]. This is especially important in light of the prevention of online financial transactions.

2.2.3. Are there Examples of Terrorists' use of SEE Cyberspace to Fund Their Activities?

Using Internet to finance terrorist activities is a growing trend. Terrorist organizations or their supporters create websites, chat-groups, or implement mass mailings to request donations from supporters and targeted communications. This is the so-called donation, or direct solicitation method of terrorist financing via the internet. Another way to finance terrorist activities via the internet could be done by using websites as online stores, offering various items for supporters. This method is known as e-commerce financing of terrorist activities. Another way to fund terrorist organizations is by using existing transferring ICT platforms. Electronic wire transfer, credit card, services such as PayPal or Skype, mobile banking or mobile payments are some of the methods that could be used to finance terrorist organizations. Financial support to charities and other organizations is another way to conduct online financing for terrorist organizations. Money laundering has also been identified as a method to fund terrorists' activities via the internet [65].

So far there is no officially processed case of terrorist financing via the internet in the region of SEE. Although there are some indications about online financial support to terrorist organizations, there is no legal case that has been processed in this context [66]. According to Natalia Tereshchenko, the Balkans is suspected of harboring the Hezbollah network, with infrastructure, operational and financial resources readily available for use [67]. Others claim that the SEE cyberspace has been used to support terrorist financing by some charitable organizations. Charitable organizations such as the Benevolence International Foundation, Global Relief Foundation and some others are listed as potential online supporters using the SEE cyberspace in many studies including in the above mentioned UN study. This is not to say that these organizations have not been confirmed as real supporters of terrorist organizations by funding their activities, but that there is no evidence that this has happened via the SEE cyberspace.

One reason for this outcome is the complex legal procedure to prove terrorist financing. One thing is to classify an online activity as illegal, another thing is to prove that this illegal activity is an act of terrorism, or related to terrorist activities. This issue is well known in the legal community which more or less is a result of the general issue of defining terrorism. Euro-Atlantic integration processes have a positive effect on improving the SEE legislation in this context. Nevertheless, even the EU itself faces serious challenges in this direction which affects SEE.

According to some views, the EU is lacking consensus and unity on foreign policy issues. Furthermore, there is an inherent institutional weakness and a lack of resources and manpower. These weaknesses prevent the EU from being able to judge any infringements in the legislation that it should guard. For example, a report issued last year by the Financial Antimony Laundering Task Force FATF, listed several countries with "strategic Anti Money Laundering AML and Counter-terrorism Financing-CFT deficiencies". One of them was Greece [68].

Even though terrorists' use of cyberspace includes planning and training along with committing cybercrime activities, there is no evidence that these types of activities have happened through the SEE cyberspace. Thus the real threat from terrorists' use of Cyberspace to the SEE region comes from the use of the internet and ICT for propaganda, instigation, recruitment, radicalization and communication. Some reports indicate that there are potential online terrorist financing activities, nevertheless so far, this has not been proved. Hence, since there are no SCADA systems, the most threatened information infrastructure in the region of SEE is the internet itself.

3. Conclusion

The process of globalization and the rise of information and telecommunication technology in the region of SEE have brought both positive and negative effects. On one hand, in the age of globalization these processes improve SEE countries prosperity and competitiveness. On the other, these processes have brought significant challenges to security posed by terrorists' use of a cyberspace. Given that modern terrorists (groups and individuals) affiliated with Al Qaeda identified critical infrastructures as their objectives in achieving strategic advantage, the issue of critical information infrastructures protection has become the main concern for NATO and its allies. The complex SEE political environment creates a unique atmosphere for Al Qaeda and its associated movements' operations and objectives' accomplishments. Trends to exploit cyberspace and affect SEE countries' security raise the concerns about SEE CIIP. Despite modernization, efficiency and market competitiveness urge SEE countries to introduce sophisticated SCADA systems and these processes are in development. Thus, debates and concerns about a direct threat to CII in the region of SEE for now are not realistic. However, given that internet itself could be considered as the most vulnerable information infrastructure, other indirect methods of terrorists' use of a cyberspace urge SEE countries to undertake serious measures to identify and assess, mitigate and counter cyber-based threat vectors that AQAM pose to their security.

References

[1] The United Nations Security Council resolution 1368, adopted unanimously on 12 September 2001 Condemned terrorist attack on the USA and stipulates that terrorism represents a threat to peace and security

[2] Reeson, Greg. C, (2011), *Stalemate, why we can't win the War on Terror and What we should do instead,* Government Institute United Kingdom, p.38

[3] Briggs Rachel, (2012), "The Changing Face of Al Qaeda", Institute for Strategic Dialogue, p.3

[4] Zakaria, Fareed, Aug 2013, "Little al-Qaedas Loom Large", Time Magazine, retrieved January 20, 2014 from: http://content.time.com/time/magazine/article/0,9171,2149125,00.html

[5] Spaaij Ramon, (2012), *Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention*, Heidelberg, London, New York: Springer, 2012

[6] The United Nations Office on Drugs and Crime, (2012), *The Use of the Internet for Terrorist Purposes*, The United Nations New York, p.3

[7] Rollins, John, (2011), "Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy", CRS Report R41070

[8] Wemann Gabriel, (2005), "How Modern Terrorism Use Internet", The Journal of International Security Affairs, Spring, Number 8

[9] House of Commons Intelligence and Security Committee, "Report into the London Terrorist Attacks on 7 July 2005", (May 2006) (Para 22)

[10] Sipress, Alan, (December 14, 2004), "An Indonesian's Prison Memoir Takes Holy War into Cyberspace," Washington Post, retrieved from: http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html.

[11] Krebs Brian, (July 6, 2007), "Three Worked the Web to Help Terrorists," The Washington Post, p. D01

[12] Michael Aaronson, Averre Diessen, Yves de Kermabon, Mary Beth Long, and Michael Miklaucic, (2012), "NATO Countering the Hybrid Threat", Prism 2, No 04, p.112-113

[13] Amaruso John, (January 14, 2014), Romania Global Center for Cyber Crime in USA",USA Toaday, retrieved 22.03.2014 from: http://guardianlv.com/2014/01/romania-global-center-for-cybercrime-in-u-s/

[14] Leavitt Lydia, (January 25, 2011), "Cybercrime writer mysteriously disappears in Bulgaria",

[15] ________, (November 20, 2012), "FBI Arrested Young Hacker from Struga" Press 24 retrieved 22.09.2013 from: http://star.press24.mk/story/poznato/foto-fbi-uapsi-mlad-haker-od-struga-sin-na-poznata-struzhanka

[16] ________, (December 13, 2012), "10 arrested in cyber-crime probe", Express UK, retrieved 24.03.2014 from: http://www.express.co.uk/news/world/364435/10-arrested-in-cyber-crime-probe

[17] Dimic Maja, Dobovšek Bojan, (2010), "Perception of Cyber Crime in Slovenia", Journal of Criminal Justice and Security, Year 12. No4, pp 378-396

[18] David Kennedy and John Besant-Jones (March, 2004), "World Bank Framework for Development of Regional Energy Trade in South East Europe", Energy and Mining Sector Board Discussion Paper, No.12

[19] For Croatia see: ICT Zdravko Oklopčić, Boris Brestovec, Dalibor Sever, Boris Njavro, IT solution for gas supply management in open gas market conditions, retrieved 17.04.2014 from: http://www.koncar-ket.hr/docs/koncarketHR/documents/158/1_0/Original.pdf; and Z. Oklopčić, B.Brestovec, D. Sever, B. Njavro, Informatičko rješenje za upravljanje opskrbom plinom kupaca priključenih na plinski distributivni sustav u uvjetima otvorenog tržišta plina, 9. Skup o prirodnom plinu, toplini i vodi, Osijek, 201; for Serbia see: Energy Regulatory Office, (2005), Annual Report for 2004, www/erokso.org, retrieved 20.04.2014 from http://ero-ks.org/Raportet-Vjetore/Srpski/ERO_Annual_Report_for_2004_ser.pdf 1

[20] Organization for Economic Co-operation and Development (OECD), (2009), "OECD Recommendation of the Council on the Protection of Critical Information Infrastructures", OECD, Seoul Korea,

[21] See for example: The EU Commission, (2009), "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions" Brussels, 30.3.2009 COM (2009) 149 final; and The EU Commission (20130, "Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection, Making European Critical Infrastructures more secure", Brussels, 28.8.2013 SWD(2013) 318 final

[22] Dunn Myriam and Wigert Isabelle, (2004), "International CIIP Handbook", Swiss Federal Institute of Technology, p. 18

[23] Ibid.

[24] Symantec, (February, 2003). *Symantec Internet Security Threat Report*, p.48

[25] ISA Expo, October 5, 2004. Retrieved 22.04.2014, from: http://www.controleng.com/single-article/isa-expo-2004-returns-to-houston/5e46593f239cf7ea6c4eb45db7900a12.html

[26] Jennifer Giroux, Peter Burgherr, Laura Melkunaite, (2013) "Research Note on the Energy Infrastructure Attack Database", Perspective on Terrorism, Vol. 7, No.6,

[27] The United Nations, (2004), "Report of the High-level Panel on Threats, Challenges and Change", retrieved from: https://www.un.org/en/peacebuilding/pdf/historical/hlp_more_secure_world.pdf

[28] Dave Clemente, (February 2013), "Cyber Security and Global Interdependence: What Is Critical?", Chatham House, USA

[29] Estonian Information System Authority, Critical Information Infrastructure protection, RIA, retrieved 20.04.2014 from https://www.ria.ee/CIIP/

[30] The United States Government Accountability Office GAO, (March 2013), "Critical Infrastructure Protection", Report To Congressional Request GAO-13-296

[31] Federal Biro For Information Security, retrieved 20.04.2014 from: https://www.bsi.bund.de/cln_093/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html

[32] Chery Steve, (October 10, 2010), "How Stuxnet will rewrite the cyberterrorim playbook", retrieved from: 20.04.2014: http://spectrum.ieee.org/podcast/telecom/security/how-stuxnet-is-rewriting-the-cyberterrorism-playbook

[33] David Geer, (February 12, 2014), "Statistics point to increased physical danger risks of cyberterrorism", CSO Online retrieved 21.04.2014 from: http://www.csoonline.com/article/2134376/malware-cybercrime/statistics-point-to-increased-physical-danger-risks-of-cyberterrorism.html)

[34] Follath Erich and Stark Holger, (November 2, 2009), "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor" Spiegel Online International, retrieved 20.04.2014 from: http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

[35] Bodansky Yossef, *Bin Laden: The Man Who Declared War on America* (New York: Forum, 2001);

[36] Kohlman Evan F, *Al-Qaida's Jihad in Europe: The Afghan-Bosnian Network* (Oxford: Berg, 2004)

[37] Fawaz A. Gerges, *Journey of the Jihadist: Inside Muslim Militancy*, (Harcourt, 2006)

[38] Ibid

[39] Deliso, Christopher, *The coming Balkan Caliphate: The threat of Radical Islam to the Europe and the West*, Praeger Security London, 2007,

[40] Antúnez, Juan Carlos (September 12, 2008 "Wahhabism in Bosnia-Herzegovina", Bosnian Institute, retrieved from: http://www.bosnia.org.uk/news/news_body.cfm?newsid=2468;

[41] The United Nations, (June 26, 2014) "The List established and maintained by the Al-Qaida Sanctions Committee with respect to individuals, groups, undertakings and other entities associated with Al-Qaida" The UN' Al Qaeda sanction list, retrieved July 28, 2014, from: http://www.un.org/sc/committees/1267/pdf/AQList.pdf

[42] Ibid, p.39

[43] Ibid, p. 42

[44] BBC, (June 27, 2010), "One Killed In Central Bosnia Bombing", BBC News, retrieved February 2, from: http://www.bbc.co.uk/news/10428626;

[45] Alic, Anes, (November 01, 2011), *III-Planned terror attack on US Embassy in Sarajevo*, ISA Intel, available at: . http://www.isaintel.com/2011/11/01/ill-planned-terror-attack-on-us-embassy-in-sarajevo/)

[46] Dimitrioska, Pandorce (April 13, 2012), Five murdered at Iron Lake, There no Suspects, (Original: петтмина убиени кај Железарското Езеро, Осомничени нема), Alfa TV, available at: http://www.time.mk/read/85fe05db07/a5bc958d44/index.html

[47] BBC, (July 19, 2012), Bulgaria Blast, Suicide bomber kills Israeli, BBC News, available at: http://www.bbc.co.uk/news/world-europe-18897772

[48] Hadji-Janev, Metodi, (2012) "Managing the consequences of terrorist attacks: The Case of Macedonia", in: Čaleta D. & Shemella P. (Eds.) *Managing the Consequences of Terrorist Acts - Efficiency and Coordination Challenges*, 2012, ISBN: 978-961-92860-5-0, available at: http://www.ics-institut.com/research/books/4

[49] Jackson William, (September 18, 2002), "Cyber Eye: A digital Pearl Harbor might not be so easy", GCN, retrieved 20.01.2014 from http://gcn.com/Articles/2002/09/18/Cyber-Eye-A-digital-Pearl-Harbor-might-not-be-so-easy.aspx

[50] See the following sites for example: Websites such as the "Way of the Believer" (*putvjernika.com*), Way of Islam" (*stazomislama.com*), *Ensarije Serijata* ("Partisans of Sharia" http://www.geocities.ws/ensarije_seriata/index-2.html), and "News of the Community" (*vijestiummeta.com*), and the Sandžak Wahhabi website *kelimetul-haqq.org*

[51] Schwartz, Stephen (January 8, 2010), VOA News Bosnian Service [Washington, DC]

[52] ____, (August 10,) Tha Wahabis from Macedonia has published a song for Bin Laden, Makfaks http://daily.mk/Kajgana/vehabistite_vo_makedonija_izdadoa_pesna_za_bin_laden/346883

[53] Likmeta Besar , (January 24, 2014), "Al Qaeda Using Sical Media to find new Recruits", Global Post, retrieved 22.04.from: http://www.globalpost.com/dispatch/news/regions/europe/140123/albania-isis-al-qaeda-social-media-europe

[54] _____(January 15, 2014), "Albanian Jihadists Recruit Fighters for Syria on Facebook", BalkanInsight, retrieved from: http://www.balkaninsight.com/en/article/albanian-jihadist-use-internet-to-recruit-fighters]

[55] Poggioli Sylvia, (October 25, 2010), "Radical Islam Uses Balkan Poor to Wield Influenece", MPR, retrieved 20.04.2014 from: http://www.npr.org/templates/story/story.php?storyId=130801242

[56] Theohary A. Catherine & Rollins John, (2001), Terrrorist Use of Internet: Information operations in Cyberspace", CRS Report, R41674

[57] Scott Gerwehr and Sarah Daly, "Al-Qaida: terrorist selection and recruitment", in The McGraw-Hill Homeland Security Handbook, David Kamien, ed. (New York, McGraw-Hill, 2006), p. 83

[58] European Commission, Expert Group on Violent Radicalisation, "Radicalisation processes leading to acts of terrorism" (2008), retrieved from www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf

[59] Associated press, (August 31, 2011), Kosovan Albanian admits killing two US airmen in Frankfurt terror attack, retrieved from http://www.theguardian.com/world/2011/aug/31/kosovan-albanian-admits-killing-airmen

[60] About the meaning of *Lex loci*, see more general in: Ehrich Eugene, (1993), "Amo, Amas, Amat and More", Collins Reference p. 170

[61] Deliso, Christopher, (November 14. 2006), *The Black Hole of Europe: Kosovo Interventionists Cover Up their Crimes,*". Retrieved June 29, 2013 from http://antiwar.com/deliso/?articleid=10011

[62] See more in Kohlmann, Evan, (2004), *Al-Qaida's Jihad in Europe - the Afghan - Bosnian Network*, New York

[63] Dorothy E. Denning, "Terror's web: how the Internet is transforming terrorism", in Handbook of Internet Crime, Yvonne Jewkes and Majid Yar, eds. (Cullompton, United Kingdom, Willan Publishing, (2010)), pp. 194-213

[64] Weimann Gabriel (March 5, 2008), "Online terrorists prey on the vulnerable", YaleGlobal Online, retrieved 10.04.2014, from http://yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable

[65] Conway Maura, (2006) “Terrorist ‘use’ of the Internet and fighting back”, Information & Security, vol. 19, pp. 12-14

[66] Republic of Serbia, (March 26 2013) “Report of the Department for prevention of Money laundering Work for 2012, Belgrade, There is one suspicious report for terrorist financing

[67] Tereshchenko Natalia, (March 25, 2013,), “Financing Terrorism: The European Nexus”, Research Institute for European and American Studies, retrieved 23.04.204 from: http://www.rieas.gr/research-areas/editorial/1939-financing-terrorism-the-european-nexus-.html

[68] Financial Antimoney Laundering Task Force FATF, 2012, Follow up Report to the Mutual evaluation Report on Greece, retrived 20.04.2014, from: http://www.fatf-gafi.org/countries/d-i/greece/

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-107

Security of Classified Information as Part of the National Critical Infrastructure Protection: Macedonian Experience

Stojan SLAVESKI [a,1] and Oliver BAKRESKI [b]
[a] *Faculty for Detectives and Criminology, European University – R. Macedonia*
[b] *Institute for Security, Defense and Peace Studies, Sent Cyril and Methodius University*

Abstract. The system of the information protection is part of the national critical infrastructure protection. Handling of classified information is one of the critical infrastructure protection components by which individual segments of the national security system are safeguarded. In organizational terms, crisis management in cyber defense implies engaging the capacities of the relevant state bodies responsible for national security. Their activities are coordinated and guided by organizations of the executive branch and usually by the National Security Authority, as a body responsible for the coordination of the national security activities in the domain of classified information. Protection of the classified information is a crucial part of the overall critical infrastructure protection in Macedonia. The leading governmental agency for classified information protection (including information regarding terrorist activities) that plays a role of the National Security Authority in the international context is the Directorate for the Security of Classified Information. In our paper we will analyze the Macedonian experience in the protection of classified information as part of national critical infrastructure protection.

Keywords. critical infrastructure, critical information infrastructure, classified information protection

Introduction

The functioning of the society in the modern world is based on interrelated national and international information infrastructures. There is a global trend for the integration of communication and information technologies, thus enhancing their efficiency on one hand and their vulnerability on the other. The possibility for failure of system segments entails the danger of interrupting the performances of the system as a whole. The constant increasing of the importance of the information makes the communication and information systems irreplaceable and, at the same time, suitable targets for attack by individuals, groups and states, whose aim is interruption of the normal rhythm of life and society. It is the reason why it is necessary to define a common and comprehensive policy and normative framework for the protection of information and communications.

Information infrastructures are an essential part of the overall infrastructures supporting modern society. These infrastructures and the services they support face increasing security threats. Ever more critical information technologies (IT) resources are supplied and operated in partnership between the public and private sectors and across national borders. In this way, IT and the marketplace for it have become truly global, and thus have security

[1] Corresponding Author: Dr. Stojan Slaveski, Faculty for Detectives and Criminology, European University – R. Macedonia, e-mail: sslaveski@hotmail.com

risks. Unauthorized disclosure, corruption, theft, disruption, or denials of IT resources have the potential to impact the public and private sectors and society as a whole. One of the objectives of every modern society is to promote the development of a culture of security across society. Among all information systems, some are critical because their disruption or destruction would have a serious impact on the health, safety, security, the economic well-being of citizens, or the effective functioning of government or the economy. These information systems constitute the critical information infrastructure (CII) [1].

1. Critical Infrastructure versus Critical Information Infrastructure

Critical infrastructure (CI) and critical information infrastructure protection have been a focus of attention in many countries in recent years. Many developed countries generally define their critical infrastructure in terms of the criticality of particular sectors or services to the safety and security of their society, government and economy. While countries widely use the term "critical infrastructure", the term "critical information infrastructure" is less common in national policies, strategies and structures. However, "critical information infrastructure" has emerged as a somewhat neutral and general term in the international community although no formal attempt has been made to reach a common definition or understanding. The diversity of input across the different countries does not allow us for a single common formal definition. Most countries have formulated a policy and developed good practices to safeguard the information systems and networks that can be considered as critical information infrastructure. However, there are different approaches to the problem [2].

Many factors such as policy, strategy, and the existing structure of authorities and agencies shape the way governments identify their critical information infrastructure and respond to the need to protect it. These factors reflect the priorities, style and culture of the country and government. They set the stage on which the protection of the critical infrastructure policy develops and operates. Likewise, these same factors provide the context for interpreting the existing measures for the protection of the critical information infrastructures and for understanding how different governments respond to the various challenges they face therein [3].

Some countries describe their high-level critical information infrastructure policy and objectives in similar ways. In one way or another, all refer to events that could lead to loss of life, serious or grave impact on the health, safety, security, or economy of their citizens. Differences exist in the language and specific organisational frameworks adopted by each country rather than in the substance. Many countries have developed their critical information infrastructure strategy and policy objectives after identifying their critical infrastructure. Though their individual views of the risk may be different, the development of their strategies and policy objectives follow similar processes. The distribution of government responsibility has a significant influence on critical information infrastructure protection strategy and policy.

International co-operation and collaborative action are imperative to building the relationships needed to increase situational awareness and improve coordinated response to cyber incidents in the global cyber environment. All countries face difficulties in information sharing, particularly of sensitive information, at the international level. In part this might be because of the link between critical information infrastructure, critical infrastructure and national security which could lead to the tendency to protect the majority of all infrastructure information because of the need to protect a minority of sensitive infrastructure information. In this respect, international co-operation between governments on the protection of critical information infrastructure may benefit from adopting a more “open and only selectively closed” security model, as opposed to the traditional “closed and only selectively open” model. This could make infrastructure information sharing easier without compromising sensitive (classified) information.

2. Protection of Classified Information as part of Critical Information Infrastructure

Free access to public information held by state bodies’ means that every person can freely access the information held by persons liable to the law, except when some information is excluded from this rule. One of these exceptions is the information which has been designated as classified according to the law governing classified information.

Categories of information that should be classified are: military plans, weapons systems, operations; foreign government information; intelligence activities, sources, methods, and cryptology; foreign relations & foreign activities on national soil; scientific, technological, and economic matters relating to national security; government programs for safeguarding WMD materials and facilities; vulnerabilities & capabilities of systems, installations, projects & plans relating to national security. Hence, classified information is sensitive information to which access is restricted by law or regulation to particular classes of people that are engaged in the field of national security.

Security is the condition of being protected against danger or loss. With respect to classified matter, security is the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. Protection of classified information is the process of protecting information from unauthorized access, use, disclosure, destruction, modification or disruption. Consequently, Protection of Classified Information (PCI) is part of national critical information infrastructure.

Protection and security of classified information is the single most important obstacle to the sharing of sensitive information. This obstacle can stem from either: technical/infrastructural, legal, functional/operational or political/institutional obstacles as well as from a combination of some or all.

A formal security clearance is required to handle classified documents or access classified information. The clearance process requires a satisfactory background investigation. There are typically several levels of sensitivity, with different clearance requirements. Depending on the level of classification, there are different rules controlling the level of clearance needed to view such information and how it must be stored, transmitted, or destroyed. Additionally, access is restricted on a “need to know” basis. Simply possessing a clearance does not automatically authorize the individual to view all material classified. The individual must present a legitimate “need to know” in addition to the proper level of clearance.

This sort of hierarchical system of secrecy is used by virtually every national government. The act of assigning the level of sensitivity to information is called information classification. The purpose of classification is to protect information from being used to damage or endanger national security. Classification formalizes what constitutes a “national secret” and accords different levels of protection. This is based on the expected damage the information might cause in the wrong hands.

Beside “national secrecy” there are two other forms of secrecy, “political secrecy” and “bureaucratic secrecy”. “Political secrecy” is the deliberate and conscious abuse of classification authority for political advantage, irrespective of any threat to national security, serving to prevent or limit official public discussion of certain aspects or performance, which is dangerous to the political health of the nation. On the other hand, “bureaucratic secrecy” is the tendency of most government bureaucracies to limit the information released to outsiders so as to control perceptions of the organization or agency.

Security classifications indicate the sensitivity of information and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of damage that would occur from unauthorized access or disclosure. There are two main approaches to information classification. Procedures based on lists of classified information, attached to laws or regulations and procedures based on (generic) rules on defining the level of sensitivity of information, written down in law or regulation. Examples of procedures based on lists are: Czech Act on the Protection of Classified Information; Polish Classified Information Protection Act; Bulgarian Classified Information Protection Act and Estonian State Secret Act. On the other site examples of procedures based on “generic” rules are: USA Classified Information Protection Act; EU Council’s Security Regulations; NATO Document C-M (2002) 49 –Security within the North Atlantic Treaty Organization; Slovenian Classified Information Act; Macedonian Law on Classified Information.

There are two main purposes of classification. First, to keep advantages against competitors/enemies. And second, to hide one’s own disadvantages, deficiency, and vulnerability against competitors/enemies. In addition, security classification specifies how people must protect the information and equipment that they handle. The classification system limits access to that information and equipment through a series of procedural and/or physical barriers.

Classification must be correctly applied. Whereas under-classification could lead to potential compromises of sensitive information, over-classification of documents may result in a loss of credibility of the classification system. It also entails significant management costs. Selecting the most appropriate classification is critical because under-classifying can have the direct and obvious consequences of inadequately protected material. On the other hand, over-classifying can mean unnecessary, expensive protection for material and loss of properly classified material among improperly classified material. Over-classifying may stem from: genuine doubt about the classification prescriptions; personal uncertainty; and a tendency to play it safe. For example, the cost of protecting America’s classified information was about $5.6 billion in 1995, including funds paid by industry for security involved with government contracts. The estimate does not include the protection of classified intelligence information, which is itself classified. Indirect costs are difficult to quantify, but often more than direct costs, which increase with level of classification. The cost of declassification must also be considered.

The most effective measure to prevent over-classification is issuing detailed guidance on the correct use of classifications. The higher the classification, the more restrictions this causes to the use of means of communication and the more it complicates dissemination.

Information shall be designated as classified by an authorized person. Authorized persons are elected or appointed officials, authorized to classify and disclose information in accordance with the law or the regulation (presidents, ministers, directors of agencies etc.) and the employees to whom these persons have issued written authorization to classify information.

Confidentiality has been defined by different international organizations. For the International Organization for Standardization (ISO) confidentiality is “ensuring that information is accessible only to those authorized to have access” [4]. While for NATO confidentiality is “the property that information is not made available or disclosed to unauthorized individuals or entities” [5]. The EU Security Regulations foresee that information should be classified only when necessary, and that the level of classification shall be determined by the level of sensitivity of its contents, in accordance with the definitions laid down in the Security Regulations. Appendix 3 to the Council Security Regulations contains a practical guide for the correct classification of documents.

There are certain norms, standards and methods in protection of classified information. They can be divided in four categories: NATO standards [6]; EU norms [7]; ISO norms [8] and national standards.

National norms and standards are usually established by body usually named National Security Authority (NSA). This body is the focal point for NATO and EU security of classified information in each country. It can be an already existing body or it can be established ad hoc. National Security Authority usually has the following tasks: maintenance of security of NATO and EU classified information in national agencies and elements; ensuring that periodic and appropriate security inspections are carried out; ensuring that nationals are appropriately security cleared; ensuring that appropriate national emergency security plans are in place; authorising the establishment (or disestablishment) of national COSMIC Central Registries; responsible for coordinating all matters concerning NATO and EU security policy in their nations; monitoring security policy implementation to ensure a common degree of protection.

Beside this national body responsible for the protection of classified information, every state needs proper legislation to be effective as well. Laws or regulations on classification should define: guidelines for which kinds of information may be classified and how; categories of information which have to be classified and conditions for its release posing a real threat to national security. In addition the Law is expected to regulate how classified information has to be protected, handled, accessed, stored, disseminated, exchanged, transmitted and archived. Also, the issue of declassification should be regulated by the law. Finally who and which agency has responsibility over the process must be regulated by the Law as well.

3. Macedonian Critical Infrastructure Protection

There is no legal document in Macedonia that contains a summarized list of dedicated critical infrastructure. Instead, the network of laws regarding the CIP gravitate over the Crisis Management Center (CMC), Ministry of Interior (MoI), Ministry of Defense (MoD), Ministry of Transport and Communication (MoTC), Ministry of Finance (MoF), Directorate for Security of Classified Information (DSCI) and Directorate for and Protection Rescue (DPR). Since there is no clear dedicated list of critical infrastructure, further legal segmentation follows regarding the anticipated roles and service support for successful CIP. However, all of these documents include acts defining the responsibilities of the government authorities in case of emergencies as well as legislation dealing with issues [9].

International legislation (NATO and EU norms and standards) further facilitates legal background for CIP in Macedonia. This is understandable since cyber-security and information protection are on the security agenda in most of the international organizations to which Macedonia is a party.

Generally, Macedonian legislation for CIP does not centralize responsibility only in one governmental authority. It consists of both provisions that directly locate responsibility and the leading role of specific agency and provisions that imply responsibility. Nevertheless, it could be argued that legal basis for CIP in Macedonia more or less, draws the organizational structure of governmental authorities involved in this process.

3.1. Organizational set up of Classified Information Protection in the Republic of Macedonia

Protection of the classified information is crucial part of the overall CIP in Macedonia. Leading governmental agency for classified information protection is Directorate for Security of Classified Information. MoI's Directorate for Security and Counter-intelligence is in close relation with the DSCI and provide necessary data for successful information protection. As a specific part of the overall security, Ministry of Defense and Intelligence Agency as well play a role in classified information protection. All of the military information protection is run by Military Service for Security and Intelligence. Inside the MoD Army of the Republic of Macedonia (ARM) plans and conducts information protection. Macedonian Intelligence Agency is in close relation with DSCI and Mol's Directorate for Security and Counter-intelligence and thus contributes to the overall classified information protection.

3.2. Regulations on Classified Information before passing the national Law

With the expressed commitment for integration into the Euro-Atlantic structures, the Republic of Macedonia has started taking the necessary steps for coming closer to NATO and EU, which also understood the exchange of classified information. In that direction, the Republic of Macedonia has taken steps for creating the legal basis for the protection of classified information, as a result of which activities have been taken on for the drafting and passing of the Law on Classified Information.

The start of project was in 2002 with the NSA analysis of the "situation" in the field of protection of classified information, made on the request of the Government. Findings were the following: don't have "general" national law on the classification and protection of data which are important or sensitive from the national security point of view; sect oral regulations (internal affairs, defense) are based on the old and inadequate Yugoslavian approach to the protection of classified information; some very important institutions are without any written rules on the protection of classified information. The overall situation is far away from the standards of the state which intends to be member of the EU and NATO.

Hence, there were very evident reasons that point at the necessity for a comprehensive legal framework of the issues concerning the classified information that had been mostly regulated by bylaws. The number of laws regulating separate issues on the creation, protection, storing, use and punitive actions concerning their violation are partially contained in a great number of acts. Furthermore, a number of bylaws treat the same issue differently, particularly with regards to the punitive actions. That was due partly to the fact that these acts have been passed in longer time intervals and they have reflected the actual society situation on this very sensitive plan of our positive legislation. To illustrate, we will mention that the issue on confidential information is basically encompassed with: 16 laws, 3 decrees and about ten regulation books, manuals and decisions.

This issue is particularly regulated in the Decree on criteria and measures for protection of the secrecy of the defense related data [10], the Regulation Book on criteria for determining the secret data related to the Army of the Republic of Macedonia that must be kept secret and the measures for their protection [11] and the Regulation Book for the keeping and protection of documents, reports, data and other acts at the Ministry of Interior that are classified as top secret, military secret or restricted by law, another regulation or the decision of a relevant body [12].

Besides the security agreement between the Republic of Macedonia and NATO from 1997, there were other international agreements that obliged RM to regulate this issue thoroughly. Many issues of common interest concerning the exchange of confidential information and data have been stipulated in details in a number of later agreements between the relevant authorities of the Republic of Macedonia and NATO.

The Agreement between the North Atlantic member countries and the other Partner countries on the status of their forces with the Additional Protocol was signed on May 30, 1996 with which the Basic Agreement among the NATO parties on the status of their forces dated June 19, 1951 (SOFA) was accepted. The Assembly of the Republic of Macedonia ratified the Agreement on June 4, 1996. Here I would particularly like to emphasize that with the signing of this Agreement, and in line with the Basic Agreement (article 7, item 2, line (c) [13], RM adopted a provision in its national legislation that the violation of any law concerning the official secrets of any signatory country, or its national defense related secrets, represents an offence against the signatory country.

By ratifying the Agreement on Stabilization and Association between the Republic of Macedonia and the European communities and its member countries, signed on April 12, 2001, RM was obligated to pass a Law on Protection of Data (article 68, paragraph 3 of the Agreement) [14] during the first stage in the preparation process for full-fledged membership in the European Union. According to the Protocol 5 of the Agreement, which regulates issues of common interest in the customs services, it is also necessary to regulate the issue on the exchange of classified information, as one of the key issues for cooperation in this sphere. This Protocol regulates many basic rules concerning the exchange of classified information depending on the regulation that are in force in each of the signatory parties. Furthermore, the need is pointed out for putting this sensitive area in a legal framework and for making appropriate adjustments of the existing laws in the European community and the member countries. Such treatment of the issues is identical for the other areas where the exchange of classified information is being accomplished, having in consideration the specifics of each area separately.

The Declaration for raising the level of the relations between the Republic of Macedonia and the European Union, which the Assembly of the Republic of Macedonia issued on November 23, 2000, and in order to support the commitment of the Government for initialing and signing the Agreement for Stabilization and Association with the European Community, which was considered to be an important step toward our full-fledged membership in the Union, also stipulates the following: “Within its constitutional responsibilities, the Assembly of the Republic of Macedonia will give full contribution to the fulfilling of the commitments stemming from this Agreement and will shape and synchronize the harmonization process of the Macedonian legislation with the legislation of the European Union on transparent basis. Thus, constant and mutual informing between the Government and the Assembly of the Republic of Macedonia is necessary.” [15]

Due to the mentioned reasons, at its session on March 31, 2003, the Government of the Republic of Macedonia issued a conclusion with which it adopted the suggestion of the NSA to establish an inter-ministerial working group that will draft the law on classified information. The National Security Authority was designated to be the coordinator for the activities. The Assembly of the Republic of Macedonia passed the Law on classified information in February 2004. The Law fully considers the established standards on the protection of classified information within NATO and the EU.

3.3. Law on Classified Information

The Law on Classified Information [16] entered into force on March 5, 2004, thus enabling the former NSA to grow into the Directorate for Security of Classified Information as a standalone body of the state administration with the capacity of a legal entity. In line with the Law, the Decree on Administrative Security of Classified Information, the Decree on Physical Security of Classified Information and the Decree on Personnel Security were passed in November 2004, while the Decree on Industrial Security of Classified Information and the Decree on Information Security of Classified Information were passed in March 2005. Also, other internal legal acts have been passed in relation to the protection of classified information in line with NATO/EU security standards.

In September 2007 the Law on Amendments and Supplements to the Law on Classified Information [17] was passed. It ensured full control not only over the foreign, but over the national classified information as well. Furthermore, it ensured inspection supervision over all state organs and other natural bodies and legal entities for the strict implementation of the Law on Classified Information.

According to the Law there are four types of classification: state secret (highest), strictly confidential, confidential and internal. When it comes to the process of classification the current law prescribes that the highest classified information – state secret can be classified by the highest state officials (President, Prime Minister, President of Assembly, Ministers etc.). The over-classification of data exists especially when it comes to the lowest level of classification (internal) so that the public cannot have access. This may be partly because of the lack of security culture or the lack of knowledge of the law. However, the person that classifies certain documents according to the Law should explain the reason behind the classification and the interests that would be threatened if that information is open.

Vetting is required for those that want to handle classified information. The procedures entitles that the Directorate for Security and Counter-intelligence and the Military Service for Security and Intelligence to perform a background check of the applicant for a security clearance on behalf of the Directorate for the Protection of Classified Information. This set up shows some downsides especially where the

Counterintelligence department has the main say in whether the person is eligible for handling classified information or not, a process that could sometimes be misused [18]. According to the Law, there is a safeguard mechanism. The Director of the Directorate for Classified Information has authority over the Directorate for Security and Counterintelligence and the Military Service when it comes to checking whether the rejection or approval of someone's security clearance has been done thoroughly and highly professionally so that there is no ground for possible doubts.

Not every level of classification requires a thorough check up. According to Art.44 security clearance is not required for information/documents which are classified as Restricted. In addition, the high state officials such as the President, Prime Minister, Vice Prime Minister, President of the Assembly, President of the Constitutional Court and the president of the Supreme Court do not require prior vetting, something which, for example, some MPs raised in couple of occasions. All state institutions are required to deliver the systematization of their workplaces in which they should clearly identify what kind of certificate is needed for what position.

Many controversies have arisen about the vetting process, especially among the members of parliament who are members of the Committee for supervision of the work of the Directorate for Security and Counter-intelligence and the Intelligence Agency, as well as the one following the telecommunication interception techniques. Knowing that the Directorate for Security and Counter-intelligence conducts the necessary check-ups, the opposition party members have expressed doubts whether the lack of timely delivery of the security clearances or lack thereof might be due to political rivalry [19]. The issue has been temporarily solved by providing the members of the committees with temporary clearances however there is the need for an amendment in the Law in order to overcome this lack in the provisions of the Law.

Ten years of experience in the implementation of the Law on classified information shows that there is still lack in the security culture of the state officials. Concerns have risen amid the disclosure of a classified document by the former President Branko Crvenkovski on a TV debate revealing proposals by the UN special envoy regarding the name dispute between Macedonia and Greece [20]. The public prosecutor's office revealed that it was considered to be a highly confidential document. A national daily newspaper investigated whether the document was in the archives of documents at the (current) President's Office, which turned out not to be the case [21]. This has raised questions as to whether some officials have "private" collections of classified information.

3.4. Directorate for Security of Classified Information as National Security Authority of the RM

The protection and security of information are issues of great importance for the future membership of the Republic of Macedonia to NATO and the EU. For, example, one of the five chapters in the Membership Action Plan – MAP, endorsed in 1999, in Washington, D.C., is dedicated to security of information. Article 4 of the Security Agreement signed between the Republic of Macedonia and NATO on January 17, 1996 that entered into force on January 19, 1996, determined the commitment of the Government of the Republic of Macedonia to inform the NATO Office of Security that a National Security Authority has been established that would be responsible for protection and security of the information exchanged between the Republic of Macedonia and NATO throughout the nation.

At the beginning of this activity it was the Service for Reciprocal Security at the Ministry of Defense that accomplished this task. However, this sensitive issue needs to be treated at the national level. The Government of the Republic of Macedonia made a step forward to full accomplishment of the commitment stipulated in the article 4 of the mentioned security agreement, by issuing a decree on March 19, 2002 to establish the National Security Authority of the Republic of Macedonia in NATO Context as an expert service of the Government to execute the rights, responsibilities and powers stemming from laws and agreements concluded between the Republic of Macedonia and NATO, concerning NATO classified information and documents. By establishing the National Security Authority, the Republic of Macedonia has ensured the reciprocal exchange of NATO classified information to be protected and ensured at the highest level. Namely, contrary to the former established Service for Reciprocal Security at the MoD, which was tasked with the security and protection only of information exchanged on reciprocal basis among the ministries of defense, foreign affairs and interior and which was directly subordinated to the Minister of Defense, the National Security Authority has much wider responsibilities and powers. It is the responsibility of the NSA to ensure secure reciprocal exchange according to NATO standards of all NATO classified information that arrives from and is sent to all state organs, including their reception, recording, distribution, delivery and storing. For its work, the National Security Authority is immediately reporting to the Government of the Republic of Macedonia, that is, the Director of this institution reports to the President of the Government of the Republic of Macedonia.

The level of responsibility of the NSA for the application of NATO and EU standards for administrative security, personal security, physical security, information security and industrial security, determines its organization and scope of work. According to the scope of operation of the Directorate for Security of Classified Information established with the Law on Classified Information [22] and in line with the Decree on the Guidelines for Internal Organization of the Organs of the State Administration [23], organizational units have been established in the Directorate.

In organizational units of DSCI tasks are accomplished in the field of: the administrative security of classified information, the physical security of classified information, the personnel security of classified information, the industrial security of classified information and the information security of classified information, as well as in the field of the general, normative and legal issues and the international cooperation. Additional organizational units have been established in the Directorate in line with the positive legal acts on the organization and the work of the organs of the state administration which ask for this kind of positioning. In these organizational units, led by heads who directly report to the official heading the state organ, works and tasks are accomplished in the field of the financial issues and human resources.

According to the Law on Classified Information the Directorate for Security of Classified Information has been founded with the purpose to implement the established policy for protection of classified information and the international standards, to carry out the exchange of classified information in line with the international agreements, to exercise inspection supervision of the implementation of the provisions of the Law on Classified Information and of the other regulation concerning classified information, as well as to accomplish other tasks regulated by the Law [24].

As a result, in general, the legal competencies of the Directorate can be divided into three groups. The first group of competencies has an internal dimension that refers to the application of the international standards and norms in the exchange of classified information at the national level, including the appropriate protection of the received information. The second group competencies has an external dimension that refer to the exercising of control on the way in which the classified information that the Republic of Macedonia has released to foreign states and international organizations as safeguarded and protected, as well as the competencies that refer to the participation of the Republic of Macedonia in the Euro-Atlantic structures and the initiation of the international agreements. And the last group of competencies refers to the development of emergency plans for protection of classified information, as well as to the training of the users of classified information through organizing workshops, seminars and individual consultations.

More specifically, the Directorate has the following competencies: ensures continuous application of the international standards and norms while taking on the measures and activities for protection of the classified information; coordinates the activities for ensuring protection of the classified information with the state bodies and the institutions that exchange classified information with foreign states and international organizations; prepares, organizes, applies and monitors the application of the measures and activities for ensuring protection of classified information that has been released to the Republic of Macedonia by foreign states and international organizations; takes on activities for protection of the classified information that the Republic of Macedonia has released to foreign states and international organizations; participates in the process of developing plans and programs of the Republic of Macedonia for membership in international organizations related to the protection of classified information; plans and accomplishes international cooperation for protection and exchange of classified information; recommends measures for enhancing the protection of classified information; initiates entering into international agreements with foreign states and international organizations related to the exchange of classified information; initiates developing of emergency security plans for protection of classified information; educates the users of classified information and the interested bodies, organizations and individuals in the Republic of Macedonia; exercises inspection supervision of the implementation of the provisions of the Law.

By passing of the Law on Amendments and Supplements to the Law on Classified Information and by expanding the competencies of the Directorate for Security of Classified Information in the area of the inspection supervision of the national classified information, as of September 2009, the directorate: exercises inspection supervision of the implementation of the provisions of the Law on Classified Information and of the other regulation concerning classified information during the handling of the national and the foreign classified information in the country through authorized inspectors of the Directorate and leads offence proceedings and brings decisions on offences committed against the national regulations concerning the security of the national classified information and of the foreign classified information exchanged on bilateral basis with other states or international organizations (NATO and the EU) through the Commission for Deciding on Offences established at the Directorate.

Beside the Directorate for the Security of Classified Information, all of the security sector institutions have designated staff that takes care of classified information protection. This staff together with the Directorate represents the operational framework for activities under the auspices of classified information protection in the country.

Regarding the functioning of Directorate, the need for an increase of staff in the national registers and the IT sector and increase in budgetary support of the Directorate should be emphasized. It is evident that there has been a decline in the budget provided to the Directorate by the Government especially compared to 2009 in total as well as when it comes to professional development. In particular the Directorate faces problems with INFOSEC: providing accredited equipment, lack of experience in that field (particularly in the field of zoning), lack of INFOSEC awareness at the national institutions, etc. [25].

4. Conclusion

There is no legal document in Macedonia that contains a summarized list of national critical infrastructure protection. Macedonian legislation for CIP does not centralize responsibility only in one governmental authority. It consists of both, provisions that directly locate responsibility and the leading role of specific agency and provisions that imply responsibility. The protection of the classified information is a crucial part of the overall CIP in Macedonia. National critical infrastructure in the field of classified information is established by passing the Law on Classified Information and establishing the Directorate for Security of Classified Information that plays a role of National Security Authority in the international context. The Law on Classified Information, adopted in 2004 establishes a comprehensive structure for protection and management of classified information. The Law on Classified Information not only united the existing laws and bylaws for protection of classified information, but it also represented a new quality of their protection. Moreover, contemporary resolutions for the security of all information (national and foreign), adjusted to NATO and EU norms, criteria and standards are envisaged. The Law regulated such protection to be controlled throughout the Republic of Macedonia by one state organ with a higher status, Directorate for Security of Classified Information. The achieving of the required standards in the field of classified information does not mean an automatic membership of the Republic of Macedonia to NATO and the EU, but a removal of the obstacle for membership. On the other hand, it also means opening of the doors for more intensive communication and the exchange of classified information not only with NATO and the EU, but with other international organizations and states as well, which will be of great benefit for the state.

References

[1] Philip Auerswald, Lewis M. Branscomb, Todd M LA Porte, Erwann Michel-Kerjan, “The Challenge of Protecting Critical Infrastructure”, *Issues in Science and Technology*, Fall 2005.

[2] “Physical Protection of Critical infrastructures and Key Assets”, *Military Technology*, April 2005, pp. 32-37.

[3] Mike Kataoka, *GIS for Homeland Security*, ESRI Press, 2007.

[4] Information Security Management System (ISMS) according to ISO 27001:2006(BS-7799-2).

[5] C-M (2002) 49 Security within the North Atlantic Treaty Organization.

[6] In NATO basic document is C-M (2002) 49 Security within the North Atlantic Treaty Organization (NATO). The following Directives support document C-M(2002)49: AC/35-D/2000 Directive on Personnel Security; AC/35-D/2001 Directive on Physical Security; AC/35-D/2002 Directive on Security of Information; AC/35-D/2003 Directive on Industrial Security ; AC/35-D/2004 Primary Directive on INFOSEC and AC/35-D/2005 INFOSEC Management Directive for GIS.

[7] Council's Security Regulations, set out in decision 2001/264/EC, lay down the basic principles and minimum standards of security to be respected in an appropriate manner by the Council, by the General Secretariat of the Council, by the Member States and by the decentralized agencies of the European Union, so that security is safeguarded and each may be assured that a common standard of protection is established. Council's Security Regulations are following: Basic principles and minimum standards of security; Basic principles; Organization of security; Security of personnel; Physical security; Security of information (INFOSEC); Counter-sabotage and other forms of malicious willful damage and Release of classified information to third states or international organizations.

[8] ISO standards and information security are: Information Security Management System (ISMS) according to ISO 27001:2006(BS-7799-2) and CRAMM Method.

[9] Metodi Hadji Janev and Stojan Slaveski, "Corporate Security and Critical Infrastructure Protection in the Republic of Macedonia", *Security Dialogs no. 4*, 2012.

[10] Official Gazette of the RM, no. 36/94.

[11] Official Gazette of the RM, no. 43/94.

[12] Official Gazette of the RM, no. 48/95.

[13] Item 11 of the same article includes the following commitment: "Each signatory country will tend towards such legislation as deemed necessary to ensure appropriate security and protection of the installations, equipment, property, register and classified information belonging to other signatory countries within its territory, and to ensure punishing of the persons that have violated the relevant laws."

[14] Official Gazette of the RM, no. 28/01.

[15] Official Gazette of the RM, no. 99/00.

[16] Official Gazette of the RM, no. 9/04.

[17] Official Gazette of the RM, no. 113/07.

[18] Stojan Slaveski, Законско уредување на тајните информации [Legal regulation of secret information], Nova Makedonija, 26.03.2012, available at: http://www.novamakedonija.com.mk/NewsDetal.asp?vest

[19] Тајните служби го владеат парламентот [Secret services rule Parliament], Vest, 18.10. 2010, available at http://www.vest.com.mk/?ItemID=8C12D57DEDDEB54BA13FB80AFC225CEA

[20] Црвенковски не издал државна тајна, вели Шврговски [Crvenkovski did not reveal state secret, Shvrgovski says], Utrinski Vesnik, 05.06.2012, available at: http://www.utrinski.com.mk/default.asp?

[21] Приватните архиви полни со државни тајни [Private archives full with state secrets], Dnevnik, 30.05.2012, available at: http://daily.mk/forward/1320778/privatnite-arhivi-polni-so-drzhavni-tajni

[22] Official Gazette of the RM, no. 9/2004, 113/2007 and 145/2010.

[23] Official Gazette of the RM, no. 105/2007, 146/2007 and 149/2011.

[24] Stojan Slaveski, "Законско уредување на тајните информации", *Nova Makedonija*, 26.03.2012, available at: http://www.novamakedonija.com.mk/NewsDetal.asp?vest=325122033117&id=13&prilog=0&setIzdanie

[25] Andreja Bogdanovski and Cveta Konevska, *Transparency of the Security Sector in Macedonia*, Analytica Think Thank, Skopje, 2012, pp. 26-34.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015

© 2015 The authors and IOS Press. All rights reserved.

doi:10.3233/978-1-61499-478-7-120

Security Vetting in Relation to the Critical Infrastructure

Milan TARMAN[1]
Government Office for the Protection of Classified Information
NSA Slovenia, Ljubljana, Slovenia

Abstract. The aim of the present paper is to introduce a case study and the best practice of security vetting in relation to the critical infrastructure and in specific to nuclear security. In Slovenia the Nuclear Power Plant in Krško (the NEK) is an important part of the energy sector and the environmental safety sector of the state's critical infrastructure. The NEK is also an important source of electricity for Croatia - in that respect the plant produces and supplies electricity for both Slovenia and Croatia, each of which has the right and obligation to use 50 percent of its total output. The structure of the management board and personnel is based on the parity principle, considering the equal business shares of both partners. When there is a need for a security check of foreign citizens working in the facilities, public-Private, inter-ministerial and international cooperation is needed. The best practice presented in this paper of a comprehensive approach to cooperation regarding legislation and implementation similar to the security vetting of foreign citizens relating to nuclear security can also be used in other sectors of the critical infrastructure. It also represents an example of best practice for the risk management of potential internal threats connected with terrorist threats to the normal functioning of the critical infrastructure.

Keywords. critical infrastructure security, nuclear security, security vetting, cooperation

Introduction

In our modern society of risks and threats, security needs an increasing amount of attention and a systematic approach also in the field of the protection of the critical infrastructure. This does not just involve the adoption of measures, legislation and regulations but also and above all, their successful implementation in practice –public-private, inter-ministerial and international cooperation in this view is necessity.

Slovenia is aware of the opportunities that come out of productive international cooperation. During the activities of security vetting in relation to the critical infrastructure, we have additionally strengthened our efforts regarding the implementation of international security standards, including those related to classified information.

Since our accession to NATO and the EU, interoperability and compliance with NATO and EU security standards have become leading principles – and along the line international, regional and bilateral cooperation are vital for the successful implementation of them.

International cooperation, education, the exchange of best practices and related research events are contributing significantly to the exchange of information, know-how

[1] Corresponding Author: MSc. Milan Tarman, Government Office for the Protection of Classified Information NSA Slovenia, 1000 Ljubljana, Slovenia, e-mail: Milan.Tarman@gov.si

and mutual understanding as well as to the fulfilment of the key task of this cooperation - namely providing the highest possible level of protection to the critical infrastructure.

The Government of the Republic of Slovenia has already adopted the decision on defining the state critical infrastructure in which the sectors of the critical infrastructure are defined on the basis of the opinion of the Inter-ministerial Coordination Group for the coordination of the preparedness for the protection of the state's critical infrastructure. The same expert group is further tasked by the government of the Republic of Slovenia to prepare a draft proposal for the Critical Infrastructure Act by the end of 2015 at the latest.

The tasks of the National Security Authority (NSA) in the Republic of Slovenia are carried out by the UVTP – The Government Office for the Protection of Classified Information. The Slovenian NSA cooperates in its activities with the relevant authorities of different sectors of the critical infrastructure with regard to the legislation and implementation of regulations such as the Ionising Radiation Protection and Nuclear Safety Act, the Aviation Act and the Electronic Communications Act.

Among other obligations, the Slovenian NSA shall also ensure the implementation of international treaties, the international commitments and obligations undertaken, concluded or adopted by the Republic of Slovenia with reference to the handling and protection of classified information, and shall cooperate in this area with the relevant authorities of foreign countries and international organisations, unless otherwise provided by the international treaty in question. This also includes security vetting procedures and assistance in carrying out security clearance procedures. Namely, upon request NSAs shall also assist each other in carrying out security clearance procedures and the parties of international treaties shall mutually recognise their personnel and facility security clearances. This comes into effect when there is a need for the security check of personnel working in facilities of the critical infrastructure - when there is the need for the security vetting of foreign citizens.

In this paper I would like to present a case study and the best practices of security vetting in relation to nuclear security. Safe operation is namely the most important priority task of every nuclear power plant.

In Slovenia the Nuclear Power Plant in Krško (the NEK) is an important part of the energy sector and the environmental safety sector of the state's critical infrastructure. It provides approximately 40 percent of the total electricity produced in Slovenia. It is also important to pay special attention to environmental protection - to practise environmental safety in all plant processes and management. The NEK is also an important source of electricity for Croatia. The NEK in that respect produces and supplies electricity exclusively in favor of the two partners (Slovenia and Croatia), who each have the right and obligation to use 50 percent of its total output. The structure of the management board and personnel is based on the parity principle considering equal business shares of both partners. The management board, which in principle makes decisions by a consensus, consists of two members – the president is nominated by the Slovenian partner and the member by the Croatian partner [1].

Out of the need for the comprehensive security vetting of foreign citizens - employees at the NEK, the relevant approach to public-private, inter-ministerial and international cooperation regarding legislation and implementation has been analysed. The outcome was updated legislation and the application of the best practice in risk management in relation to the potential internal threat connected with terrorist threats to the normal functioning of critical infrastructure.

1. Personnel Security and Security Vetting – The Classified Information Act

The Slovenian NSA is the responsible authority for the preparation and drafting of the Classified Information Act and related legislation regarding the protection of classified information [2] as well as for coordinating the relevant authorities for ensuring their implementation.

1.1. Personnel security - Basic security

Personnel security with regard to the protection of classified information means that every person who requires access to classified information in order to discharge his/her tasks or functions must undergo a personnel security clearance procedure. The personnel security clearance procedure is used to determine the loyalty, dependability and authenticity of the person concerned for the purposes of delivering or extending personnel security clearance. During the personnel security clearance procedure, any circumstances and aspects of the person's character which might result in potential security problems are considered.

LEVELS OF VETTING PROCEDURE:

- basic vetting procedure – CONFIDENTIAL
- extended vetting procedure – SECRET
- extended vetting procedure with security inquiry – TOP SECRET

LEVEL OF VETTING PROCEDURE – CONFIDENTIAL data:

- name, including any previous names
- personal identification number
- date and place of birth
- nationality or nationalities, including any previous nationalities
- place of residence (permanent, temporary and actual)
- stays abroad, if lasting 3 months or longer (place, period and reason for the stay abroad)
- marital status and number of children
- occupation and job performed
- military service
- study and participation in seminars or other forms of training and education abroad, if lasting 3 months or longer (place and period)
- employers (present and past) and their addresses
- unerased final convictions for criminal offences prosecuted ex officio, and data on offences dealt with by violation authorities or courts
- ongoing criminal proceedings
- alcohol, drug or other addiction
- disease or mental disturbance that might threaten the safe treatment of classified information
- contacts with foreign intelligence and security services
- membership or participation in organizations or groups which threaten the vital interests of the Republic of Slovenia (RS) or member states of political, defence or security alliances of which the RS is a member

- pronounced disciplinary measures
- previous vetting procedures

1.2. The security clearance process to access national classified information

Any person required to have knowledge of relevant classified information in the performance of his/her work must be security cleared prior to obtaining access to classified information. Personnel security clearance is an inquiry carried out by a competent authority prior to issuing permission to access classified information; its aim is to gather data on any possible security restrictions regarding access to classified information. The procedure for obtaining personnel security clearance complies with the provisions of the Classified Information Act and with the decree on the vetting and issuing of personnel security clearances.

The personnel security clearance procedure is initiated on the written proposal of the proposer (either the head of the authority or a person authorised by the head) and must contain the name and date of birth of the person to be vetted and the level of classification allocated for the proposal to issue a security clearance certificate. The proposer referred to is required to inform a person of the reasons for the following: of the scope, of the contents and procedures, and call upon this person to consent in writing. When a person subject to security clearance provides his/her written consent to commence personnel security clearance (and declares in writing that he/she has knowledge of the regulations on classified information), the proposer forwards him/her the relevant personnel security clearance questionnaires. The person subject to security clearance returns the completed personnel security clearance questionnaires to the proposer in a sealed envelope.

If the person subject to security clearance does not give consent to the commencement of the personnel security clearance procedure, personnel security clearance shall not be carried out.

The written proposal, the signed consent, the evidence of basic training (this may not be older than a year) and the envelope containing the completed personnel security clearance questionnaires are submitted by the proposer to the authority competent for vetting and issuing personnel security clearance. Where no security restrictions are established during the personnel security clearance procedure, the person subject to security clearance will be delivered a personnel security clearance certificate granting him/her access to national classified information.

Personnel security clearance in Slovenia is carried out by the authorities defined by law. These are as follows:

- The Ministry of the Interior (MNZ); it carries out personnel security clearance for the persons employed in this ministry and for persons employed in other bodies and organisations of the Republic of Slovenia (with the exception of the Ministry of Defence and the Slovenian Intelligence and Security Agency (SOVA)), where their work does not involve the performance of defence duties or military service.
- The Ministry of Defence – Intelligence and Security Service (MO OVS); it carries out personnel security clearance for the persons employed in this ministry and for persons involved in the performance of defence duties or military service.
- The Slovenian Intelligence and Security Agency (SOVA); it carries out personnel security clearance for its own employees.

When the above-mentioned activities include Security vetting procedures and assistance in carrying out security clearance procedures based on international treaties and the international commitments and obligations undertaken, concluded or adopted by the Republic of Slovenia, the Slovenian NSA shall ensure their implementation. Namely, upon request NSAs shall assist each other in carrying out security clearance procedures and the parties to international treaties shall mutually recognise their personnel and facility security clearances [3]. This comes into effect when there is a need for a security check on personnel working in the facilities of the critical infrastructure - when that involves the security vetting of foreign citizens.

2. Nuclear Security – The Ionising Radiation Protection and Nuclear Safety Act

The Ministry of Agriculture and the Environment and especially the Slovenian Nuclear Safety Administration (SNSA) within the Ministry is the responsible authority for the preparation and drafting of the Ionising Radiation Protection and Nuclear Safety Act and related legislation as well as for coordinating the relevant authorities for ensuring their implementation [4].

2.1. Nuclear security – definition and activities

According to the IAEA, Glossary [5], nuclear security is defined as the prevention and detection of, and response to theft, sabotage, unauthorised access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.

Nuclear security – activities:

- nuclear and radiation safety of nuclear facilities;
- circulation, transport and management with nuclear and radioactive materials;
- control and material balance of nuclear material;
- physical protection of nuclear materials and nuclear facilities;
- responsibilities for nuclear detriment;
- staff qualifications at nuclear facilities and their education with appropriate quality assurance;
- assurance of radiological monitoring;
- early notification in case of nuclear and radiological emergencies;
- international cooperation in the work areas of the administration.

In the future, the energy sector will be heavily stricken, namely regarding the implementation of new projects, financing problems, clashes of interest and more and more numerous security threats [6]. Furthermore, according to Prezelj, [7] electrical power supply problems would have immediate effects because of the dependence of a majority of society's activities. The same goes for nuclear energy as an important part of the Energy Sector and the Environmental Safety Sector of the Slovenian state's critical infrastructure.

According to Radović and Trivan [8], it is proven that in the global community the link between the environment and security has grown. Therefore, ecological security starts to be an issue of paramount interest of the security services and of the intelligence community.

2.2. Nuclear security – internal threat

When discussing nuclear security, considering potential internal threats is a necessary element in providing the proper safety of nuclear facilities. Based on the IAEA approach, the following characteristics are typical for the insider as a subject of internal threats:

- Motivation: Ideological, Financial, Personal (revenge, ego), Psychotic,
- Coercion
- Attributes: Access, Authority, Knowledge, Technical skills and
- Experience
- Tactics: Stealth, Deception

When there is an opportunity added to certain of the above characteristics, an insider attempt to threaten nuclear security is possible.

According to Čaleta [9], the critical infrastructure is not only threatened by international terrorism, but there are also other direct threats to it such as natural and man-made disasters and other deviant acts intentionally performed by external or internal bodies in the process of its functioning. A potential source of an internal threat is all employees who can cause damage to the assets and interests of the company in a conscious or unconscious way with sabotage, theft, fraud, deception or another shape of negative behaviour [10].

The critical infrastructure's security therefore cannot be discussed without considering potential internal threats and relevant preventative measures for ensuring security.

2.3. Nuclear security – security screening of persons considered for employment

The security screening of persons considered for employment according to the valid Ionising Radiation Protection and Nuclear Safety Act regarding foreign citizens (in the case of NEK employees) is defined as: If the worker's employer or employee is not a citizen of the Republic of Slovenia, the authenticity of the data shall be proved by a certificate of impunity under the regulations of the state (the parent nation) the worker is a citizen of. That means that in the case of NEK employees who are foreign citizens, there is a rather complicated and incomplete system of gathering all the necessary documents proving their impunity. Namely, the relevant authorities in Slovenia can only check their official records regarding certain personal data and related events in Slovenia.

From the above described procedures an initiative was made to improve the security screening of persons considered for employment. Consequently several inter-ministerial meetings were proposed to approach the issue.

3. Inter-ministerial Cooperation

The Slovenian NSA is in charge of and is proactively participating in various forms of inter-ministerial cooperation within the framework of the following bodies regularly: the Commission for IT Security; the Commission for Assessing the Legitimacy of the Prevailing Public Interest in the Disclosure of Secret Classified Information; the Inter-Ministerial Working Group for Industrial Security; the Inter-Ministerial Working Group for Personnel Security; the Inter-Ministerial Working Group for Documentation Security; the Inter-Ministerial Expert Working Group for Communication Security; and the Inter-Ministerial Expert Working Group for Unintentional Compromising Emanations.

Nuclear security – the security screening of persons considered for employment was discussed at ad-hoc meetings involving representatives and opinions of the Ministry of the Interior, the SNSA, the NSA, the NEK, the Ministry of Defence and the Slovenian Intelligence and Security Agency. In the discussion previous experiences and good practices were presented, especially based on the results of the Inter-ministerial working group for personnel security and past activities when the NSA cooperated with the relevant authorities of different sectors of the critical infrastructure on the legislation and implementation of the Aviation Act, the Electronic Communications Act and others.

According to Radović [11], a careful planning and balancing of security measures with risk reduction measures is necessary. That is another function of the Inter-ministerial working group for personnel security, which was appointed by the NSA director and has been active in the field of personnel security since 2009. Apart from the NSA‘s representatives, the group is composed of representatives of the Ministry of the Interior, the Ministry of Defence and of the Slovenian Intelligence and Security Agency. The basic tasks of the Inter-ministerial working group are to find solutions to open issues, adopt guidelines in the field of personnel security, and draft proposals for amendments to regulations on the handling and protection of classified information, including personnel security.

The relevant activities are carried out in compliance with the resolution on the National Security Strategy of the Republic of Slovenia, the guidelines and action plan relating to Slovenia‘s policies in the Western Balkans, and other strategic documents and rules. The NSA carried out all the internal legal procedures required in order to adopt, sign and ratify several bilateral agreements on the exchange and mutual protection of classified information (with the focus on South Eastern European States). In addition, the agreements yet to be concluded with several other countries are in various phases of the adoption process. As an appropriate legal basis, bilateral agreements facilitate cooperation between state authorities and economic entities, and strengthen mutual trust.

4. Security Vetting in Relation to Nuclear Security

According to the findings of the Inter-ministerial meetings at the expert level of the Ministry of the Interior, the SNSA, the Ministry of Defence and of the Slovenian Intelligence and Security Agency and the NSA, suggestions were made that in the definitions of the terms in the Ionising Radiation Protection and Nuclear Safety Act the following terms should be entered:

- “Security check” is a person’s query before issuing a permit to enter in the controlled facility or space, physically controlled facility or space and vital facility or space of the nuclear facility, realised by the employer and the operator of a nuclear facility and whose purpose is to collect information about potential security restrictions;
- “Security restrictions” are findings of the security vetting procedure, which indicate that there are doubts about the reliability and loyalty of a person to be granted permission to enter the controlled facility or space, physically controlled

facility or space and vital facility or space of the nuclear facility (for example alcohol, drug or other addiction; disease or mental disturbance; membership or participation in organisations or groups which threaten the vital interests of the Republic of Slovenia or the member states of political, defence or security alliances of which the Republic of Slovenia is a member, etc.).

For reasons were that in accordance with the Classified Information Act, the security vetting procedure for persons wanting access to information classified as CONFIDENTIAL is equivalent to a security check on persons that work in the controlled facility or space, physically controlled facility or space and vital facility or space of the nuclear facility, in which the equipment, devices, nuclear or radioactive materials or documentation relevant to the nuclear safety of nuclear installations are stored. However, it is necessary to properly define the concepts of security checks and security restrictions in terms of providing the physical protection of nuclear facilities.

Particular attention to the protection of classified information and sensitive data relating to the physical protection of nuclear facilities and their own safety of nuclear installations is given by the International Atomic Energy Agency (IAEA) - which continually points out that both the operators of nuclear installations as well as countries need to devote special attention to this aspect of security.

Furthermore, according to Grošelj [12], we cannot ignore the fact that the energy sector is located at the intersection of a number of areas and interests (ecology, security and protection, security of supply, economically viable prices of energy products and their supply, etc.), while Hellstrom [13] defines a risk assessment formula related to critical infrastructure as: Risk = danger or threat (trigger events) + vulnerability.

Besides the definitions of the terms in the Ionising Radiation Protection and Nuclear Safety Act reached through the inter-ministerial meetings at the expert level, several changes were also proposed for the current Article 120 of the Ionising Radiation Protection and Nuclear Safety Act defining security vetting procedures of persons who perform or will perform work in a nuclear facility.

The reasons for this were to elaborate in the article that the logical topic within provides greater transparency in the implementation of the security vetting procedure. It regulates the vetting of foreign nationals who wish to work in nuclear facilities in Slovenia in accordance with international treaties and agreements. The article provides that a person must complete a security clearance questionnaire, security restrictions, and the duties of the employee to communicate to the employer any changes related. Also official records are defined, from which operators and employers are able to obtain information for vetting. Furthermore, it defines a way of keeping records, the length of data retention and an obligation of the employee to sign a statement of understanding of the regulations in the area of the physical protection of nuclear facilities and of nuclear and radioactive substances.

The provisions of this article shall apply mutatis mutandis for the vetting of persons working with radioactive materials and personnel involved in the transport of nuclear materials. The provisions of this article shall also provide a basis for interim and periodic security checks. In the security vetting procedure of persons with foreign nationality, the nuclear operator cooperates with the Slovenian NSA.

5. International – NSA Cooperation

In addition to its role in various forms of inter-ministerial cooperation, the Slovenian NSA also has the role of ensuring the implementation of international treaties and the international commitments and obligations undertaken, concluded or adopted by the Republic of Slovenia with reference to the handling and protection of classified information. It also shall cooperate in this area with the relevant authorities of foreign countries and international organisations, unless otherwise provided by the international treaty in question. For the mentioned purposes, the NSA shall coordinate activities aimed at ensuring the security of national classified information abroad and foreign classified information in the territory of the Republic of Slovenia.

The procedure for concluding bilateral agreements such as international treaties is defined by the provisions of the Foreign Affairs Act under the title International Treaties, which is based on the principles of the Vienna Convention on the Law of Treaties. The procedural provisions are also determined by the Government of the Republic of Slovenia Act and the Rules of Procedure of the National Assembly of the Republic of Slovenia in the third chapter under the title Ratification of International Treaties. In this respect, the basis is also provided by the provisions of the Constitution of the Republic of Slovenia which refers to the subject concerned. By concluding an agreement, the NSA creates a relevant basis for the implementation of the tasks entrusted to the national authorities who exchange classified information with the representatives of other countries in the course of their working activities. The reasons for the conclusion of agreements include also enabling Slovenian companies and organisations to participate on an equal footing in tenders and the conclusion of business deals associated with the protection of classified information.

The NSA also attends to the implementation of:

- the accepted international obligations and international treaties on the protection of classified information, and
- cooperation in this field with the corresponding agencies of foreign countries and international organisations.

The NSA has carried out all the internal legal procedures required in order to adopt, sign and ratify several bilateral agreements on the exchange and mutual protection of classified information. In addition, the agreements yet to be concluded with several countries are in various phases of the adoption process. As an appropriate legal basis, bilateral agreements facilitate cooperation between state authorities and economic entities and strengthen mutual trust.

According to Kostadinov [14], the vulnerability of the critical infrastructure also increases because of natural disasters and calamities, inadequate procedures and regulations, inadequate leadership, projects with incomplete designs, used equipment, inadequate staff training and experience, as well as because of equipment failures.

Regarding adequate procedures and regulations, international treaties may determine that, in carrying out personnel security clearance, the competent bodies of the Republic of Slovenia may cooperate with the security clearance agencies of foreign countries or international organisations, provided that this is not in conflict with the regulations on personal data protection in the Republic of Slovenia.

The above mentioned cooperation enables the security vetting procedure for persons with foreign nationality when all the related legislation is in place. In the case of the

NEK and similar cases, there are to that respect crucial following provisions regarding bilateral agreements between two governments on the mutual protection of classified information:

- The Parties shall mutually recognise their Personnel and Facility Security Clearances,
- Access to information classified as CONFIDENTIAL and above shall be limited to persons on a Need-to-Know basis who, in accordance with national laws and regulations, have been security cleared, authorized to have access to such information and have been briefed accordingly and
- Upon request, the National Security Authorities shall assist each other in carrying out security clearance procedures (for example: if a Croatia citizen stayed in Slovenia for a longer period of time, the Croatian NSA can ask the Slovenian NSA to have the relevant authorities in Slovenia check their official records regarding this person's data in Slovenia).

In the case of the NEK, these provisions form a legal basis for bilateral cooperation mostly between the Slovenian NSA and the Croatian NSA. Similar bilateral agreements, provisions within and joint participation have also been agreed on with many other states.

During negotiations on bilateral agreements and joint participation, representatives of the NSA are in a position to create a network of contacts with representatives of the NSAs of other countries. In addition to the agreements‘ regulated legal bases, it is this network that enables NSAs to participate efficiently in the area of security clearance and fosters mutual consultation in setting up uniform standards and assistance in drafting amendments to regulations. According to Niglia [15], information and intelligence sharing might represent a further strategic way to contribute effectively to global energy security.

6. Conclusion

In times of rapid development and increasingly close international cooperation between countries, it is essential that all the relevant standards and rules are provided and complied with so as to ensure proper security. The aim of this paper, by presenting the case study of security vetting in relation to nuclear security, is to provide a good example of a systematic approach in the field of the protection of the critical infrastructure. Also in this field of protection and security, special attention is given to international cooperation, education and related research events as an effective way for resolving the current security challenges and for setting the ground for efficient future work.

Human factors and human resources are also crucial when we discuss the risk management of any potential internal threat connected with terrorist threats to the critical infrastructure's normal functioning. If we just consider the potential internal threat [16], similar characteristics are also typical for potential internal threats in other sectors of the critical infrastructure. Approaches regarding legislation and implementation similar to those involved in security vetting in relation to nuclear security can thus be used in other sectors of the critical infrastructure when there is a need for the security vetting of foreign citizens.

During the Nuclear Security Summit [17] in The Hague, the main theme of the discussion was improving security, the international exchange of information and international cooperation.

Cooperation – multilateral, regional, bilateral and internal – is therefore vital for effective security. The legislation setting the relevant legal basis has to be accepted or has to undergo through proper adjustments. Within relevant standards, upon best practices and lessons learned, we can find an effective way to resolve the current security challenges.

Meetings of NSAs and other relevant authorities can strongly contribute to:

- networking
- building relationships
- strengthening trust
- joining efforts to face common security challenges
- setting the legal basis needed for the cooperation of state entities, companies and international organisations.

NATO plays an important role in international cooperation, education, and related research events as well as in the exchange of best practices that contribute significantly to the exchange of information, know-how and mutual understanding as well as to the fulfilment of the key task of these activities, i.e. providing the highest possible level of protection of the critical infrastructure.

References

[1] Nuklearna elektrarna Krško – official website, available at, http://www.nek.si/en/. Accessed 10 March 2014

[2] Pravno-informacijski sistem RS - official website, available at, http://www.pisrs.si/Pis.web/. Accessed 3 March 2014

[3] Urad Vlade RS za varovanje tajnih podatkov – National Security Authority (NSA) official website, available at, http://www.uvtp.gov.si/. Accessed 26 March 2014

[4] Uprava Republike Slovenije za jedrsko varnost - Slovenian Nuclear Safety Administration (SNSA) official website, available at, http://www.ursjv.gov.si/. Accessed 14 March 2014

[5] IAEA Safety Glossary. http://www-ns.iaea.org/standards/safety-glossary.asp. Accessed 2 April 2014

[6] Vršec M (2011) Managing Corporate Security in the Energy Sector: Energetics as a Vital (Critical) Infrastructure for the Functioning of a State; economy and Civil Society. In: Čaleta D, Shemella P (ed) Counter terrorism challenges regarding the process of critical infrastructure protection. ICS, Ljubljana and Center for Civil-Military Relations, Monterey.

[7] Prezelj I ed. (2010) Kritična infrastruktura v Sloveniji. Fakulteta za družbene vede, Ljubljana.

[8] Radović V, Trivan D (2014) Do We Really Understand Why the Environment Has become an Important Task For the Intelligence Community in the Global World? In: Čaleta D, Shemella P (ed) Intelligence and Combating Terrorism New Paradigm and Future Challenges. ICS, Ljubljana and Center for Civil-Military Relations, Monterey.

[9] Čaleta D, Shemella P ed. (2011) Counter terrorism challenges regarding the process of critical infrastructure protection. ICS, Ljubljana and Center for Civil-Military Relations, Monterey.

[10] Trivan D (2012) Korporativna bezbednost. Dosije studio, Beograd.

[11] Radović V (2011) The role of Corporate Sector in Disaster Management: Innovative Public-Private partnership and Development of insurance systems in the field of DRR in SEE. http://www.gripweb.org/~gripwebo/gripweb/sites/default/files/PROF_VESELA_PPP.pdf. Accessed 16 April 2014

[12] Grošelj K (2011) Critical Infrastructure Protection and the Energy Sector. In: Čaleta D, Shemella P (ed) Counter terrorism challenges regarding the process of critical infrastructure protection. ICS, Ljubljana and Center for Civil-Military Relations, Monterey.

[13] Hellstrom T (2006) Critical Infrastructure and Systemic Vulnerability. Towards a Planning Framework, Safety Science.

[14] Kostadinov V (2011) Vulnerability Asessment: New Nuclear Power Plants Universal Methodology for Terrorism Threats and Natural Disasters Analyses and Predictions. In: Čaleta D, Shemella P (ed) Counter terrorism challenges regarding the process of critical infrastructure protection. ICS, Ljubljana and Center for Civil-Military Relations, Monterey.

[15] Niglia A (2013) Critical Energy Infrastructure Protection (CEIP): The role of EU and NATO. Executive summary. http://www.ata-sec.org/projects/ceip-for-xxi-century. Accessed 17 April 2014

[16] Internal Threat (Based upon IAEA approach). Preventive and Protective Measures against Insider Threats. http://www.fmwg.org/sitefiles/iaea.pdf. Accessed 3 March 2014

[17] Nuclear Security Summit (NSS 2014) in The Hague – official website, available at, https://www.nss2014.com/en. Accessed 5 March 2014

This page intentionally left blank

Section 3:
Terrorist Threats to Critical Infrastructure Operation – Environmental Aspects

This page intentionally left blank

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-135

Environmental Terrorism as a Threat to the Serbian Water Infrastructure Sector-through the Lens of Regional Perspective

Vesela RADOVIĆ[a,1] and Aleksandar ANDREJEVIĆ [b]
[a] *Faculty of Applied Security, University Educons*
[b] *Faculty of Business Studies, University Educons*

Abstract. Terrorism in the global world is recognized as one of the most significant threats. Hence, combating terrorism has become a primary focus for security professionals throughout the world. By studying the phenomenon of modern terrorism, we can easily conclude that the nature of terrorism has changed. Therefore, the authors are focused in the article on a new form of terrorism, named "environmental terrorism". Environmental terrorism is an old type of conflict with a new face, and we have to confront it. For the purpose of this article the authors have chosen to present the environmental terrorism threat to the Serbian water infrastructure sector. The available scientific data witnessed that the water infrastructure system in Serbia is already vulnerable and needs a lot of improvement. A terrorist attack on such a fragile infrastructure could have enormous consequences and be devastating in its scope. Hence, the authors have analyzed the current state in the water infrastructure sector, which is already compromised with numerous problems and have addressed the question: do we fully understand the water infrastructure vulnerabilities and what has to be done to ensure its protection as one of the part of the Serbian critical infrastructure? The protection of the water infrastructure sector against terrorist attacks is a task for the Serbian Government, but it has to be solved in collaboration with neighboring countries. The final goal for all activities has to be the greater scope of trust among the neighbors and the achievement of an adequate level of security regarding environmental terrorism threats in the region of South Eastern Europe. Furthermore, environmental terrorism as a threat has to be settled at a national and regional security agenda in a more visible way.

Keywords. water infrastructure sector, environmental terrorism, security threats, critical infrastructure, South Eastern Europe, regional perspective

Introduction

Environmental security has been included for a long time as a necessary part of national and global security. As we have seen in the past several years, the responses to environmental risks in the region of South Eastern Europe were not always adequate in their scope. In many cases the authorities needed to accept help from the international community to mitigate the consequences. Terrorism in the region of South Eastern Europe is recognized as a threat and initiates numerous agreements among countries. Among all, the threat of environmental terrorism is not recognized as a reason for warring or acting in a manner of security services. The environment literally means the surroundings, and everything

[1] Corresponding Author: Dr. Vesela Radović, Vojvode Putnika 87, 21208, Sremska Kamenica, Serbia; Phone number: +381214893680; e-mail: veselaradovic@yahoo.com.

that affects an organism during its lifetime is collectively known as its environment. Environmental terrorism involves targeting natural resources, and it is different from eco-terrorism which involves targeting the built environment. Environmental terrorism can be applied at all levels within a state, region or internationally. The efficacy of terrorism is dependent upon the reaction of the target audience. If the audience does not believe that the environment is susceptible to damage, it is unaffected by the act. From another point of view, it is not a new issue because the manipulation of the environment has been tried for centuries with varying degrees of success. The purpose of this study is to provide a background on environmental terrorism in order to understand how it is dangerous for critical infrastructure, in this case for the water infrastructure system. So the important linkage between integral water management and counterterrorism action is recognized by the authors and initiated the creation of this article.

A few decades ago the world's population started to realize the importance of the environment and the effect of mankind on it. People started to discuss how to mitigate their impact on the environment. It was obvious that the concern was strongly influenced by economic factors. The concept of sustainable development has been introduced and accepted in the international community. For the purposes of this article, environmental terrorism can be defined as the unlawful use of force against *in situ* environmental resources as to deprive populations of their benefit(s) and/or destroy other property. Environmental terrorism, like a threat to every component of the environment (lithosphere, hydrosphere, atmosphere and biosphere) has to be seriously examined as a threat to various parts of critical infrastructure. The history of human civilizations is rich of conflicts regarding water resources. They have been described in testimonies since the first civilizations (stored in intangible heritage, legends and myths) to the current state, visible in reports, peace agreements and numerous bilateral and multilateral conventions. Hence, due to numerous vulnerabilities the water infrastructure is considered as being among the most crucial in the strategies and plans regarding the protection of critical infrastructure in the world. It is equally important for global, regional and local levels, as well for every person individually as a part of the wider concept of human security. This article discusses the risk of environmental terrorism as a function of consequence and probability, and examines various types of attacks that use the water resources both as a target and a tool of terror.

Certain types of infrastructure, like the water infrastructure, play vital roles in underpinning our economy, security and way of life. The hypothesis of this article is the following: is the threat of an environmental terrorist attack on Serbian water infrastructure real, and what is the role of security services in its prevention at a national level? The sub-hypothesis is what implications such an attack could have on neighboring countries, with the view of preventing cross-border impacts regarding shared water resources and hydro-technical objects. The methodology is typical for social researchers: historical analyses, comparative analyses, and data analyses. The documents were collected from electronic sources and printed material (books, journals, official documents, scientific journals, official reports and positive practice from the international community). All data were arranged and used for the purpose of achieving the article's objectives.

In the introduction, the authors present the brief review of a current state regarding the research problem and used methodology. The next chapter covers a brief overview of the development of the environmental security concept and threats of terrorist attacks. The third chapter explains the Serbian water infrastructure sector and its threats and vulnerabilities. Since, due shared water resources, the regional cooperation in the protection of the water infrastructure sector is important, one whole chapter is devoted to these efforts. The last chapter includes some recommendations about the actions needed to prevent environmental terrorist threats on critical infrastructure in Serbia and the region, and highlights the need or a greater inclusion between stakeholders in this important field. Concluding remarks review actions that should be implemented in Serbia in order to strengthen this nation's ability to prevent, prepare for, respond to and mitigate the long term consequences of terrorist attacks on the water infrastructure that could devastate the nation, the fragile environment, and the economy and affect regional cooperation. The article is helpful for the wider public as well as for the academic community and could be useful for all interested parties in the area of environmental protection, emergency management, policy makers and security and the intelligence community.

Hence, sharing information between neighboring countries is very important for environmental security and security in general and it would improve the regional security and numerous misunderstandings from the past will be easier to overcome.

1. Environmental Terrorism versus Environmental and Overall Security

The concept of international environmental security was initially formulated by the Soviet theorists as a component of an all–encompassing "System of International Security" (known by its Russian acronym, Военние системе международной безопасности – ВСМБ/VSMB) [1]. Therefore the link between security and the environment is recognized also in the United States of America (USA), where the environmental security application in practice is recognized with the promotion of a concept named "preventive defense". It is addressed in a speech of President Clinton in his 1996 State of the Union Address, where he described these threats in his call to maintain America's leadership in the world [2]. In 1996, for the first time, the adopted American National Security Strategy recognized new priorities after the end of the Cold War. It was the first American Strategy which addressed the national security threat, saying that "long term environmental degradation caused by the growing population is a political threat in many countries and regions all over the world" [3].

Many other officials in the United States accepted the view of environmental security as a part of "preventive defense", like State Secretary Warren Christopher, who in a major speech in April 1996 at Stanford, stressed that "addressing natural resource issues is frequently critical to achieving political and economic stability, and to pursuing U. S. strategic goals around the world" [4]. The intelligence community has also included environmental issues on its work agenda since the end of the 1990s. The Central Intelligence Agency (CIA) has started to use its resources to monitor environmental degradation and the security issue that has arisen from such degradation [5]. One of the well known officials in the U. S., who won the Nobel Prize for his effort in raising awareness about environmental protection, is Vice President Albert Arnold Gore Jr. (Al Gore). A lesser-known part of his work for the wider public was his collaboration with Russian officials, first of all with the Russian Prime Minister, the result of which was, among other things, the establishment of a special joint commission, known as the Gore-Chernomyrdin Commission [6].

In the global community numerous institutions and organizations have recognized that an inadequate level of environmental protection can interact with political, economic, social, and cultural factors to cause instability and conflict. During the 1970s and 1980s the scope of security changed, as well as referent security objects from a national to a human centered security concept. Those changes are recognized in the United Nations (UN) system and in the academic security community. The brief overview of the development of the concept of environmental and overall security in the global community would not be complete if we did not have a look at the development of efforts of influential security and military organizations like the North Atlantic Treaty Organization (NATO) and its partners who have started to think about the so-called "threat without enemies" [7]. Among different initiatives, it is interesting to mention a pilot study launched by NATO's Committee on the Challenges of Modem Society (CCMS) as a call for the NATO representatives to work closely with the representatives of the North Atlantic Cooperation Council and the Partnership for Peace countries entitled: "Environment and Security in an International Context" [8]. The authors of the article also addressed the importance of the identification of threats from environmental terrorism on critical infrastructure as it had been done previously in a NATO initiative in April 2010, when a NATO Science workshop was organized in Moscow which addressed the issue of environmental security and "eco-terrorism "[9].

Terrorism is the most threatening issue in the world and it endangers the lives of millions of people and their environment. There are well known ambiguities in defining "terrorism" and specifically environmental terrorism. The environmental terrorism is a relatively new concept, but it is studied as an important issue which contributes to a better understanding of the Persian Gulf War in the context of its environmental impact and has brought the issue to the forefront of international attention [10].

The objective of environmental terrorism, however, is to have a psychological effect on the target population. As environmental awareness increases in global agenda and human minds, it is reasonable to expect also that environmental terrorists could find environmental targets more and more attractive in their importance to society. The security services and other stakeholders have to address the difficult and unique challenges posed by environmental terrorism as a threat to environmental and human security. Therefore, successful efforts in combating environmental terrorism need implementation policies which have already been seen in the activities of combating other kinds of terrorism and in the end provide the adequate level of environmental security and overall security within a society.

2. The Serbian Water Infrastructure Sector - Threats and Vulnerabilities

At the beginning of this chapter there is a need to present just a brief overview of the current state of Serbian water resources. Serbia is situated in the Balkan Peninsula and its water resources are diverse. Approximately 8% of all available surface waters are domestic. The remaining 92% are transitional waters. Serbia's predominantly upland terrain can be divided into a northern region (part of the Pannonia Plain intersected by the Danube, Sava, Tisza, Tamiš and Begej rivers, the Danube-Tisza-Danube canal system (DTD) and several lakes. This central-southern region is connected to the southern Balkans via the Morava and Vardar/Axios Basins. Hydropower is a significant power generator and water user in Serbia where there are 13 major reservoirs greater than 10 million m^3 dedicated to energy production [11]. The waterway network extends over 1,700 km of the Danube, Sava and Tisza rivers respectively as well as the 600 km navigable part of the Danube-Tisza-Danube (DTD) system. All are directly or indirectly connected with the European inland network.

Flood control in Serbia is mostly provided by levees on the major rivers of the Pannonia Plain and central Serbia where all major cities and significant industrial facilities are located in potential flood areas. Environmental flood effects manifest through jeopardize environmental components like water and soil. The spilling of sewage is a common case in towns during flood, as well as water supply damages and the pollution of drinking water.

There is an estimation that an area of some 1.6 million hectares in Serbia is under the threat of the detrimental effects of water. The Northern Province of Vojvodina is particularly under threat, since it comprises the Southern part of the Pannonia Plain and has significant parts lying below the high waters of transitional watercourses [12]. One of the recent analyses of floods has been presented in the work of Milanovic et al. This study reviewed the greatest floods recorded in Vojvodina and central Serbia within the period from 1999 to 2009. It confirmed that at the end of the 20th and beginning of the 21st century, the frequency of catastrophic floods on the Danube and its tributaries increased. Even where the protection system has been built, the potential risk of flooding exists, since the protection facilities are often not appropriate (dimensions of objects; objects are not connected in compact units; quality and type of applied material are not satisfactory) [13].

Serbia, like many transitioning and developing countries, has been facing many challenges to implementing integral water management policy. The data about the previous and current state of the water sector is presented in numerous reports and are an issue of various national, regional and local studies [14, 15 and 16]. The country's environmental regulator, the Serbian Environmental Protection Agency (SEPA) made annual assessment of Serbia's water infrastructure. Some facts in these reports are very disturbing. In the Autonomous Province of Vojvodina there are 465 settlements, 69 of which do not have piped water. The data on rural public water supply systems are very scarce, but it is estimated that there are about 5,000 that are not registered and are not water quality controlled. Water supply systems cover 300,000 private wells. In the water sector there is obviously a big gap between the financial needs and the current investments in this area. Irregular and inadequate maintenance has resulted in various degrees of damage to the water infrastructure and a consequent decline in the quality of services provided by some facilities and systems, as well as the reduced safety and level of protection against the adverse effects of poor water quality [17]. Due to the consequences of the global financial crises and the enormous budget deficit in the country, the situation has started to be more serious. Therefore, urgent changes in the legislative framework are required at a time when all indicators of social development are rather problematic, and the expectation of any improvement in the nearest future represents a big issue [18].

With all the above-mentioned in mind as well as the possibilities of terrorist attacks in a still vulnerable geo-political region, the Serbian water infrastructure sector is vulnerable to the threats from terrorist attacks. On the one hand, water resources are vulnerable as "resource-as-tool terrorism", and on the other hand as "resource-as-target terrorism".

Concerns about the safety of municipal water supplies in light of the recent terrorist activities in the world have raised questions about the continued integrity of hydraulic structures such as dams, as well as the contamination of public water supplies. It is not strange that the threats from environmental terrorism as domestic terrorism threats are encompassed in the national strategies of some of the most developed countries like the USA and Canada.

The Serbian water infrastructure sector may be a target of terrorist attacks devoted to ruining the national critical infrastructure, but it may be also the target of abuse where some water infrastructure object is used for the execution of terrorist acts in some neighboring countries due to geographical conditions. From disturbing facts about numerous constraints in water management, it is clear that even in the current "regular condition" Serbia is faced with enormous obstacles to providing the adequate level of integral water management. The reason for this statement is caused by numerous objective and subjective factors, and regarding that fact the outcome of possible environmental terrorist attacks could be enormous in its scope. Furthermore, Serbia has already been faced with numerous examples of citizen protests against the government and policy makers due to the current status of drinking water in many towns, like in Zrenjanin, Užice, Odzaci, and permanent scarcity of water in summer which makes the situation even harder. Despite the existing plans prepared decades ago, global climate change and interruption in the construction of regional water supply systems create daily cover pages and news in printed and electronic media [19]. So, any additional deterioration of the water infrastructure system could impact political and social conditions in the country.

Many times in the past Serbia faced with enormous environmental consequences of the pollution of transitional water flows (trans-boundary pollution). During such an event there was an urgent need to understand critical vulnerabilities within the water infrastructure, especially in the water supply infrastructure (reservoirs, pumping wells, and distribution systems). The two most serious accidents which caused both short- and long-term environmental effects on Serbian water and the ecosystem were the accident on the evening of 30 January 2000, the breakage in the Aurul dam near the city of Baia Mare, and the next well known in the public as the "red sludge spills". The first accident led to approximately 100,000 m^3 of waste water containing up to 120 tons of cyanide and heavy metals being released into the Lapus River, then traveling downstream into the Somes and Tisza rivers into Hungary before entering the Danube [20, 21]. The second serious accident happened on 4 October 2010, in a factory belonging to a privately owned company, Magyar Alumínium ZRt. In this accident there were ten victims, and several hundred people were injured. The pollution plume also reached the Danube but samples showed that no significant amount of pollution entered into the Danube [22]. While neither of these incidents was terror-driven, they illustrate how much damage can be caused by a similar terrorist attack or even sabotage.

The Serbian water infrastructure sector is vulnerable to environmental terrorist attacks in the two already accepted forms of terrorist attacks: destroy/damage it by using various forms of explosives or the introduction of poison or disease-causing agents (which could be considered as a sub-form of environmental terrorism-bioterrorism). It is surprising that despite numerous accidents, risks and threats it is not recognized that some similar accident could be caused by terrorists. The physical attributes of water resource sites that make them attractive to terrorists, or site weaknesses, are many. Most of the water infrastructure, such as dams, reservoirs, and pipelines are easily accessible to the public at various points. One such attack might involve a large hydroelectric dam on a major river. Alternatively, damage to the spillway gates could cause significant downstream.

There are two components to measuring the risk of terrorism: the severity of the attack, and the probability of a particular scenario actually occurring. Environmental terrorism has the potential to combine the worst of both of these scenarios: it can have higher consequences than conventional civil terrorism because the potential damage from an environmental attack can be long-lasting and widespread, and it can be carried out using conventional explosives or specific contaminants [23].

In the global community characterized with the increasing use of Information Communication Technologies (ICT) in every part of social life, the cyber threats start to be a great fear. Major Cyber attack against critical infrastructure could have an enormous impact on the environment and could be used for the purpose of environmental terrorism. It has already been noted that a computer hacker could break into the supervisory control and data acquisition (SCADA) computer system that runs the water flow in a dam and use that for his own objective(s). Threats to the nation's water infrastructure are as real as any other form of terrorism [24].

Numerous results from various researches have shown that gaps still remain in effectively understanding the water infrastructure's vulnerabilities and integrating appropriate security measures.

3. Regional Cooperation in the Protection of the Water Infrastructure Sector from Terrorist Attacks

Regional cooperation in the area of the protection of the water infrastructure from environmental terrorism or another kind of terrorist attacks is a very complex issue. It consists of a few different areas of initiatives.

- First, it is the establishment of integral water management and the establishment of cooperation in the drastically changed conditions, and
- Second, it is counter terrorism cooperation necessary for the mitigation of terrorist threats to the critical infrastructure sector - for the purpose of this article the emphasis is directed on the water infrastructure sector.

Therefore, in this chapter we give a brief overview of both of these initiatives, having in mind all aforementioned obstacles.

In one of the recent documents about the current conditions in the Western Balkan region and the Black Sea region, the authors addressed numerous common risks and challenges in these countries, including fragile statehood, a shared history of conflict, unconsolidated democratization and economic underdevelopment. It is interesting to see how in the introduction of the same document Otto Simonett colorfully described that state. He wrote: “Consequently talk of the Balkans, the environment and security may sound like yet another indigestible cocktail of pollution, conflict and poverty, with maybe some sex and crime too” [25]. The region of the Western Balkan countries is one of the richest regions in clean water in Europe. The value of these waters is estimated at 4-6 billion Euros annually. In most of the countries the management over the waters is divided between different ministries, institutions, funds and local municipality units. This separation of jurisdictions creates preconditions for different sorts of crime, corruption and the neglecting of public interest. According to the experts from this field, the entire financial debts in the region exceed 2 billion Euros annually [26]. It is hard to imagine how any kind of terrorist attacks in water infrastructure could be devastating for the future development of some country, or a few of them.

In the area of water management, it is important to address the fact that before the dissolution of the Socialist Federal Republic of Yugoslavia (SFRY) there were six international river basins in the Balkans. After 1992 (historical sources recognized this year as official for the creation of new countries in the Balkans) there are 13 internationally shared river basins and four trans-boundary lake basins. Such a fragmented situation needed new international agreements and established various kinds of cooperation on different bases in numerous areas, as well in the area of water management. The establishing new kinds of relations was and still is extremely hard, bearing in mind that due to ethnical conflicts, neighboring relations are still burdened by past experiences. The international community was enormously helpful in overcoming various sensitive regional issues. Among numerous useful incentives, two are especially significant for the objective of this article:

- The first, called the Petersburg Process, started in 1998 from the point of view of development, the environment, and policy on security and the economy [27].
- The second is the Environment and Security Initiative (ENVSEC), which is mainly focused on strengthening the cooperation between and within countries that are vulnerable to environmental damage and competition for natural resources, contributing to a reduction in cross-border risks arising from hazardous substances and pollution; supporting improved urban development and adaptation to climate change; as well as fostering the empowerment of civil society to address environment and security risks [28].

The further tasks for regional and international cooperation in the area of water infrastructure protection is numerous: the protection of the source used for drinking water supply as well as the prevention of sediment management (quality and quantity), the prevention of accidental pollution, and emergency preparedness. The dangers caused by morphological alterations due to dams and hydropower plants, and hydrologic alterations due to water abstractions for agricultural and industrial purposes, and hydropower operation must also be dealt with, especially with attention paid to possible terrorist attacks and future plans in the use of hydro power for energy production. Additional obstacles are that, even in one country, there are so many stakeholders involved in the processes of integrated water resources management, and inappropriate legislation and institutional capacity, as well as collaboration which is often missed or inadequate in scope.

The Republic of Serbia is devoted to the extension of the regional cooperation and coordination in the future in various areas, as well as in the area of the environmental protection. In this process, various activities regarding the fulfillment of the European Water Framework Directive (WFD) requirements have an essential role [29]. Multilateral cooperation in the field of water is implemented through the work of the International Commission for Protection of the Danube River (ICPDR) - Danube Commission, the International Sava River Basin Commission and expert groups within the UNECE Convention on the Protection and Use of Trans-boundary Watercourses and International Lakes (Water convention), the Hydrology and Water Resources Programme of World

Meteorological Organization, UNESCO International Hydrological Programme, and especially within the Danube countries, and the cooperation of competent national hydro-meteorological services [30].

Trans-boundary cooperation on water management has been established by the Ministry of Agriculture, Water Management and Forestry (MAFWM) and the Republic Water Directorate (RWD) and other stakeholders in this area. Despite numerous positive efforts to contribute to both the environmental and overall security in the Danube region, as well in the Black Sea region, Serbia still has a lot of room for improvement. One of those areas where Serbia has to improve is participation in the Danube Accident Emergency Warning System (AEWS). It is a web-based messaging tool for international coordination organized by the ICPDR. In the event of an accident on surface waters with a possible trans-boundary impact, Principal International Alert Centres (PIACs) share relevant information: the respective PIAC submits a message by filling in a form for the specific situation. All relevant PIACs – primarily those located downstream of the accident site – are then automatically and instantly notified by SMS and e-mail and can view the full message on the web. The system is extremely useful for further communication on the similar accidents which are presented in the article [31].

Detailed issues about the cooperation in water management due to various challenges is addressed in a holistic way in the first assessment of trans-boundary rivers, lakes and groundwater entitled: Our waters: joining hands across borders - first assessment of trans-boundary rivers, lakes and groundwater in 2007 [32].

Similar facts are also a part of several important regional studies performed by Katerina Tumbovska in 2011 and Ruzhdi et al. in 2010 [33, 34]. Water that crosses national borders takes more complex and strategic importance and has to be "everyone's business".

Another important issue regarding water sector protection from terrorist attacks is hard to explain because in the region there is still fear existing mainly from ethnical conflicts and religious terrorism. Environmental terrorism is not an issue which is recognized in the actions of stakeholders in the security area despite the examples of current practices and strategic development all over the world. It is expected that greater attention would be presented in future documents which have to be established on the Serbian path to the European Union and the necessity to fulfill the criteria about critical infrastructure protection (and so on in the water infrastructure sector).

An act of terrorism puts an entire society immediately into a state of shock and, in addition to material damage caused to infrastructure, results in irreparable consequences for the population of a city or country where the act had been committed [35]. Protecting the water infrastructure from a terrorist attack as well as from other existing threats is a task for national security services, but also for neighboring countries because of the great possibility of cross border environmental, health and economic impacts. The European Union (EU) Strategy for critical infrastructure protection defines critical infrastructure as an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behavior, may have a significant negative impact for the security of the EU and the well-being of its citizens [36]. The severe consequences of an attack on water infrastructure as a part of critical infrastructure and the significant interdependencies among water and other numerous sectors are enough to provide a motive to terrorists. Environmental terrorism is not recognized as a threat to the society in any country in the region in greater scope, but from another point the environment is a part of every national security strategy, which seems pretty illogical. Legal framework obliged security forces, policy makers and other stakeholders to protect the environment from all threats, but environmental terrorism is not recognized as a threat among many others. Most strategies point to the environmental threats caused by natural disasters or anthropogenic in origin, like technical-technological disasters, mostly industrial accidents, but the environment (or any environmental component) is not recognized as a direct or indirect target for terrorist attacks.

Environmental security as a term refers to the entire array of security forces, measures, and arrangements with which a terrorist group must cope in order to operate and carry out its objectives. Unless they can be sure about the achievement of surprise, and long-term fear among citizens, terrorists cannot hope to accomplish their goals. In the USA, particularly useful research was carried out about the categories of terrorists which had conducted the majority of attacks against critical infrastructure (CI) worldwide. The authors suggest that three main categories of terrorist groups may have the highest disposition to attack the U. S. critical infrastructure targets in the future:

1. Transnational Islamist terrorist groups;
2. Domestic right wing “militias”, and
3. The most violent fringes of the radical ecology movement - Radical Ecology Groups.

Although such groups have often proclaimed their intent to avoid causing human casualties, the weakening of such restraints cannot be ruled out in the future. Some radical ecology movements could be extremely dangerous and are recognized as a threat in numerous reports in the intelligence community. The most important to be recognized are those with an uncompromising anti-technology or neo-Luddite agenda [37].

Critical infrastructure protection in Europe as well as “across the ocean” in the USA and Canada, started to be an important issue in national security decades ago. The procedure for the identification and designation of European Critical Infrastructures (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructures is established by legal framework. The EU-Directive 2008/114/EC introduces a practice to identify and designate European critical infrastructures (ECI), committing each member state to designating potential ECI according to the EU-definition and according to cross-sectored criteria (casualties, economic and public effects) and sector specific criteria (taking into account individual sector characteristics). Further criteria to be considered, as addressed in the European Programme of Critical Infrastructure Protection (EPCIP) are the geographic scope of impact (when disrupted or destroyed), severity and consequences (public, economic, environmental, political and psychological effects, and public health consequences) or geographic- and sector-specific dependencies [38]. The EPCIP points out the all-hazard approach (prioritizing terrorism) and the principles of subsidiarity, complimentarity, confidentiality, stakeholder cooperation, proportionality and sector-by-sector approach. The framework comprises the identification and designation of CI, an action plan, the establishment of a Critical Infrastructure Warning Information Network (CIWIN) and a CIP Contact and Expert Group; further the support of the member states, contingency planning and the external dimension. The objectives to guarantee European-wide adequate and equal protection levels, minimal single points of failure and rapid and tested recovery processes were defined earlier on. In almost every document in the EU, the threat is recognized from terrorist attacks on critical infrastructure and that should be the path for the future Serbian authorities to do the same, as well as for other countries in region which still have not established the legal framework for the protection of critical infrastructure [39, 40, 41].

The United Nations, the most influential international organization, adopted the Global Counter-Terrorism Strategy in 2006 as a unique global instrument that will enhance national, regional and international efforts to counter terrorism. Therefore, as the Strategy needs permanent review, the General Assembly renewed it in June 2012 [42]. The EU developed its own Counter-Terrorism Strategy aimed at responding to the current terrorist threats around four objectives: prevention, protection, pursuit and response [43].

Serbia is a country devoted to all counter terrorism activities in the region and international community. During the last decade the government created the legislation in accordance with the existing EU Counter Terrorism Strategy in all areas regarding the protection from different hazards [44, 45]. A lot of activities have been performed by the engagement of the Ministry of Defense and the Armed Forces of the RS in terms of internal security which are regulated by numerous strategies, laws, and sub-laws. According to the Serbian Defense Strategy, the mission of the Armed Forces of Serbia is to support the civil authorities in opposing security threats.

The Serbian policy highlighted the need for cooperation and trust on external relations with neighboring countries as a prerequisite for full membership in the European Union. Among all, Serbia enhances international cooperation on the detection and monitoring of the environmental threats related to water infrastructure protection. During all these actions it must be noted that Serbia still lacks the financial means, modern governance, responsible natural resource management, technology transfer, trans-boundary environmental cooperation, institutional strengthening and capacity building for crisis management, adequate resource planning, climate-sensitive policy and equality and favorable conditions for foreign investments and has to work on the improvement of its current state [46]. Despite the obstacles, it is clear that a new age in better cooperation in the region will come. With regard to the trans-boundary water management for any country, it is important that the country takes part in many projects that deal with these issues so that the country could be an active participant for improving and maintaining trans-boundary water management. Another important issue regarding the protection of the water infrastructure sector from terrorist attacks has been seen from numerous kinds of cooperation in the area of organized crime and counter terrorism efforts, and so it could be expected that the future actions would be aimed at the well being of every country and the region as a whole. After all, peace in the region has no price.

4. Challenges of Protection of Water Infrastructure Sector

The Republic of Serbia is devoted to achieving full membership in the European Union. Therefore, the security policy and environmental protection policy have to be established on the accepted European legal framework in those areas. However, critical infrastructure protection is still not included in the current defense strategies. Despite the fact that terrorism and different threats of organized crime are recognized in Serbia, awareness about environmental terrorism is still not evaluated as a respectable threat. In numerous scientific publications and official reports about the security in South Eastern Europe and the Western Balkans, it is clear that there exists a permanent threat from terrorist activities. Those threats are explained in the recent report from the USA: “Ethnic and internal political divisions in the Western Balkans will continue to pose the greatest risk to regional stability. Many fragile states in that region suffer from economic stagnation, high unemployment, corruption, and a weak rule of law” [47]. Therefore, it is not surprising that the scientific community speaks loudly about the urgent goals in protection of critical infrastructure. The majority of those warnings are devoted to the identification of existing weaknesses, future promises about better cooperation and coordination at national and regional levels, and within the EU, various theoretical approaches and the “newest threat from like cyber criminals”, since the water infrastructure sector is not so recognized in the counter terrorism efforts, even though there is a long history of using water as a political or military target or tool, going back over 2500 years [48]. Therefore, it looks like some security “experts” do not recognize and ignore the complex and real relationships between water and security, which could be one of the major challenges for future development.

The risks of water-related violence and conflict are growing, not diminishing, as population, resources, and economic and environmental pressures on scarce water resources increase. Many of these risks are materializing at the sub-national level rather than as disputes among nations, but even at the national level, there are growing concerns about tensions in Africa and parts of Asia that share international rivers but lack international agreements over how to manage those waters [49]. Policy makers have to be aware that water sector protection, as a part of critical infrastructure, is a task of paramount priority in the future implementation of the accepted concept of sustainable development. In the social sphere and relations, due to the expectation of changed Labour Law in Serbia, workers’ rights could be a serious issue, even though, of course, an unsatisfied labor force is not a part of the terrorist community. The initiative connected with protests could have the same results as environmental terrorist attacks on water resources. This doubt has been generated after the event when workers at the Cellatex chemical plant in northern France dumped 790 gallons of sulfuric acid into the Meuse River when they were denied workers’ benefits [50]. In Belgrade Bear Factory, a similar accident happened in 2009, and it was declared an industrial accident. In that accident about 20 tons of hydrochloric acid from a reservoir of 25 tons was spilt. After an examination, it was confirmed that there were approximately 70 industrial facilities which produced, used or stored hazardous chemicals in the city center and/or residential areas of the Serbian capital [51]. Leaving aside the question of whether or not the workers would be considered terrorists, they certainly do not appear to have committed a terrorist act, since there was no way to isolate the effects of the acid from the general population.

In Serbia in the last few years, despite numerous reforms in the security sector, there are still many vague issues in the area of environmental and overall security. The Law on Emergency Situations was passed, but the system still does not have all the necessary legal and organizational prerequisites for reaching maximal efficiency. The activities of the Sector for Emergency Management in regional and international cooperation in the field of cooperation and mitigation of consequences of natural disasters are encouraging, but still not adequate in scope [52]. Furthermore, we still have daily cover pages in newspaper and news in electronic media about enormous damage and devastated infrastructure in floods, destroyed bridges and roads, land covered by water in planting season, high levels of ground waters, numerous warnings about the interruptions of the water supply system due to unsafe conditions, and so on. Scientists all over the world warn that a comprehensive public policy for critical infrastructure protection must begin with an understanding that "protection" per se should not be the goal. In an open society, higher fences and thicker walls do little to reduce aggregate vulnerabilities. In many instances, protection simply shifts the focus of terrorists to other, less heavily fortified targets. Even if one accepts the word "protection", what is being protected is not the infrastructure itself but the services it provides. With regard to terrorist threats, the policy goal should be to build capabilities for the prevention of attacks that interrupt such services and for an effective response and rapid recovery when such attacks do occur [53].

Enhancing capabilities in the water infrastructure protection at national and regional levels based on prevention, recovery, and response relating to environmental terrorist attacks on it is not, and would not be easy. In the long run, responding to this challenge will not only require changes in the policies adopted by interested parties. It will also require improving the effectiveness of other strategies and public policies, reflecting an emerging balance of roles and responsibilities. Institutional capabilities to identify, negotiate, and implement such policies are at least partly in place. Regardless of the currently established cooperation in the field of the integral management of water resources and intelligence cooperation regarding counter-terrorism, at a national level the countries have yet to give priority to addressing the vulnerability of water infrastructures.

Serbia is devoted to the extension of the regional cooperation and coordination in the area of environmental and overall security, but in this process it is faced with numerous obstacles [54]. In many international projects devoted to the area of environmental protection, upon their completion, the sustainability of those projects is not provided in further activities of competent authorities. Few important projects are conducted by the United Nations Development Program (UNDP), the Western Balkans Environmental Program, as well as the Environment and Security Initiative (ENVSEC). Additional challenges lay in establishing a close cooperation in the area of intelligence sharing because Serbia and other countries in South Eastern Europe have to strengthen their intelligence capabilities in the area of ecological security. Environmental terrorism could be a great threat and so a strong response is needed.

A Fifth Geneva Convention on the Environment provides a legal framework for global environmental protection, and symbolizes the international community's intolerance for and solidarity against environmental terrorism. To prevent future acts of environmental terrorism, the international legal community must provide a more comprehensive and predictable system of resolving conflicts, providing remedies, and prosecuting war criminals [10].

5. Conclusion

In global community it is proven that the link between the environment and security has grown. Therefore, environmental security starts to be an issue of paramount interest of the future development in the global community. Environmental terrorism as any other kind of terrorism is considered a form of low intensity conflict. It can be applied at all levels within a state, region or internationally. It is a relatively new concept which needs the greater attention of those who have to plan our security strategy. Hence, the current environmental status in Serbia, as well as in the region of South Eastern Europe, still suffers from the consequences of historical pollution and any additional environmental threat could have a drastic impact on the fragile environment. That sensitivity is especially visible in the water infrastructure sector.

From all the facts presented in this article it is obvious that environmental terrorism and the vulnerability of the water infrastructure, as a critical infrastructure, are clearly a great danger to the Republic of Serbia and a few other states in the region. The budget shortfall makes the security services' job even harder and due to that there are so many useful incentives which contribute to a higher level of security on the one hand, and avoid the duplicating of resources in the region on the other hand. Therefore, despite the fact that some negotiation process is still ongoing in the region which needs international arbitrage, there are many reasons to believe in the need of a better cooperation in the area of integral water management and environmental and overall security. Every Government is devoted to providing its citizens peace and economic well-being, and therefore mitigating the risk which we share with our neighbors is recognized as an urgent need. Serbia is devoted to the extension of the regional cooperation and coordination in the area of water management and environmental and overall security. In many of the international projects devoted to the area of environmental protection, upon their completion, the sustainability of those projects is not provided in the further activities of the competent authorities, and so there is a need for permanent work in the future. Hence, in the future work of security and others services, especially in the water infrastructure sector, all stakeholders have to start bridging a gap among them. In the future we have to experience some of those changes in the work of intelligence systems at national and regional levels, and due to that initiative, provide a greater public participation in the area of environmental security and the protection of critical infrastructure. The practice in the work of intelligence in the global community in counterterrorism shows us the path to follow it in the future.

References

[1] United Nations, International Ecological Security, UN/A/C.2/42/L.34, 1987.

[2] The American Presidency Project [Internet]. Available from: http://www.presidency.ucsb.edu/ws/?pid=53091.

[3] Federation of American Scientist [Internet]. Available from: https://www.fas.org/spp/military/docops/national/1996stra.htm

[4] U.S. Department of State [Internet]. Available from: http://1997-2001.state.gov/www/global/oes/speech.html

[5] Central Intelligence Agency [Internet]. Available from: https://www.cia.gov/news-information/speeches-testimony/1996/dci_speech_072596.html

[6] Memorandum between the Department of Defense of the United States of America, and the Ministry of Defense of the Russian Federation on cooperation in environmental protection issues, (1993).

[7] P. Hough, Understanding Global Security, Rutledge Taylor & Francis Group, (2008), 10.

[8] Sherri Wassermann Goodman. The Environmental and National Security. Loyola University Maryland [Internet]. Available from: http://www.loyola.edu/departments/academics/political-science/strategic-intelligence/intel/goodman.html

[9] NATO [Internet]. Available from: http://www.nato.int/cps/en/natolive/topics_49216.htm

[10] J.E. Seacor, Environmental Terrorism: Lessons from the Oil Fires of Kuwait, *American University International Law Review* 10, no. 1 (1996), 481-523.

[11] Water resource base of the Republic of Serbia (VOS). Official Gazette of the Republic of Serbia number 11/2002.

[12] V. Radović, Lj. Ćurčić, J. Stepanov, D. Prokić, Increasing awareness about need of preparedness and response of agricultural household and enterprises in floods in Vojvodina, Proceedings of the International Conference NewEnviro: New Approaches for Assessment and Improvement of Environmental Status in Balkan Region – Interactions between organisms and environment, 28-30 May (2012).

[13] A. Milanović, M. Urošević, D. Milijašević. 2010. Climatic Extremes in Serbia, definitions, types and classification. *Bulletin of the Serbian Geographical Society* Tome XC 1 (2010), 93-121.

[14] Ekonomska komisija za evropu - Komisija za programsku politiku u oblasti zaštite životne sredine, *Pregled stanja životne sredine Republika Srbija, Drugi pregled*, Ujedinjene nacije, Njujork i Ženeva, 2007.

[15] Institute for the Development of Water Ressources "Jaroslav Cerni", *Study of Sustainable Development of Water Management Sector in the Republic of Serbia* (in Serbian), Belgrade, Serbia, 2003.

[16] Institute for the Development of Water Ressources "Jaroslav Cerni", *Instruments for development of the water sector in the Republic of Serbia – Phase One* (in Serbian), Belgrade, Serbia, 2006.

[17] Institute for the Development of Water Ressources "Jaroslav Cerni*", Instruments for development of the water sector in the Republic of Serbia – Phase Two* (in Serbian), Belgrade, Serbia, 2011.

[18] V. Radovic, Protecting and improving water quality in Vojvodina, In: Environmental and Food safety and Security for South-East Europe and Ukraine. Springer Publishing, NATO Science for Peace and Security: Series C Environmental Security, (2012), 189-202.

[19] V. Radovic, Climate Change and Adoption Strategies: A Report from the Republic of Serbia, In: National Security and Human Health Implications of Climate Change. Springer Publishing, *NATO Science for Peace and Security: Series C Environmental Security* (2012), 95-102.

[20] European Commission [Internet]. Available from:
http://viso.jrc.ec.europa.eu/pecomines_ext/docs/bmtf_report.pdf

[21] Regional Environmental Center [Internet]. Available from:
http://archive.rec.org/REC/Publications/CyanideSpill/ENGCyanide.pdf

[22] Euronews [Internet]. Available from: http://www.euronews.com/tag/hungary-toxic-sludge-spill/

[23] E.L. Chalecki, A New Vigilance: Identifying and Reducing the Risks of Environmental Terrorism, *Pacific Institute for Studies in Development, Environment, and Security,* Oakland, USA, 2001.

[24] V. Radovic, D. Trivan, Do we really understand why environment became an important task for the Intelligence Community in the global world, *The 6th International Regional Conference "Counter Terrorism Challenges In The Region Of South Eastern Europe*, (2014).

[25] UNEP/GRID-Arendal, *Balkan Vital Graphic*, Zemun, Serbia, 2007.

[26] Water Resources of Western Balkan [Internet]. Available from:
http://i-scoop.org/fileadmin/download_files/WATERS_2_.pdf

[27] TWRMinSEEandMENA [Internet]. Available from:
http://www.twrm-med.net/southeastern-europe/regional-dialogue/framework/petersberg-phase-ii-athens-declaration-process/petersberg-process

[28] Regional Environmental Center [Internet]. Available from: http://www.rec.org/envsec.php

[29] European Union, Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for Community action in the field of water policy, *Official Journal of the European Communities* L 327, 1-72.

[30] Response to the EU Questionnaire for the Member States on Experiences: Chapter 27 Environment. Questionnaire on Addressing new and emerging challenges, 2011, Available from:
www.serbia.gov.rs/?change_lang=en

[31] International Commission for the Protection of the Danube River [Internet]. Available from:
http://www.icpdr.org/main/activities-projects/aews-accident-emergency-warning-system

[32] Economic Commission for Europe, Convention on the Protection and Use of Transboundary Watercourses and International Lakes: Our waters: joining hands across borders - first assessment of transboundary rivers, lakes and groundwater. *United Nation Publication*, New York and Geneva, 2007.

[33] K. Tumbovska, Water Resources Management in the Western Balkan Region (Case study of Macedonia, Albania, Kosovo and Montenegro) Geneva, Switzerland, 2011.

[34] P. Ruzhdi, P. Vahdet, E. Arsim, B. Valbon, Water Resources Challenges in Kosovo and their Transboundary Impacts, Prishtina, Kosovo, 2010.

[35] D. Čaleta, Coordination and its impact on process efficiency of consequence management after terrorist attack, *Managing the Consequences of terrorist Acts-Efficiency and Coordination Challenges*, 2012, 11-27.

[36] The Council of the European Union, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union* L345 (2008), 75-82.

[37] G. Ackerman, P. Abhayaratne, J. Bale, A. Bhattacharjee, C. Blair, L. Hansell, A. Jayne, M. Kosal, S. Lucas, K. Moran, L. Seroki, S. Vadlamudi, Assessing Terrorist Motivations for Attacking Critical Infrastructure, Center for Nonproliferation Studies, Monterey Institute of International Studies, California financed by Science and Technology Directorate and U.S. Department of Homeland Security (2007).

[38] European Commission, Staff Working Document, On the review of the European Programme for Critical Infrastructures Protection (EPCIP), Brussels, 2012.

[39] European Commission, Staff Working Document, A new approach to the European Programme for Critical Infrastructure Protection: making European critical infrastructures more secure, Brussels, 2013.

[40] European Commission [Internet]. Available from: http://ec.europa.eu/dgs/homeaffairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm, 20/06/2013, 15h30.

[41] European Union [Internet]. Available from: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33262_en.htm, 20/06/2013, 17h15.

[42] General Assembly, United Nations, Global Counter-Terrorism Strategy, *Resolution* 60/288, (2006).

[43] Council of the European Union, *Counter-Terrorism Strategy*, Brussels, 2005.

[44] Republic of Serbia, Ministry of Defence, National Security Strategy of the Republic of Serbia, *Official Gazette of the Republic of Serbia* No. 88/09, (2009).

[45] Republic of Serbia, Ministry of Interior, National Strategy for Protection and Rescue in Emergency Situations, *Official Gazette of the Republic of Serbia* No. 86/11, (2011).

[46] V. Radovic, A. Andrejević, Serbian efforts to improve environmental and overall security in Black Sea regional cooperation, Springer Publishing, *Black Sea Energy Resource Development and Hydrogen Energy Problems,* (2013), 271-290.

[47] United States of America, Director of National Intelligence [Internet]. Available from: http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

[48] P.H. Gleick, The water conflict chronology, *The World's Water 2004–2005: The Biennial Report on Freshwater Resources* (2004), 234–255.

[49] Pacific Institute [Internet]. Available on: http://pacinst.org/issues/water-and-conflict/

[50] The Christian Science Monitor [Internet]. Available from: http://www.csmonitor.com/2000/0721/p8s1.html

[51] Green Horizon [Internet]. Available from: http://www.greenhorizon-online.com/index.php/Serbia/acid-spill-prompts-investigation.html

[52] V. Radovic, Climate Change and Adoption Strategies: A Report from the Republic of Serbia, Springer Publishing, *National Security and Human Health Implications of Climate Change,* (2012), 95-102.

[53] P. Auerswald, L.M. Branscomb, T.M. La Porte, E. Michel-Kerjan, The Challenge of Protecting Critical Infrastrcure, 2005. Wharton University of Pennsylvania [Internet]. Available from: http://opim.wharton.upenn.edu/risk/downloads/05-11-EMK.pdf

[54] V. Radović, *Bezbednost životne sredine-evolucija i savremeni pristupi*, EDUCONS Univerzitet, Sremska Kamenica, 2013.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015

© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-151

Assuring Food Security in Agricultural Production in the Republic of Bulgaria under the Conditions of General Globalization

Ekaterina ARABSKA[1] and Ivanka SHOPOVA
University of Agribusiness and Rural Development - Bulgaria

Abstract. The paper scrutinizes the current situation in agricultural production in the Republic of Bulgaria as the sector of the national economy with the greatest significance in food supply and as the most vulnerable in respect to common production menaces and terrorist challenges in particular. It focuses on food quality and safety as the major priority of humanity and the ways of their achievement in the globalizing world starting from the national level plans, decisions and actions. In addition, the connection to the development of tourism in Bulgaria as the most expanding industry in recent years will be considered as well as the importance of risk management in food supply. The following questions are discussed: the importance of agriculture and food safety in the contemporary world; the state-of-art of agricultural production and food safety in the Republic of Bulgaria as a Balkan country and as a member of the European Union; common threats and probable targets of terrorist attacks affecting agricultural and tourism sector and having impacts on food quality and safety; legislation, national and local authorities' responsibilities and competences in forecasting and preventing terrorist attacks, especially those considering agricultural produce and tourist services; recommendations for assuring food security in national and international aspects. The conclusion summarizes the findings concerning current and possible future national contributions to global antiterrorist responses. It will stress the crucial issue of international cooperation in counteracting terrorism threats and attacks.

Keywords. agroterrorism, crisis management, risk assessment, food safety, agriculture

Introduction

The globalization embraces many processes intending to transform current social state in global. New social activities and networks are being created overcoming traditional political, economic, cultural or geographic borders and leading to intensification and acceleration of social activities and exchange. It is a process of historical necessity aiming at sustainable development and improvement in quality of life. The new conditions in the last decades, as business globalization, changes in governmental infrastructures, structural changes in business, new as well as fast changing technology showed that globalization causes not only positive trends but challenges and risks as never before. Thus, the process contains many provocations to national and international security. The changes in national and international security environment in conditions of the general

[1] Corresponding Author: Dr. Ekaterina Arabska, University of Agribusiness and Rural Development, 78, Dunav Blvd., Plovdiv 4003, Bulgaria, e-mail: katya_arabska@abv.bg

globalization impose the necessity to look at the security questions not only in their traditional territorial aspects but as the security of society, families and individuals. The roles of the state and national institutions concern such problems as national security, defense, informational assurance, social order, protection of population and infrastructure, economic security, law order, scientific research, provision of resources, monitoring and control. Under the conditions of globalization the concept of security goes far from the military power but embraces also the social, political, economic and individual elements. Thus, the system of national security embraces political, economic, information, social, military, citizens' protection, social system and ecological security. Sometimes national security is conditionally divided to inner (political, economic, social, informational, citizens, etc.) and outer (political, diplomatic, integration, transorder, international law, etc.). The challenges and threats of the use of mass destruction weapons led to the approach: from guaranteed mutual destruction to guaranteed mutual safety (fig. 1).

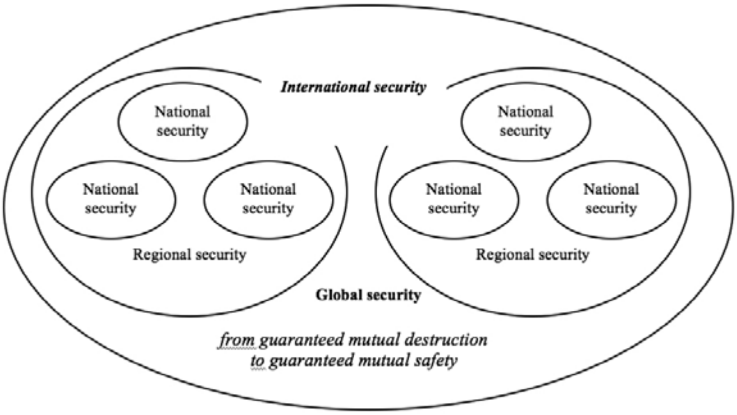


Figure 1. The global security system

Globalization contains common threats and imposes the need of international collaboration. As a result of the state of the global human community, on the one hand, and the biosphere on the other, in the world, a specific security environment is formed understood in its broad aspect. That environment is determined more and more by its parameters of unreliability and crisis [1]. The specificity of the crisis, raised as a consequence of terrorist activities, is usually connected to the surprise and high level of risk. The reaction of the responsible structures is very important and their effectiveness is determined by the preliminary preparation. A specific characteristic for contemporary terrorism is the striving towards high efficiency through detailed planning, good preparation and organization, perfect coordination and synchronization. Faced with numerous challenges, the civilization tries to resist and mitigate the consequences of emerging threats. One of the greatest threats in the world is terrorism in agriculture and food safety. Therefore, agricultural safety starts to be an issue of paramount importance in the counter terrorism community [2]. Biological weapons that target agriculture are relatively simple to acquire, weaponize and use [3]. Biological weapons are disease-causing organisms (or having other effects), products of their activity and the means of their use. Those are special biological agents capable to cause mass and severe diseases in plants, animals and humans. Biological weapons are not just a threat to human health. A terrorist armed with animal or plant pathogens also threatens the livestock, poultry, and crops of the agricultural sector [4]. A biological attack on agriculture may have no human casualties and is therefore less likely to prompt members of the terrorist cell to sabotage the attack. Furthermore, if the terrorists are not using zoonotic organisms, they need not worry about becoming casualties of their own weapons. The fact that the consequences for using a weapon of mass destruction against agriculture are less severe that using one that will inflict mass human casualties allows terrorists who do not wish to sacrifice themselves to employ them [3]. Those weapons are an overlooked class of weapons of mass destruction. Both the potential economic impact of a bio attack against an agricultural target and the cost of the response to this threat suggest a need for better organizational models from the response community [5]. The first important point is to inform the public that scientific evidence about the agroterrorist threat is not enough. The stakeholders have to include the agroterrorist threat in all kind of documents, plan prevention and preparedness measures and start to act proactively [2]. The potential threat of agroterrorism is an additional reason for the international community to invest more resources in activities that are already justified on more general grounds: contributing to the prevention of conflicts and to promoting security, including biosecurity, and assuring food safety and quality in developing countries [6].

The study considers antiterrorism as a part of national and international security assurance and food quality and safety, as it is dealt with terrorist threats in the legislative and strategic documents in the Republic of Bulgaria. That's why in the course of this study the authors examined the strategic and legislative documents in the Republic of Bulgaria in relation to the agroterrorism threats and then make some recommendations for establishing a system in which to be effective and internationally recognized.

1. Agriculture and food safety in the contemporary world - common threats and probable targets of terrorist attacks affecting the agricultural and tourism sectors and having impacts on food quality and safety

The agricultural and food industries are extremely susceptible to agroterrorist incidents because of the geographic concentration, agromovement, and the interrelationship between the agricultural industry and other segments of the nation's critical infrastructures [7]. The importance of agricultural infrastructure is indisputable. The most basic principle that every government should follow to ensure its continued survival is the protection of its citizens while ensuring the fulfillment of their basic needs. At the very lowest level of human existence, the basic needs are food, shelter and water. The validity of the government that fails to provide these needs will soon be questioned by its citizenry [8]. With the development of the international economy, humans, animals and consumer products can travel across the globe within 14 hours. In today's world, extremism and the frequency of international travel make the intentional introduction of foreign disease agents a possibility and unintentional introduction a probability [9].

Agroterrorism is a subset of bioterrorism, and is defined as the deliberate introduction of an animal or plant disease with the goal of generating fear, causing economic losses, and/or undermining stability. Attacks against agriculture are not new, and have been conducted or considered by both nation-states and sub-state organizations throughout history [10]. The majority of researches categorized three types of agroterrorist weapons: invasive plants and animals, pathogens, and toxic chemicals. Terrorists, in their plans, showed the intention to attack the most vulnerable social sector, and agriculture, due to its specific characteristics, is one of those sectors [2]. Benjamin (2011) considers the vulnerability of agriculture in: transportation of food supply; lack of security; plants and animals are susceptible to a larger amount of biological agents; international trade; lack of technology and resources [11]. Attack strategies could be: contamination of livestock or plants; direct contamination of the food supply; contamination of animal feed; contamination of water supply. Plant pathogens: affect production of crops, difficult to identify; only small amounts needed; great economic impact. Contamination of seeds: contamination of seeds with disease causing agents, may cause deformed crops, taint seeds, yield tainted crops; simple attack method. Contamination of water supply: contamination of ground water; dumping of materials that consume oxygen; contaminating groundwater used for irrigation; contamination of water with viruses. In the prevention of attacks some stages are identified: steps to prevention (border inspections, surveillance, adequate knowledge on possible biological weapons, implement biosecurity measures, increased biodiversity, advance technology); coordination between agencies (selection of one lead agency; delegation of responsibilities; interchange of information and resources; coordination of systems); steps to handling an attack (stop the spread of the disease at the source, confinement and eradication of the disease or pest, economic recovery, reestablishment of export and trade markets, rebuilding of confidence in the food market, compensation for destroyed animals to farmers); review (impacts on the economy, reasons why an attack is likely; vulnerabilities within the food supply chain, possible attack methods, prevention steps, handling an attack) [11].

The openness of national economies (especially in agriculture and food production sectors) makes them suitable terrorist targets. The results of an agroterrorist attack may include major economic crises in the agricultural and food industries, loss of confidence in government, and possibly human casualties. Humans could be at risk in terms of food safety or public health, especially if the chosen disease is transmissible to humans (zoonotic) [10]. Agriculture is a soft target, meaning it is largely unprotected, vulnerable to attack and easily interdicted. The effects of such an attack would be compounded if the timing occurred during transport. Not only would the original feedlot be contaminated, and therefore subject to infecting arriving cattle, but also, other feedlots receiving contaminated cattle, the road and rail distribution mechanisms, and slaughter houses. The problem would no longer be localized, very possibly crossing state and regional boundaries [8].

The complexity of biological terrorism targeted at agriculture has been considered through the example of the threats to US national security [3]. In this work it is emphasized that biological weapons targeted at agriculture could cause massive economic damage, special attention is paid to biological weapons that do not kill people and the low probability compared to a bomb. Agroterrorism aims at financial gain rather than to kill as many people as possible. Furthermore, there are low technical barriers to obtain non-human pathogens. The ways to obtain a pathogen are described as: isolate the organism from the environment, order it from a biological collection or laboratory; be given it by a state sponsor – a “shadow” war. The conclusion is that anti-agriculture weapons are easy to be produced but the questions of their virulence spread and lethality still stay.

The tricky question is to define natural or intentional occurrence of plant or animal diseases. But in both cases the preventing and control systems should work. It should embrace domestic and wildlife organisms in the disease control. Bearing in mind the incubation periods and asymptomatic hosts, it could be very difficult to manage a disease, especially when wild animals are reservoirs and the eradication is extremely difficult. Differentiating between a natural and an intentional animal disease outbreak is very difficult [12]. Potential targets include: farm animals including livestock (cattle, swine, sheep, and horses), poultry, and fish; field crops including grain, trees, fruits, and vegetables; processed food; agricultural storage facilities. Independently of the stage of attack (before or after harvest) agroterrorism could affect agriculture and all the sectors of national economy. There are many scenarios that could create major disruptions in the food supply and economics in national and international scope. In addition, the question of consumers' behavior has been concerned too – harmless to people products scaring consumers because they are considered potentially tainted and that way terrorists can create economic disasters. Agricultural pandemics can lead to economic losses of immense proportions [3]. The conclusion points focus on agroterrorism that could disrupt the food supply not only on national and regional aspects. The market could be destroyed for years ahead. That's why the future of terrorism may be not in destroying and killing but in non-lethal ends (vulnerable infrastructures as targets) – property (avoiding human presence) and commerce as targets – financial costs – direct (buildings, equipment, roads) and indirect (insurance recovery, business and tourism). Economic terrorism, incl. agroterrorism and tourism as targets, are among the most probable types but usually financially neglected. It touches one very important point - human food chains. That way it could easily gain one of the main terrorist's goals of publicity – gain the attention for long without killing people, but affecting a broader spectrum – and attracting followers. Measures to prevent and mitigate anti agriculture attacks include prevention (labs, programs), recognition and response to agricultural diseases outbreaks (state agencies to notice, report and react do a disease). The prevention costs are minimal compared to those that should be spent if such events occurred.

However, the general susceptibility of the agriculture and food industries to bioterrorism is difficult to address in a systematic way due to the highly dispersed, yet concentrated nature of the industry and the inherent biology of growing plants and raising animals [10]. The paper accepts the opinion that agroterrorism presents the greatest threat to society as an economic impact weapon. As a vector for attacking a population with disease, bioterrorism has many more efficient vectors of disease distribution than those offered by agriculture e.g. infecting people with a virus on a tube train. However, affecting a population's health cannot be ruled out [13]. Terrorist attacks against the food system can occur in many ways and points across the food supply chain. Terrorist objectives can be confined to causing economic damage, sickness or death to animals, plants and humans or altogether. If the objective is to kill humans, then it is unlikely that the food system would be used as a vector since more powerful biological agents (e.g. anthrax, plague, small pox) than food-borne illnesses or zoonosis are available. In this regards, agroterrorism can be distinguished from bioterrorism in that the former is directed towards economic damage while the latter is a direct assault on human life [14]. The threat of an agroterrorist attack can be countered on four levels [4]: (1) at the organism level, through animal or plant disease resistance; (2) at the farm level, through facility management techniques designed to prevent disease introduction or transmission; (3) at the agricultural sector level, through disease detection and response procedures; and (4) at the national level, through policies designed to minimize the social and economic costs of a catastrophic disease outbreak.

Governments and citizens must be prepared to minimize incidents of national significance or large scale domestic emergencies. This requires emergency management organizations and communities to respond in a timely fashion and perform activities that reduce the consequences of disaster [7]. Addressing the threats of food and agricultural terrorism strategies for counteracting threats should be focused on prevention, surveillance and response, public health and promotion of food safety, biosecurity on the farm, promoting food safety in distribution and retail, promoting food safety at home, etc. Knowing that acts of agroterrorism are both expected and feasible today, prevention, deterrence, preparedness, detection, response, attribution, recovery, and mitigation programs must be altered and based on a better understanding of the threat. There are a number of things that can be done in advance of agroterrorism, none of which are impossible or beyond the current means and abilities [15].

An investigation states that an avalanche of invaluable information and misinformation has been provided to the American public regarding weapons of mass destruction, biological terrorism, biological crimes, and biological warfare [12]. The use of these agents may target civilians, military personnel, and critical aspects of national infrastructure including financial services, computer networks, transportation systems, and water supplies. The study goes deeply into definition, etiology, host range, geographic distribution, transmission and epidemiology, incubation period, clinical signs, pathology, morbidity and mortality, differential diagnosis, diagnosis, control and eradication, zoonotic potential and public health implications for a number of threats.

Attractive features of agroterrorism include its relative affordability or cost-effectiveness, the difficulty in detecting bioagents, the high concentration of livestock in a limited number of places, and the high mobility of animals and animal products. In addition, the terrorist who deploys the bioagent faces limited risks because the pathogens that attack cattle usually do not affect humans. Non-state actors may resort to agroterrorism due to its low costs [5]. Historically, most attacks against agriculture worldwide have been directed at consumer confidence and could more legitimately be described as credible threats than as genuine attacks [16]. Agents and toxins that can cause disease in plants and animals are often easy to employ, spread rapidly through the environment, they are generally safe for humans to handle and have a potential for great economic damage. Terrorists would not only want to create as much damage as possible, but would also want to take credit for the attack in the ensuing media coverage [9]. Agricultural terrorism is viewed as a new kind of war [17] in the food sector and agriculture.

A study concludes that concurrent with the change from small diversified farms to larger, more specialized farms, has been the vertical integration of agriculture. In a vertically integrated system, producers, shippers, processors and often retailers are all part of the same company [9]. There are economic advantages to this business model as well as greater control of product quality and uniformity. Vertical integration provides an opportunity to develop and implement effective biosecurity programs such as Hazard Analysis of Critical Control Points (HACCP), since one management team has control of all aspects of production, processing and retailing to consumers, essentially the ‘farm to fork’ concept. However, there are risks with vertical integration. From an agroterrorism perspective, the danger of vertical integration is that a breach in any part of the system could conceivably affect the entire system, resulting in widespread exposure of consumers to tainted produce and massive financial loss to the company [9].

Agroterrorist attacks can be targeted towards a) production (supply) without causing a behavioral or structural shift in demand, b) consumption (demand) without causing a behavioral or structural shift in supply, or c) both supply and demand [14]. In the

Final summary report of SPPA (September 2005-September 2008) it is stated that it is virtually impossible to guard against all threats to the food and agriculture supply. Food and agriculture industries must anticipate the possibility of a terrorist attack on their products and evaluate their preparedness and mitigation strategies to either thwart an attack or, at the very least, mitigate the damage, and recover from the economic and psychological impact of an attack [18].

Agroterrorism is a threat facing the public today. National response systems are not yet able to perform efficiently and effectively to address this threat. Any locality can be targeted, and the immediate response will come from local entities, regardless of how adequately prepared they are to respond [15]. In the event of a terrorist attack against agriculture, the public will be forced to make life-sustaining decisions in regard to their health, safety and the food they provide to their families. State agencies, special interest groups and the media will have the responsibility of disseminating communication to consumers and producers alike [19]. The threat of terrorist attacks against the agricultural and food system is believed by many to be imminent. But there has been surprisingly little research to determine what the economic impacts of terrorism can be [14]. However, the initial impact of an attack against agricultural infrastructure will be economic in nature [8]. Otto Doering, Purdue Extension agricultural economist, noted that the key determinants of the economic impact are: geography – where and over what area will the outbreak occur; timing – how quickly will outbreaks be detected and dealt with; strategy – what strategy will be used to respond to the outbreak [20].

Discussing the feasibility of an agroterrorist attack, it is stated that the threat of an agroterrorist event hinges on three factors: (1) a terrorist or terrorist group must have the technical ability to acquire and deploy a biological weapon; (2) the terrorist or terrorist group must be interested in infecting or killing animals or crops as a means to its goal; and (3) the terrorist or terrorist group must have the desire to do so using biological weapons [4].

The ways or methods for protecting agriculture infrastructure from terrorist attack and mitigating the consequences of an attack should deterrence fail are addressed in seven areas of effort for combating terrorism: intelligence support, anti-terrorism, counter-terrorism, terrorism consequences management, research and development, international cooperation; public information [8]. The main principle is the prevention which answers the requirements of rationality, competence, efficiency, flexibility, coordination and transparency. The most important factor is information on which basic prognosis and risk and threats analyses to be made for establishment of an early warning system in order to plan, coordinate, prepare and to be ready for adequate reactions. Stages in reaction could be summarized as: immediate reaction, stabilization, recovery.

The connection of agriculture and food supply to the tourism sector is more than obvious. One of the potential effects of agroterrorism that has an economic impact is the deliberate contamination of food in the tourism sector. Outbreaks of foodborne illness can damage trade and tourism and lead to loss of earnings, unemployment and litigation. Food spoilage is wasteful, costly and can adversely affect trade and consumer confidence (CAC/RCP 1-1969) [21]. Tourist streams are an attractive terrorist target and the impact through the food chain could have tremendous effects and spread. The vulnerability of the sector is difficult to measure. A lot of security and preventive measures are directed towards assuring the safety of tourists: physical as a whole and health, including food quality and safety in tourist locations and travels. As potential carriers of harmful agents, tourists passing country borders are an object of border controls, and if needed additional sanitary and medical measures are undertaken. Providing the emotional impact and impacts on the satisfaction level, the aspirations of state and business are towards limiting the negative emotions for tourists and assurance of their comfort. That leads to the establishment of security systems embracing different levels and sectors connected to tourist experiences incorporated in the general security systems. There were no registered cases of food terrorism in the tourism sector in Bulgaria. The most common cases of food poisoning of tourists are related to irregularities in the kitchen which provided the food (for example bad control of incoming food, improper storage of raw materials, a kitchen worker who is unhealthy contaminates, etc.). The opportunities of media reports of food safety incidents, which could seriously harm tourism in a country, should not be underestimated.

The sector analysis of tourism in 2012, made by the Bulgarian National Network for Competence assessment [22], is considered while outlining developments in the field of safety and reflecting the findings of the World Economic Forum. When discussing the increase in tourism indicators the cases that could prevent tourism development should be concerned. Risks related to security in tourism adopt new, unfamiliar, unusual and unpredictable forms, and the industry itself must be able to adequately respond to this challenge. The World Tourism Organization argues that one of the factors limiting the development of the industry is that issues related to security in tourism are not sufficiently regulated. The statistics show that the vast majority of organizations in tourism infrastructure are operating at a loss due to terrorism and natural disasters. Taking into account the growth in demand for international tourism, tourism operators not only in Europe but worldwide should consider a quality tourism product that will meet the security standards [23]. According to the Travel&Tourism Competitiveness Report 2013 [24], safety and security are the critical factors determining the competitiveness of a country's travel and tourism industry. New priorities must necessarily be defined for the safety of tourists. The World Travel&Tourism Council (WTTC) in its Travel&Tourism Security Action Plan [25] offers four key principles: 1) coordinate all policy, actions and communications; 2) secure operating environments; 3) deny terrorists freedom of action; 4) access and work with the best intelligence. Those four principles are mutually supporting. In developing a security policy, adherence to all four is essential for maximum effectiveness, otherwise gaps might appear that terrorists can exploit. The principles are essentially a response to terrorism, rather than a solution. The industry already possesses much of the infrastructure needed to gather and disseminate intelligence, which can counter the menace of terrorism. Through their established commercial networks, with the associated capacity for highlighting regional and local issues and exerting beneficial influence, companies can make a fundamental contribution to the campaign to eradicate global terrorism altogether.

For agroterrorism and terrorism targeted at tourism the main factors determining the high level of the threat could be determined as: high destruction effect using low quantities of specific substances, multiplication, easier transport and spread, difficult to detect, access to technology and ease of production; easier contamination; duration of the effect and difficulty to manage the diseases; impossibility to detect by human sense; low probability to identify and catch the performer – enough time and opportunity to leave the place; low costs.

Based on the above review, the authors propose a scheme of the process for addressing and counteracting the threats in food safety (fig. 2).

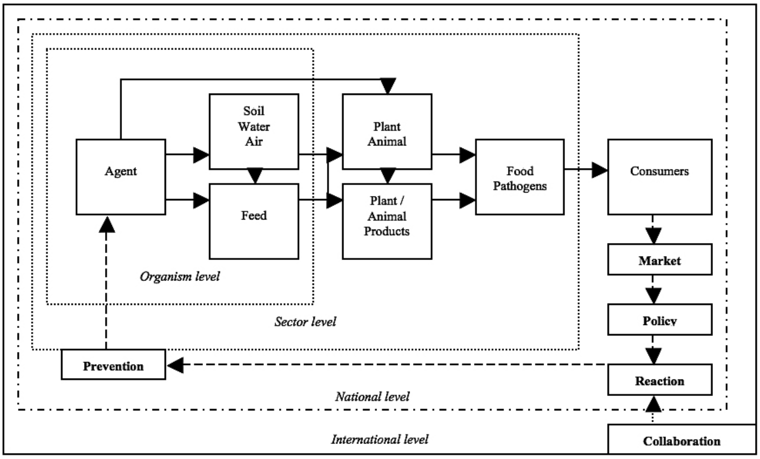


Figure 2. Addressing and counteracting threats in food safety

2. Legislation, national and local authorities' responsibilities and competences in forecasting and preventing terrorist attacks, especially those considering agricultural produce and tourist services as part of the critical infrastructure in the Republic of Bulgaria

The legislative, strategic and other documents of the Republic of Bulgaria reviewed in the study are the following (ordered in alphabetical order): Action plan of the National Rural Network 2009 – 2015, Ministry of agriculture and food of the Republic of Bulgaria, Animal breeding law, Annual report for the implementation of the common long standing plan of control of food, feed, animal health care and human attitude and plant protection 2010, Ministry of agriculture and food. Annual report for the state of development of agriculture (Agrarian report) 2013, Ministry of food and agriculture of the Republic of Bulgaria. Bulgarian food safety agency law and Rules of the structure of Bulgarian food safety agency (2011), Constitution of the Republic of Bulgaria, Environmental protection law, Feed law, Food law, GMO law, Law for the implementation of the common organization of agricultural markets of the European Union, Law of Advisory council for national security, Law of defense and armed forces of the Republic of Bulgaria, Military doctrine of the Republic of Bulgaria, Ministry of interior law and the Rules of its application, National plan for disasters management, Sofia, 2010, National plan for terrorism counteraction, Plan for crisis management as a result of terrorist activity, Sofia 2008, Plan for implementation of the Strategy for development of voluntary formations for protection in case of disasters, fires and other extraordinary situations in the Republic of Bulgaria (2013-2020), Plant protection law, Strategy for development of voluntary formations for protection in case of disasters, fires and other extraordinary situations in the Republic of Bulgaria (2012-2020), Strategy of the national security of the Republic of Bulgaria 2020, Tourism law, Veterinary activity law. All these are published on the web-sites of the relevant institutions [26-30].

According to the definitions part in the Law of Defense and Armed Forces of the Republic of Bulgaria: the critical infrastructure is a system of equipment, services and information systems of which the ceasing, incorrect functioning or destruction of would have a serious negative impact on the population's health and safety, the environment, the national economy or on the effective functioning of state governance.

In the National Plan of Crisis Management of the Republic of Bulgaria it is written that terrorism is a consciously created social event which serves itself with fear by means of violence or threat of violence in order to achieve a political change and / or significant negative impact on stocks important for the state and society. Unlike illegal armed structures and criminal intent, terrorism is characterized by some specific features among which are: political motives; violence or violent threats aptitude; the activity is intended to find lasting psychological effects exceeding the direct goal/s; the consequences have great economic impacts, etc. Modern terrorism entered in a new stage in its development because of the globalization processes embracing the whole world. New information and communication technology provide opportunities for both terrorist and antiterrorist actions. Already far away of concrete political goals in a concrete country or region, it impacts international relations, especially the economic stability and psychological influence on a population in a broad territorial scope. At its new stage of development, terrorism is identified as an international event. As with globalization, it is a social event / crisis which should be understood in order for society to properly react. Specific crisis threats could be natural events or human activities. Terrorism is put in the second group. The antiterrorism considers detection, ceasing and consequence mitigation. The most effective are the first steps because the economic consequences afterwards reflect on lost produce value; managing diseases costs; quittances; markets loss; dependent business – supply, processing, trade, tourism; consumer trust; consumer confidence in government, etc.

When investigating responsibilities and competences in forecasting and preventing terrorist attacks, especially those considering agricultural produce and tourist services, the authors examined legislative and strategic documents having relation to anti-agroterrorism bearing in mind that agriculture is part of the critical infrastructure and an important object of national and food security measures, i.e. national security. The documents are discussed below in different aspects: national security assurance and food safety. The general questions concerning national security are set in the main law – the Constitution of the Republic of Bulgaria. From the point of view of the national security, the defense is part of it as is set in the Law of defense and armed forces of the Republic of Bulgaria. The activities are in conditions of collaboration with NATO and European security and defense policy, laws and international agreements. The goal is to create, sustain and use the resources for stable security environment. In connection to that, the armed forces could participate in disaster management. The tasks are implemented on the basis of strategic and operational plans. For the current research, it is important to notice that in time of peace they participate in such activities as preparedness for risks and threats, humanitarian aid and rescue missions, preparation and foundation of units for conducting rescue and urgent actions for overcoming disasters, etc. Another state structure having competences in the field is the Ministry of Interior whose activities are directed towards the protection of citizens' rights and freedoms, national security and social order.

From the point of view of food safety, the most important document is the Food law which arranges the requirements towards food, measures and conditions for assurance of food hygiene and safety, packaging, labeling, marketing, etc.; all stages in production, the processing and distribution of food; control; functions and competencies of professional organizations of food producers and the Bulgarian Association of food and drink Industry. Its scope does not cover the food production and preparation for personal needs and consumption. The goal of the law is to guarantee the observance of the legislative requirements in food production and trade in respect to the protection of health and rights of consumers, as well as to provide the application of the EU regulations in the field of food quality and safety. The Minister of agriculture and food and the Minister of health care conduct the state policy in the field of food safety. Other relevant laws are: Plant protection law, Feed law, Animal breeding law, Veterinary activity law, Environmental protection law, GMO law, Law for the implementation of the common organization of agricultural markets of the European Union and a number of regulations, instructions and other documents created on the basis of the primary laws. Tourism law regulates social relations connected to the management and control in the tourism industry, the interactions with the state and municipalities during tourism activities' implementation and mostly indirectly addresses the issue.

The strategic documents published on the Internet portal of the Council of Ministers for public consultations (http://strategy.bg) were examined and especially some strategic documents having relation to the topic discussed as: Strategy of the national security of the Republic of Bulgaria 2020, National plan for terrorism counteraction, National plan for disasters management, Plan for crisis management as a result of terrorist activity, Military doctrine of the Republic of Bulgaria, Strategy for development of voluntary formations for protection in case of disasters, fires and other extraordinary situations in the Republic of Bulgaria (2012-2020) - all dealing with the examined questions according to the main laws.

From the point of view of food security measures some structures should be underlined as the key actors. The Ministry of health care and the regional health inspections accomplish the human health policy as a whole but focus on more general issues and contemporary medicine. Bulgarian food safety agency is the state body having competences in relation to food quality and safety over the whole food chain executing the official control over: phytosanitary activities; plant protection products, fertilizers, soil improvers, biologically active substances and food substrates; veterinary activities, identification, health protection and human attitude towards animals; disinfection, disinsection, deratisation, etc.; raw materials and food, excluding bottled natural mineral, spring and table waters; waste animal products, not intended for consumption by humans and the products derived from them; feed; GMO and products containing, consisting or produced of GMO; materials and equipment in contact with food; the correspondence of fruit and vegetables quality to EU requirements. Bulgarian food and safety agency also implements a number of activities as food quality assessment; laboratory and diagnostic activities, scientific research; risk assessment and communication; trainings and qualification. According to the Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety [31] Rapid Alert System for Food and Feed (RASFF) has been created which allows for the fast exchange of information about the risks and the measures – undertaken or to be in order to overcome the risks. The national rural network, as a partner of the Ministry of agriculture and food of the

Republic of Bulgaria, provides an exchange of information and experience, the transfer of good practices and joint partners' actions. In that way it is directly or not involved in the agroterrorism response system.

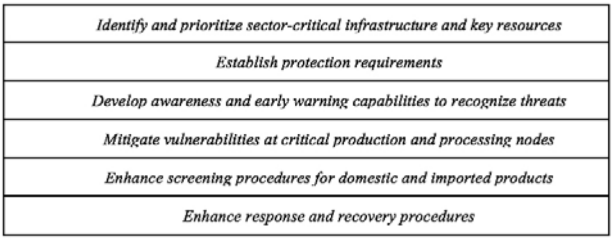
There are yet a number of legislative and strategic documents, some of them being too general, but some containing concrete measures and actions and point out responsible authorities and institutions. Although at first sight it is difficult to understand how so many documents and institutions work together, it is obvious that all those have worked well in prevention till now. An Annual report of the Ministry of agriculture and food for the implementation of the common long standing plan of control of food, feed, animal health care and human attitude and plant protection is prepared in accordance to the Regulation (EC) 882/2004 [32] and presents the progress in the plan stated above, as well as assessments of the effectiveness of the conditions and the systems of control based on the results and consequences of the official control in the Republic of Bulgaria. Its scope is the following: food safety, feed safety; animal health care and human attitude; plant protection. The report contains extended data on control, monitoring programs and the work of the competent bodies and institutions, nonconformities and risk analyses. In the focus is the animal health care, which is put in the main priorities, and is a subject of special audit and control procedures. Additionally, it is difficult to find plans, concrete funding instructions, etc. and reports for the implementation of strategic documents, the few reports (Agrarian report of the Ministry of agriculture and food and the above paragraph's stated report) show that the prevention system perhaps works. Based on the main problems faced by the country in recent years from the economic point of view (lack of finances for state activities), and particularly by the agricultural sector, the authors state that the economy and infrastructure in the country as a whole are not prepared for a terrorist attack if it happened.

3. Recommendations for assuring food security in national and international aspects

The investigation of strategic and legal documents showed that food security should be set as a part of national security in a formal way. The main recommendation is for agroterrorism threats to be recognized officially by the state, assuring interagency coordination and effectiveness of work and preparedness, one key issue of which is funding. Being the most important part, prevention should include both planning and preparation (structures, population, infrastructure, resources, laws, etc.). Local communities should be actively involved in prevention through an early warning system. Thus informational campaigns and modules should be planned and funded too. They should stress environmental management and risk assessment. Establishing networks would be an easy way to unite and coordinate the efforts of all – state, business, non-governmental organizations, media and individuals. Producers, processors and traders should be convinced of the importance of prevention which is usually financially neglected. The laboratories for diagnosis and applied research must work in close cooperation with farmers, processors, traders and consumers who should be provided with information for such labs and the ways of giving feedback.

The state's efforts in assuring food quality and safety meet the problems of limited funding. Furthermore, stakeholders as a whole suffer financial problems and rely on the support of European funds. Counteracting systems should embrace the following activities: deterrence and prevention, detection and response (laboratories, research, state and local authorities, competent bodies); recovery and management.

The safety system (preventing and counteracting) should reduce the vulnerability to agroterrorism and minimize the damage from potential threats. There is a need of industry vulnerability assessments and advice. Multiple points of access in the farm to fork continuum must be monitored. Bearing in mind that possible contamination is difficult to monitor, even accidental contamination can result in widespread outbreaks. Rural emergency planning (fig. 3) should be the first step in setting up an integrated disaster management strategy in agriculture and tourism (fig. 4). The process of management in crisis in agriculture and tourism is proposed in fig. 5.



Identify and prioritize sector-critical infrastructure and key resources
Establish protection requirements
Develop awareness and early warning capabilities to recognize threats
Mitigate vulnerabilities at critical production and processing nodes
Enhance screening procedures for domestic and imported products
Enhance response and recovery procedures

Figure 3. Rural emergency planning

<table>
<tr><td colspan="4">Decision taking èAction</td></tr>
<tr><td rowspan="8">Deterrence
Resilience
Recovery</td><td>Prevention & Deterrence</td><td>Knowledge of threats
Vulnerability analyses
Risk assessments
Preventive actions</td><td rowspan="6">Information
Communication
Coordination
International collaboration</td></tr>
<tr><td>Food safety in:
- production - trade
- processing - tourism
- distribution - home</td><td>State and local authorities
Business / Stakeholders
Civil society
Consumers</td></tr>
<tr><td>Surveillance & Response</td><td>Monitoring
Identification of threat / risk / exposure
Reaction</td></tr>
<tr><td>Biosecurity on the farms and tourist objects</td><td>Status
Control</td></tr>
<tr><td colspan="2">Critical nodes</td></tr>
<tr><td>Report</td><td>Inform / Analyze / Recommend</td></tr>
<tr><td colspan="3">Mitigation & Recovery</td></tr>
<tr><td>Mitigation recommendations</td><td>Research gaps and needs</td><td>Assessment
Observations</td></tr>
<tr><td colspan="4">Detection &Preparedness</td></tr>
<tr><td colspan="4">Preventive and operative measures</td></tr>
<tr><td>Organizational managerial</td><td>Political</td><td>Information
Communication</td><td>Law</td></tr>
<tr><td colspan="4">International collaboration</td></tr>
</table>

Figure 4. Strategies that should be integrated for counteracting threats in agriculture and tourism

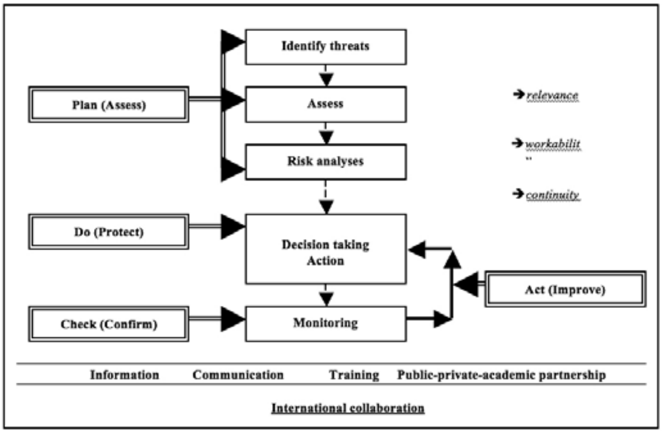


Figure 5. The process of agriculture and tourism crisis management

4. Conclusion

The national security of any country is in close connection to regional and international security. There are many opportunities and readiness for globalization in the interactions and collaborations in the sphere of agriculture and tourism security including the military sphere. The development of a new international architecture of security and defense is a fact with the common goals to answer properly the challenges and threats to international stability. Each country builds its own security system without threatening that of other countries, reflecting geographical position, historical, demographic and other conditions and optimal use of available resources through a number legislative documents, strategic documents, plans, research, information systems, early warnings systems for achieving preparedness and aiming at public health.

The study shows that the establishment of the national safety system in the field of agriculture and tourism is based on the following principles: assuring physical safety – safety in work with pathogens and toxins, protection of infrastructure, epidemic control, and the early diagnosis of diseases, prevention products and medicines. In Bulgaria the term 'agroterrorism' was noticed only in mass media as a threat. The analyses made in the progress of the investigation of the legislative and strategic documents of the Republic of Bulgaria show that in none of those examined was the term agroterrorism discussed. Terrorist threats are usually determined very broadly and in many cases in the scope of disasters and crisis management. Issues being faced: food safety and consumer confidence; security of farms and processing facilities; transportation security; plant and animal disease outbreak detection; public, government, and industry education and preparedness, etc. That way in the Republic of Bulgaria, an extended law system concerning indirectly the issue of anti-agroterrorism has been created focused on preventive measures and effective mitigation if dangerous events occur. The fact that there is no evidence of mass terrorist invasions in the country could be discussed on one hand that the system is well-planned and properly working by inclusion of many state and non-state structures communicating effectively between each other and providing enough information for citizens. But is it the case? The relations and connections as stated in all the documents are very difficult to follow and summarize the responsibilities and competencies. The information provided in some reports show that a number of threats and risks (not accepted as terrorist attacks but as threats to food quality and safety) have been managed – the prevention is good, but that does not mean that in case of a terrorist attack all that will do. The recent years' problems in the country, mainly funding of state activities, as well as some reactions to natural disasters, showed that although broad legislation and structures, the reactions are slow and lack information and good communication (especially important are those in which the local culture and traditions are concerned).

Of course, it is impossible for a single country to manage self-dependently the risks and threats in contemporary globalizing world. They are influenced by many factors, high dynamics, indefiniteness, ambiguity and too complicated for prognoses processes. The importance of international organizations – preventive diplomacy, crisis management, post conflict stabilization, etc. is commonly accepted. In all the documents the Republic of Bulgaria states the will to contribute to regional and international security and recognition of the country as one of the key factors in the stability in South-East Europe. So, the process of preparing and developing documents is in close connection to international agreements the country has signed and the membership in the EU. Among the important factors are: geographical distribution of agriculture and tourism, transportation, science, information, communication, etc. Sometimes this occurs as the main problem – in striving after answering international requirements; national characteristics that should be reflected are neglected. On the other hand, the international collaboration and experience exchange are invaluable tools in national and regional development in conditions of globalization and common good will for sustainable development.

References

[1] Milushev L. (2007) *Crisis – managerial aspects and opportunities*. Europress, Plovdiv.

[2] Radović V. (2012) The mitigation of agroterrorism threat in the Republic of Serbia, In: *Managing the Consequences of Terrorist Acts - Efficiency and Coordination Challenges*. Ed. Denis Čaleta, Paul Shemella. Institute for Corporate Security Studies-ICS, Ljubljana, Slovenia, and Center for Civil Military Relations , Naval Postgraduate School Monterey, USA, 2012 M 14.

[3] Casagrande R. (2000) Biological terrorism targeted at agriculture: the threat to US national security, *The nonproliferation review / fall-winter 2000*, 92-105.

[4] Kohnen A. (2000) Responding to the threat of agroterrorism: Specific recommendations for the United States Department of Agriculture. *BCSIA Discussion Paper 2000-29, ESDP Discussion Paper ESDP-2000-04*, John F. Kennedy School of Government, Harvard University, October 2000.

[5] Polyak M G. (2004) The threat of agroterrorism, economics of bioterrorism, *Business&Finance, Summer/ Fall 2004*, 31 – 38.

[6] Linacre N. A., Koo B., Rosegrant M. W., Msangi S., Falck-Zepeda J., Gaskell J., Komen J., Cohen M. J., Birner R. (2005) Security analysis for agroterrorism: applying the threat, vulnerability, consequence framework to developing countries, environment and production technology division, *August 2005 EPT Discussion Paper 138*, International Food Policy Research Institute.

[7] Dykes J.P. (2010) *Agroterrorism: Minimizing the consequences of intentionally introduced foreign animal disease*, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, AY 2010.

[8] McNeely K. A., Powers J.F. (2001) Agricultural terrorism: breaking new ground, *USAWC strategy research project*.

[9] Herrmann J. A. (2013) Agricultural terrorism - the US perspective, *Food Safety and Public Health 36*, 296-376.

[10] Monke J. (2005) Agroterrorism: threats and preparedness, *CRS Report for Congress, updated February 4, 2005*, Congressional Research Service, The Library of Congress.

[11] Benjamin T. (2011) *Agroterrorism: Preparing for an attack*, Walden University.

[12] Wilson T. M., Gregg D. A., King D. J., Noah D. L., Perkins L. E., Swayne D. E., Inskeep II W. (2001) Agroterrorism, biological crimes, and biowarfare targeting animal agriculture. The Clinical, Pathologic, Diagnostic, and Epidemiologic Features of Some Important Animal Diseases, *Clinics in laboratory medicine, volume 21, number 3, September 2001*, 549 – 591.

[13] Byrne R. (2007) *Agro-terrorism and bio-security, threat, response and industry communication*, A Nuffield Farming Scholarships Trust Award 2007.

[14] Turvey C. G., Mafoua E., Schilling B., Onyango B. (2003) Economics, hysteresis and agroterrorism, *Principal Paper Presented at the Canadian Agricultural Economics Society 2003 Annual Meeting Montreal*, Quebec, July 27-30, 2003, Food Policy Institute Working Paper No. WP0703-011.

[15] George A.M. (2007) Response is local, relief is not: the pervasive impact of agro terrorism, *Vanderbilt journal of transnational law Vol. 40:1155*, 1155-1170.

[16] Pate J., Cameron G. (2001) Covert biological weapons attacks against agricultural targets: Assessing the impact against U.S. agriculture, *BCSIA Discussion Paper 2001-9, ESDP Discussion Paper ESDP-2001-05*, John F. Kennedy School of Government, Harvard, University, August 2001.

[17] Byrne R. (2011) *Agricultural terrorism and the US response system*, Centre for Rural Security, Harper Adams University College, Shropshire, TF10-8NB, United Kingdom, RJB Biosecurity Seminar, Keele May 2011.

[18] Strategic Partnership Program Agroterrorism (SPPA) Initiative final summary report September 2005 – September 2008. December 2008.

[19] Ashlock M. A. (2006) *The uncertainty of agroterrorism: a study of Oklahoma beef producers' risk perceptions, information sources and source trust in the pre-crisis stage*. Oklahoma State University

[20] Cain S. (2001) Agroterrorism, A Purdue Extension backgrounder, Compiled by Steve Cain, Purdue Extension Specialist.

[21] General Principles of Food Hygiene, CAC/RCP 1-1969. Available at: http://www.codexalimentarius.org/standards/list-of-standards/en/.

[22] National Network for Competence Assessment: http://www.competencemap.bg/

[23] Minchev D., Binev D. (2010) Providing Training on Safety and Security in Tourism Developed within an European Project "TSST", *Journal Business Directions, Burgas Free University, issue 1-2*, p. 152.

[24] Travel&Tourism Competitiveness Report 2013. Available at: http://www3.weforum.org/docs/WEF_TT_Competitiveness_Report_2013.pdf.

[25] Travel&Tourism Security Action Plan. Available at: http://www.ontit.it/opencms/export/sites/default/ont/it/documenti/archivio/files/ONT_2003-01-01_00155.pdf.

[26] Council of Ministers Internet portal for public consultations: http://strategy.bg/

[27] Ministry of interior: http://www.nspbzn.mvr.bg/

[28] Ministry of agriculture and food: http://www.mzh.government.bg/

[29] Bulgarian Food Safety Agency: http://www.babh.government.bg/

[30] National rural network: http://www.nsm.bg/

[31] Regulation (EC) No. 178/2002 of the European Parliament and of the Council laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety.

[32] Regulation (EC) No 882/2004 of the European Parliament and of the Council of 29 April 2004 on official controls performed to ensure the verification of compliance with feed and food law, animal health and animal welfare rules.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015

© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-167

Safety & Security Assessment to Prevent a Terrorism Attack in the Centralized Facility for Radioactive Waste Management in Albania

Luan QAFMOLLA[1]
Institute of Applied Nuclear Physics (CANP), Tirana, Albania

Abstract. In the last decade, substantial progress has been made in improving safety & security for nuclear material worldwide, both by states' own domestic actions and through international cooperation. Al Qaeda has continuously expressed interest in unleashing radiological terrorism by building and using radiological dispersal devices (RDDs), known as "dirty bombs" for instance. Common radioactive materials, such as commercial radioactive sources used in medicine, industry scientific research could fuel RDDs. Since 1998, in Albania a special centralized building exists for radioactive waste management and as a temporary storage facility situated inside the INP territory. Radioactive waste conditioned with or without shielding was successively placed into this building for long-term storage. So far, there have been several incidents worldwide with terrorism potential that involved nuclear waste materials and radioactive materials and its repository facilities, which may serve as a target by attacks of terrorism. DU was also feared to causes environmental contamination through it being spread, especially in territories and borders of our countries involving the risk and injuring of the civilian population.

Keywords. safety and security, radioactive waste, radiological disperse device

Introduction

In Albania a special centralized facility exists for radioactive waste management and temporary storage situated inside the IANP territory, as well as a radiopharmaceutical Lab established since 1998. Radioactive waste conditioned with or without shielding was successively placed in the drum until an activity of about 20 GBq was reached. Large amounts of big radioactive sources used in research, industry, medicine, and the army are stored in the interim storage facility in IANP.

The designs of the facilities were intended for temporary storage of significantly smaller amount of radioactive material, as well as Spend High Activity Radiation Sources (SHARS), which are used usually in tele-therapy devices, semi industrial irradiators and in radioisotope thermoelectric generators like: ^{60}Co, ^{137}Cs and ^{90}Sr with activity some thousands TBq reached.

Factors determining the security risk to a type of radioactive source include: prevalence of use, radioactivity content, contamination level and portability. Generally, the most prevalent, radioactive, portable, and dispersible sources, the higher security

[1] Corresponding Author: Dr. Luan Qafmolla, Institute of Applied Nuclear Physics (CANP), Tirana, Albania, e-mail: l_qafmolla@hotmail.com

risk present. For instance, cesium chloride containing relatively large amounts of radioactive cesium ^{137}Cs, and consisting of an easily dispersible powder would definitely be categorized as a high security compound. If this material were also housed inside a portable container, a thief or terrorist could readily seize and transport the radioactive source if adequate security measures are absent.

The radioisotopes of highest security concern include the reactor-produced americium-241, californium-252, cesium-137, cobalt-60, iridium-192, plutonium-238, and strontium-90, as well as the naturally–occurring radium-226.

For the moment, our centralized facility stores some tenth-conditioned drums. We have conditioned by Oncological Hospital some pieces of ^{137}Cs, with initial activity A≈0.55 GBq for each of them. A manual device with five ^{137}Cs spent sources with total activity A_t= 18.5 GBq was conditioned and also generated by the oncological hospital. In December 2006 was conditioned and stored in centralized repository facility a spent source ^{60}Co tele-therapy with activity A= 92.5 TBq. In this building were conditioned some metal scraps contaminated with strontium-90, Iridium-192, americium-241 etc., generated by Albanian private and public companies. Regulatory agency (authority) has also place emphasis on focusing on safety and security enhancements on this class of radioactive sources used in Albania.

1. Establishing a layered and integrated safety and security System

Perfect safety and security systems do not exist, but Albanian authority tends to overact by plugging the exposed gap in the system while often neglecting other gaps. A layered system means that multiple barriers are in place to lessen the likelihood of a radiological terror act. Added layers would frustrate terrorists' attempts to break through the security system. An integrated security system means that adequate layers of safety and security protect every stage of a high-risk radioactive source's lifecycle from cradle to grave. This lifecycle begins with radioisotopes production in research reactors, accelerators or radiopharmaceutical Labs etc., as first stage, continuing with their transport at the end users in an application, such as food irradiation, medical instrument sterilization, cancer treatment at a hospital, industrial radiography, scientific research at a university, etc.

Since 1998, a building has been constructed as a centralized waste management facility, based on the IAEA reference design for such components facilities. The Technical Cooperation with ALB/4/008 IAEA Project, untitled "Upgrading of Radioactive Waste Management in Albania", was development during the years 2003-2004 [1, 2]. During this period an IAEA mission defined the needs for equipment to improve the waste management processes in that facility.

In our centralized radioactive waste management facility all entries to the operated, storage and disposal areas of building are protected with security locks, a PIN Code, a magnetic panel, as well as with alarm systems, which are connected to a central system alarm at the main safeguard building. There is a fire brigade with radiation protection training present in IANP, which is on duty during working hours. Outside working hours there is police officer present on the site. Also, some improvements need to be taken into consideration for more safety and security in infrastructure of our system:

1. The RAW management Lab & Interim Storage Facility is the main centralized site / center to the whole country for the processing and storage of radioactive

materials and wastes, which needs to be implemented in a secure infrastructure and system.

2. The procedures to secure spent high radiation sources or indeed any other radioactive material stored in this facility, often requires the use of highly-expensive, specially trained staff that in this context need to be improved / upgraded for more security in our case.
3. The infrastructure of Albanian's borders to monitor / check the penetrating of smuggling / illicit trafficking of the radioactive material / spent radiation sources by neighbor countries like: Kosovo, Montenegro or Macedonia is limited but a terrorist attack can always happen.
4. A regional infrastructure strengthened, including the Albanian territory, to help and to solve the problems associated with disused / spent sealed radioactive sources during an emergency situation under / after a terrorist attack in our and regional countries needs to be implemented.

The safety assessments to the centralized facility and for the planned waste storage operations were undertaken. This was performed on the basis of an assessment of the potential impacts of the waste management at this facility to workers and to the public and addressed engineering aspects, as well the management regime required for a safe operation of the facility [3]. To perform this assessment the following topics are addressed:

- Assessment of whether the facility is general suitable for safe waste management;
- Assessment of the potential hazards to workers and to the public;
- Evaluation of the safety of the present system (building, characteristics, used material etc.) and of the planned waste management operations based in the international, specialized organization requirements and identification of possible deficiencies;

2. Centralized Waste Management Building in IANP

The dimensions of this centralized waste management building are 16 x17 x 3.20 meters and contain the following areas:

- waste reception area for checking the kind of wastes and their documentation,
- two temporary decay-storage areas for solid waste and spent radioactive sources,
- operational area for the storage of the delivered waste prior to their conditioning, selection and for the manipulation of conditioning of the waste,
- storage area with dimensions 16 x 7 x 3, 20 meters to store 200 liter standard conditioned drums, which will last until about 2040.

The facility represents a solid concrete construction with outside walls of a thickness between 20 and 40 cm. All main entrances to the facility are protected with double security locks. There exists an alarm system, which is monitored by cameras at the main entrance of the Institute by policeman. The position of the waste management facility is indicated. The three adjacent buildings are the neutron generator (10 m distance) and Van de Graf accelerator and Food Irradiator source ^{137}Cs are in 20-meter distance. These buildings have reinforced concrete structures.

Behind the fences of the IANP a residential area begins. The closest buildings are at a distance of 60-80 m. The fence separating these building from the site has a height of 2, 5 m., but the fence needs security improvements [4].

The seismicity of the IANP site belongs to the VIIth degree of MSK-64, so that potentially severe impacts can be avoided by an adequate design of the building structure. The waste management facility has been designed for the VIIIth degree of seismicity MSK-64; therefore no detrimental impacts from earthquakes are to be expected. There are no faults close to the site and geo-technical conditions are appropriate. In the site vicinity are no major industries with a risk of explosion. There is a sufficient distance from railway lines and the airport (over 10 and 20 km., respectively). Policemen permanently guard the IANP site for 24 hours and visitors are checked and accompanied by the staff of the institute. At night two policemen are on duty.

Exposures from incidents and accidents are addressed in the emergency response planning, ensuring that adequate responses are taken. Security technologies and systems are evaluated in terms of current and long-term impacts. Security technology has a very important role in creating more secure facilities and we need to invest precious resources in more secure facilities and greater physical protection and better protection of our vital information system [5]. Though these challenges appear daunting, prioritizing security improvements on high-risk radioactive sources will make great strides toward reducing the risk of a radiological dispersal device attack by terrorists.

3. Recommendations

Recommendations for further development of the waste management concept are given, addressing the safe operation of waste processing and storage. The recommendations derived from the assessment of the current situation and of the plans for the further development of strategies and procedures are:

- Although a substantial degree of the physical protection is provided in the current situation, improvements should be considered. An important step could consist in the installing of a new sounding and lighting alarm system, which will notify the guards of any attempt to enter the waste storage building. The physical security of the waste storage building should be integrated into the planned project to upgrade the physical protection of the IANP.
- Appropriating the main facilities into the IANP territory, this should be included into the already existing emergency plans from Albanian government.

References

[1] Tec-Doc No. 806, International Atomic Energy Agency, Vienna, Austria, 1995.

[2] Safety Standard Series WS-R-2, Predisposal Management of Radioactive Wastes Including Decommissioning, International Atomic Energy Agency, Vienna, Austria, 2000.

[3] Safety Standard Series WS-G-2.5, Predisposal Management of Low and Intermediate Radioactive Waste International Atomic Energy Agency, Vienna, Austria, 2003.

[4] Albanian Academy of Science, Institute of Nuclear Physics, “Strengthening of Agricultural, Industrial and Medical Uses of Isotopes by Means of a Research Reactor”, Tirana, Albania, 1989.

[5] NSS No. 11, Model Regulations for the Security of Radioactive Sources during Manufacture, Use, Storage and Transport, IAEA, Vienna,, Austria, 2009.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015

© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-171

Bioterrorism as a Threat to Food Supply Systems

Elizabeta RISTANOVIĆ [a,1] and Sonja RADAKOVIĆ [a]
[a] *University of Defense, Belgrade, Serbia*

Abstract. Bioterrorism presents the use of microorganisms and their toxins as agents in terrorist actions in political, economic, religious, ideological or other purposes. Today, in the changing world of many contradictions bioterrorism is a real challenge for many non-state and state actors. The main target of bioterrorist acts are humans while a critical infrastructure can be used as a target depending on its impact on life and everyday activities. Among them, food supplies and distribution systems are extremely important and their deliberate contamination as a part of terrorist action is a real threat that can cause even global and serious health, ecological, economic and political consequences. Most health professionals have limited knowledge in the recognition of diseases from either natural or intentional contamination of food. They are not trained to respond appropriately to a terrorist assault for management of the consequences. Outbreaks of both unintentional and intentional food-borne disease can be managed by the same mechanisms contained in a crisis management plan. So, in order to be prepared for any incidents of food and water terrorism, it is essential to establish procedures, plans, to train the experts and to improve response capacities. The other subjects of society, especially decision makers as well as security professionals must also pay more attention to this problem in order to prevent it.

Keywords. bioterrorism, microorganisms, toxins, food-borne, water-borne diseases

1. Food supply as a target for potential terrorists

Attacks upon an enemy's food supply have been used since the time of the Ancient Greeks. Today it is a real and current threat and challenge for terrorists, criminals and other anti-social groups. This statement can be documented by many examples from our time.

So, in an intentional attack in the US in 1984, 751 people became sick after members of a religious sect infected 10 Oregon salad bars with salmonella. Their aim was to incapacitate people and prevent them to vote at local elections. In January 1998, Thomas Leahy was sentenced to 6 years in Federal prison for having made deadly agents in his laboratory (i.e.ricin, *Clostridium botulinum* and weaponized nicotine sulfate). Starting in the fall of 2001 and continuing into the spring of 2002, bulk milk tanks on 14 dairy farms in the US were contaminated with antibiotics as a "test" of the feasibility of an attack using the milk system as a delivery vehicle. In China in 2002 a business owner poisoned hundreds and killed 77 persons by spiking his competitor's baked goods with tetramine-based rat poison. The contamination of 200 lbs of ground beef with an insecticide containing nicotine (Black Leaf 40) by a disgruntled employee in a supermarket in Michigan in 2003 results in 111 ill, including 40 children and the recall of 1,700 pounds of ground beef. The employee was sentenced to prison [1].

[1] Corresponding Author: Dr. Elizabeta Ristanović, University of Defense, Belgrade, Serbia, e-mail: elizabet@EUnet.rs

According to the World Health Organization (WHO), **food terrorism** is defined as the deliberate contamination of the food or water supply. The food supply system is the most complicated of all industrial or infrastructure-related activities in the world, and has a global impact. Trends in global food production, processing, distribution, and preparation present new challenges to food safety. Food grown in one country can now be transported and consumed halfway across the world. People demand a wider variety of foods than in the past; they want foods that are not in season and often eat away from home [2].

Food can be used to spread chemical, biological or radio nuclear agents. Deliberate contamination of food can occur at any vulnerable point along the food chain. Food attacks can have great consequences on human and animal health (disease and death), public health services, economics and trade, as well social and political implications. The safeguards and many points of inspection and monitoring already in place would likely prevent contaminated food from reaching and affecting large numbers of consumers.

Contaminating food does not require as much technical skill and organization as do microorganisms used as a weapon. Terrorists could introduce an agent during the harvesting, packing, shipping, delivery, or preparation stage.

Otherwise, food-borne illnesses are more common than most people realize. Thousands of outbreaks of disease occur annually among humans, domestic animals, crop plants, and wild animals and plants. The causes of food-borne illness include viruses, bacteria, parasites, toxins, metals, and prions. More than 200 known diseases are transmitted through food. According to the CDC, there are approximately 76 million illnesses; 325,000 hospitalizations; and 5,000 deaths every year due to naturally occurring food borne illnesses in the United States [3]. The symptoms of food-borne illness range from mild gastroenteritis to life-threatening neurologic, hepatic and renal syndromes. The exact numbers are unknown because many people just wait for their symptoms to go away and do not go to see a doctor or the doctors don't report it to the health departments

Terrorist attacks can be difficult to distinguish from natural events considering the number and variety of human food-borne illnesses coupled with crop and livestock diseases. Deliberate contamination of food might, in some regards, be easier to control than attacks through air or water. The safety of food is closely controlled in many developed countries, both by the government and the private sector. Food safety infrastructures offer a means for preventing and mitigating sabotage of the food supply.

At the same time, many developing countries which lack basic food safety infrastructures are highly vulnerable to deliberate acts of sabotage. On the other hand, food is also one of the most vulnerable vehicles for intentional contamination by debilitating or lethal agents. The diversity of food sources, including the global market, makes prevention difficult [4].

2. Food bio-terrorism

Food bio-terrorism is defined as an act or threat of deliberate contamination of food (including water used in the preparation of food) for human consumption with biological agents for the purpose of causing injury or death to civilian populations and/or disrupting social, economic or political stability.

Bioterrorism attacks could be directed at many different targets in the farm-to-table food continuum, including crops, livestock, food products in the processing and distribution chain, wholesale and retail facilities, storage facilities, transportation, and food and agriculture research laboratories [5].

Here we will provide basic information on specific bioterrorism threats to the food supply in order to prepare you to counter such threats. Threats to food security include: biological warfare against livestock and crops, the contamination of imported foodstuffs, the contamination of the water supply and tampering with food because certain bacteria and viruses could be deliberately added.

Food-borne diseases causing microorganisms mainly belong to CDC-class B list of potential biological warfare (BW) agents (*Salmonella spp., Shigella dysenteriae, E. coli O157:H7, Vibrio cholerae, Cryptosporidium parvum*). But agents such as *Clostridium botulinum* from the BW Class A could be also used to deliberately poison the food supply. Analysis of Mead at al. in their study suggested that unknown agents account for approximately 81% of food-borne illness and hospitalizations, and 64% of deaths. Among cases due to known agents, Norwalk-like viruses account for over 67% of all cases, 33% of hospitalizations, 7% of deaths. *E.coli* O157:H7 was estimated to cause 10,000 to 20,000 illnesses annually [6].

Civilian populations are usually more vulnerable than military personnel. Large farms and food processing plants with widespread distribution networks are vulnerable targets for food terrorism [7].

Agriculture can be a suitable target because biological agents do not present a direct threat to human subjects, are not easily identified, artificial pest infestation can be masked by natural epiphytoty or epizooty, the increase of scale of international trade, the unification of agricultural production by growing similar genotype sorts of plants, the majority of farms and fields are not protected from bioterrorists, and the planning of large-scale attacks is facilitated by long incubation periods. So, a bioterrorist attack against an agricultural facility is not only a psychological and ecological attack; it also produces a long-term destabilization of a system of food security in an entire region, causing rapid price increases for food before the occurrence of infection/intoxication symptoms [8].

Potential biological weapons that can be used for food terrorism range from sophisticated bio-engineered pathogens to other agents that are part of the natural environment. Genetic engineering development makes possible the modification of microorganisms in order to defeat detection and identification, increases their virulence, resistance to antibiotics, environmental conditions, makes novel dangerous microorganisms etc.

Outbreaks of both unintentional and intentional food-borne disease can be managed by the same mechanisms usually contained in a crisis management plan. Any release would probably initially be considered as a natural or unintentional event.

The economic and health care impacts of the food-borne outbreaks, even if they are not deliberately caused or it is not clear, can be illustrated by several examples. So, the U.S. food-borne illness outbreak in 1994 sickened 224,000 people nationwide with *Salmonella enteritis* from eating a national brand of ice cream. That outbreak, though not deliberate in nature, is estimated to have cost about $18.1 million in medical care and time lost from work. The U.K. outbreak of foot and mouth disease in 2001 resulted in over 10 billion USD in losses to tourism and the food and agriculture sectors and the slaughter of over 4 million animals. In 2002, one involved ground beef produced by a plant in Colorado that caused at least 46 people in 16 states to become ill from *E. coli*

O157:H7. The plant conducted a recall to remove about 18 million pounds of potentially contaminated beef that had entered commerce. The other outbreak involved fresh and frozen ready-to eat turkey and chicken products. Those products, in a Pennsylvania plant, carried *Listeria monocytogenes*, caused 46 illnesses in eight states, as well as seven deaths and three stillbirths or miscarriages. The plant recalled approximately 27.4 million pounds of potentially contaminated poultry products that had entered commerce.

The largest incidents with microorganisms also include an outbreak of an *S. typhimurium* infection in 1985, affecting 170,000 people, caused by the contamination of pasteurized milk from a dairy plant in the United States of America. An outbreak of hepatitis A, in 1991, associated with the consumption of clams in Shanghai, China, affected nearly 300,000 people and may be the largest food borne disease incident in history. An *S. enteritidis* infection outbreak, in 1994, from contaminated pasteurized liquid ice cream that was transported as a pre-mix in tanker trucks caused illness in 224,000 people in 41 states in the United States of America. In 1996, about 8,000 children in Japan became ill with an *Escherichia coli* O157:H7 infection from contaminated radish sprouts served in school lunches. Some of the children died [4].

Because of the potential similarity between naturally occurring and intentional outbreaks and the increased threat of bio-terrorism, intentional contamination should be considered in cases of: 1) unusual or not easily explained outbreaks, 2) outbreaks resulting from bio-engineered pathogens, not easily detected by existing methods.

An attack could occur at any point along the food supply chain from farm to fork. Terrorists could create harm through: (1) final product contamination using either chemical or biological agents with the intent to kill or cause illness among consumers, (2) the disruption of food distribution systems, (3) damage to the agricultural economy by introducing devastating crop pathogens or exotic animal diseases such as foot-and-mouth disease, or (4) hoaxes, using the mass media or Internet, which create anxiety and fear.

If there is information about the absence of reliable protective methods against biological weapons in the target area and no possibility of their rapid development, the area is classified as risky for bioterrorism. When the used biological agent possesses high harmfulness and has a wide range of response on environmental conditions, it is more likely to be used with terrorist purposes. If the potential damage to the crops is high, detection of the act of aggression in a short period of time is difficult, then terrorist attack is more likely to be undiscovered which becomes a strong point of terrorist or criminal groups [9].

3. Food bio-terrorism: prevention and defense

In the context of food bio-terrorism it is extremely important to prevent the sabotage of food during production, processing, distribution and preparation. The key to preventing food terrorism is enhancing existing food safety programs and implementing reasonable security measures on the basis of vulnerability assessments. Food defense involves activities associated with protecting the food supply from deliberate or intentional acts of contamination or tampering.

The food supply system is quite difficult to protect for many reasons: it encompasses many different industries, a variety of potential bioterrorism and chemical agents could contaminate the food supply, and the possible scenarios for deliberate contamination events are essentially limitless. Then, the public health system is complex, and responsibilities for prevention and control may overlap or fall in the gray area between the authorities of different agencies. To achieve food and agricultural bio-security, the activities are needed in the areas of prevention, detection, and response [10].

Prevention, although it can never completely be effective, is the first line of defense. The keys to prevent food terrorism are establishing and enhancing food safety management programs and implementing reasonable security measures. The measures of precautions, coupled with a strong surveillance and response capacity including established procedures, plans and training scenarios prior to actual events are essential in the preparation of efficient and effective countering food-bioterrorism. Prevention is best achieved through a cooperative effort between government and industry, given that the primary means for minimizing food risks lie with the food industry [4].

Prevention includes education for food producers about bioterrorism and chemical agents likely to contaminate food, where in the production process contamination would likely occur, and what food-processing steps can be taken to eliminate or deactivate potential agents and chemicals. Guidance on how to assess plant or company vulnerability against a bioterrorist attack and to reduce the likelihood of a bioterrorist attack must be developed and introduced to practice. Detection means the availability of methods for identifying credible threats, rapid and secure communication systems for the sharing of information on unusual events within the industry, enhanced laboratory capacity, the development of a primer for clinicians (including signs, symptoms, laboratory diagnosis, and treatment) on potential high-impact food-borne bioterrorism agents (e.g., food-borne anthrax, botulism toxin, chemical agents) to aid in the rapid recognition of outbreaks. Guidance on developing action plans for response is also necessary, including information on which agencies to contact for which types of events [10].

Response includes methods to increase government/industry coordination for investigating food-borne outbreaks, including issues of improving product traceability: improved coordination between animal health, public health, law enforcement, and industry for responding to bioterrorism events; guidance on developing streamlined systems for risk management communication throughout a product supply chain from farm to table in the event of a real bioterrorism attack; "just-in-time training" that provides accurate information in a timely manner to key industry leaders, employees, public health officials, and consumers in response to current events involving new or re-emerging disease threats [11].

Food safety must be well regulated because food is critical infrastructure with high national, regional and global health, economic and security impacts. Thus, the local, national governments, health and agricultural experts and other social factors, as well international community with its political, expert, regulatory and control bodies must be involved in the process of increasing food safety and protect it from potential bio-terrorist events.

The concern of people about food safety has increased recently, people have got more informed about food safety, and more often people have started to claim their rights and defend them. People also read more carefully the labels on food products, paying attention to the ingredients of the product, nutrition value, and the presence of preservatives and GMOs.

4. International food defense

Concerning food system safety since 2001, at the international level some steps have been taken, both unilaterally and cooperatively, by individual nations, the United Nations, and some NGOs.

Unfortunately, we can say that everything that is being done is at a rather low, relatively ineffectual level, or has only included a subset of the required stakeholders.

The World Health Organization (WHO) has published several useful guidance documents that address the defense of food supply systems. Guidance on "Terrorist Threats to Food," which was published in 2002 as a food safety issue, provides useful guidance on protecting food supply chains and emergency response systems. The WHO also maintains the Global Outbreak Alert and Response Network to provide rapid assistance for public health emergencies that could be related to contaminated food, among a number of potential bio-terrorism possibilities [4].

In 2004, at the annual meeting of the Biological Weapons Convention (BWC), the issues of protecting the international food supply chain were discussed, and while no concrete action was taken, there was an agreement to continue the discussion of potential international action on this matter at future meetings. Subsequent meetings have not produced any substantive progress on broad international cooperation. The 2005 session merely concurred with the results of the 2004 annual meeting, and no concrete action to further defend international food systems was taken or proposed.

The Asia-Pacific Economic Cooperation (APEC) has addressed the issues of food system defense in the Asia-Pacific Region at conferences and workshops [12].

There have been some efforts by organizations, such as the FAO to develop food supply system defensive programs, but these are still primarily targeting food safety and sanitary issues in specific countries where insurgencies and famine are prevalent already.

The events of 9/11/02, reinforced the need to enhance the security of the food supply worldwide. So, the US Congress responded by passing the Public Health Security and Bioterrorism Preparedness and Response Act. Title III, Subtitle A of the Act is named: Protection of the Food Supply. There are four provisions that require regulations: Administrative Detention, Registration of Food Facilities, Establishment and Maintenance of Records and Prior Notice of Imported Food Shipments. The Bioterrorism Act granted the Food and Drug Administration-FDA the authority to require domestic and foreign food facilities to register with the agency and provide prior notice when bringing food into the US from other countries. The law covers all human and animal food, drinks, and dietary supplements imported or offered for import to this country. The FDA and customs are working together to share information and computer systems and to keep food imports safe without creating unnecessary delays. The FDA is now authorized to administratively detain suspect food. This means that the FDA can remove food from the food supply if it has credible evidence or information that it presents a threat of serious adverse health consequences or death to humans or animals. Another new regulation under the Bioterrorism Act creates a requirement regarding the establishment and maintenance, for no longer than 2 years, of records by persons (excluding farms and restaurants) who manufacture, process, pack, transport, distribute, receive, hold, or import food [4].

In January of 2003, the US President issued Homeland Security Presidential Directive 9, which declared the nation's food supply chain as a Critical Infrastructure and mandated necessary protective actions [13]. Presidential Directive 9 represents the first time the food supply chain was identified as critical to the nation. This document sets forth actions that will improve the protection of the food supply chain, both within the United States and for their food and agriculture trading partners.

The FDA proposed the Food Protection Plan ("FPP") that was adopted in 2007 and described the food supply protection strategy, comprised of preventing food borne contamination in the first instance, intervening at critical points in the food supply chain, and minimizing harm from contamination that does occur. The Food Safety Modernization Act ("FSMA") was enacted in 2011 and will be implemented by the FDA over the next few years in order to enhance the safety of the U.S. food supply through a host of food safety requirements and strengthen food defense safeguards. In July 2011, the FDA released its strategy to prevent food from being smuggled into the US [14].

The European Union has been rapidly expanding its regulatory authority and available food processing and handling guidelines to improve the defense of its food supply chains from terrorist acts, as well as to improve the overall safety of its food systems. The European Union takes a comprehensive approach to food defense due to the "sheer complexity of [European] food systems," incorporating food defense into the European Commission's ("EC") general food safety legislation. The European Food Safety Authority is responsible for assessing risks in the European food supply, including risks of intentional contamination. The EC is responsible for risk management. There have been attempts to broaden cooperation between the European Union and the U.S., including the exchange of information, threat data, and technology [15].

2004 Sea Island Summit, the *G8 Action Plan on Non-Proliferation* articulated the G8 commitment to defending against bioterrorism. G8 countries pledged to initiate new bio-surveillance activities, increase protection of the global food supply, and mitigate intentional uses of biological weapons.

Under the World Trade Organization ("WTO") Agreement on the Application of Sanitary and Phytosanitary Measures ("SPS Agreement"), members have the right to take food safety and plant and animal health measures necessary to protect human life provided that those measures are consistent with the rest of the agreement. Here is an exemption under the General Agreement on Tariffs and Trade ("GATT") for measures necessary to protect essential security interests, but the exemption is ambiguous and its applicability to food defense measures is questionable. Other international organizations are also beginning to focus on food defense. Likewise, the International Organization for Standardization's ISO 22002-1 prerequisite programs include food defense measures, and the organization has indicated that its standards need to be updated with comparable requirements [16].

5. Food bio-defense: the local efforts with global impact

At the national levels the highest governmental bodies as well as regulatory agencies must control the process of food production informing the responsible - Ministries of Health and Agriculture. Laws and regulations which set out the Government's role in food safety must be well defined. In the event of a terrorist incident, the Government and other services would be responsible for crisis management including law enforcement, intelligence gathering, surveillance, negotiation, and investigation. Swift communication among all the components of an emergency response system is essential and should be an integral part of preparedness planning. Governments also have a role in promoting preventive food safety.

In developing the food defense standards, it might be instructive to consider concepts that underpin the dual-use export controls system as well. The government, academia and industry partners must work together to develop the food defense standards. Such an approach would identify where the greatest threats to the food supply chain around the world exist. It would also identify the types of foods and ingredients that pose the greatest hazard if they become contaminated. Governments and industry could then intelligently deploy their resources and efforts to counter such threats proportionately, as opposed to treating every risk area as equally susceptible and potentially damaging.

The greatest threat to the food industry is likely the health and economic impact of terrorism. The solution lies in developing a preventive strategy for a terrorist attack. Typical food safety management programs within the food industry include good agricultural practice, good manufacturing practice and management of food bioterrorism risks. The main risk Management Tools are: ORM (Operational Risk Management), TEAM (Threat Exposure Assessment & Management) and HACCP (Hazard Analysis Critical Control Points).

As its name implies, HACCP identifies critical points along the food production and processing chain where contamination is most likely to occur. According to the EU Directive on Hygiene for Foodstuffs (93/43/EC), the HACCP system must be the basis for safety procedures for all foods.

While HACCP is typically applied to a process, it can also be applied to the complete food supply chain. The first step is to identify critical control points by examining the flow of food production and distribution. Food Security HACCP differs by accounting for areas inside and outside the plant. We must also consider the security of ingredients and products entering plant, individuals and vehicles entering plant, facility (external and internal) and processes, products leaving the facility. If indeed an event does occur, we need an Incident/Crisis Response Plan that covers food security. The following are key elements of such a plan: reporting procedures, emergency evacuation plans, a plant plan at the local fire department or in a secure location outside the plant, a strategy for continued production, an effective recall policy, cooperation with a qualified forensic lab, prepared press and customer statements and a designated spokesperson [17].

Meanwhile, companies must continue to take all reasonable steps to protect their customers, their reputations, and their products by being vigilant about food defense issues. Among other things, they must continually re-examine their business models for potential risks and take steps to best position their resources against them.

Each establishment shall assess the hazard to products posed by potential acts of sabotage, vandalism or terrorism and shall put in place proportional protective measures. Potentially sensitive areas within the establishment shall be identified, mapped and subjected to access control. Innovation will undoubtedly play an important role in countering these ever-evolving threats, and industry should be on the lookout for new tools and systems that will help them on this front.

According to GAO report, there is a broad consensus worldwide that farm, food and agriculture systems are vulnerable to potential attacks and deliberate contamination.

If you notify that you have a threat or issue at your facility including suspicious behavior it is necessary to contact the appropriate authorities [18].

National health surveillance systems may allow early detection of bio-terrorism. Education about bio-terrorism should enhance the epidemiologic and investigative skills of healthcare professionals, including laboratory personnel, especially those in primary care settings, who are likely to be the first contact for people and communities affected by acts of bio-terrorism [19].

6. Food borne Disease Surveillance and Public Health Response to Food Terrorism

Surveillance of food-borne illness is complicated because of underreporting and not being detected through routine surveillance. Many pathogens transmitted through food are also spread through water or from person to person, thus obscuring the role of food-borne transmission. Finally, some proportion of food borne illness is caused by pathogens or agents that have not yet been identified and thus cannot be diagnosed (the pathogens of greatest concern e.g. *Campylobacter jejuni, Escherichia coli O157:H7, Listeria monocytogenes, Cyclospora cayetanensis* were not recognized as causes of food-borne illness just 20 years ago).

Contamination of food in one country can have significant effect on health in other parts of the world. The WHO is in a unique position to coordinate existing international systems for public health surveillance and emergency response, which could include consideration of food bio-terrorism. Member States require alert, preparedness and response systems that are capable of minimizing any risks to public health from real to threatened food terrorism [4].

Intentional contamination of the food supply by terrorists is a new threat with unique challenges. Thus, it requires increased food inspection, disease surveillance, laboratory capacity, and awareness among health professionals and the general public.

Acts of food terrorism must first be detected by real-time surveillance and other alert systems, before a response can be mounted. The response may include verification of the threat, including the cause of disease, management of the consequences by aiding the affected population, identification and removal of the food from sale and management of the social, political and economic consequences of the act [20].

The main requirement for rapid detection of an epidemic is a surveillance system that is sensitive enough to identify small clusters of an illness. Such a system will permit the identification of disease outbreaks, whether intentional or unintentional, but may not initially permit the identification of the disease or its mode of transmission.

The deliberate contamination of food may be very difficult to recognize, especially if the agent is uncommon, or if the agent is not usually associated with the food. This is made more difficult if the clinical symptoms are obscure. Linkage of surveillance systems to other related systems might provide valuable information for the detection of outbreaks caused by food terrorism [21].

According to the WHO, identifying food bioterrorism considers early detection of disease resulting from covert food terrorism and depends on sensitive surveillance systems for communicable diseases at the local and national levels, with close cooperation and communication among clinicians, laboratories and public health officials. Public health response to food terrorism will depend on the type of agent, efficiency of the attack and the geographic distribution of cases. Acute and unusual illnesses clustered by time and location will trigger immediate response. Typical enteric-related food borne disease, even if in large numbers of cases, if distributed nationally, will be difficult to detect and identify the source in a timely manner.

Outbreak investigations need to be conducted *rapidly* if they are going to help identify contaminated products and remove them from the marketplace. It is necessary to have close collaboration among epidemiologists, public health laboratories and environmental health specialists.

Food-borne illnesses cause symptoms such as nausea, vomiting, diarrhea, or fever. Symptoms can occur between 1 hour and 3 weeks after eating contaminated food, depending on the agent ingested (bacterial, viral, or parasitic), so tracing the source of a food-borne outbreak can be very complicated and time consuming.

The most difficult aspect of intentional food contamination is the rapid diagnosis of its true nature. The ability to respond to such an event is skewed by the speed of healthcare recognition, reporting by state agencies to the federal government, and in many cases, an event that may occur over multiple states and geographical boundaries. Bioterrorism within the food system is made especially difficult by the sheer magnitude of biological agents that can be used. The first difficulty with identifying an outbreak, let alone a food-borne outbreak, is whether the affected individual seeks out medical attention. Secondly, a misdiagnosis of the agent or the healthcare provider simply diagnosing it as basic food poisoning without taking samples occurs frequently.

Epidemiological research performed during thesis work made use of provided FDA data sets of outbreaks from five involved regions, etiology, months, seasons, and location of outbreaks and were statistically analyzed.

The need for increased security via the technological tracking of carrier vehicles and shipments, as well as microbial risk assessment and modeling, are aspects that must be addressed by the public health system, food distributors and consumers. An event of intentional contamination can cause death, illness, hysteria, loss of trust within agencies, disruption of everyday life, and sometimes, complete economic collapse of the particular food industry

In the context of food bio-terrorism, prevention means preventing the sabotage of food during production, processing, distribution and preparation. Although never completely effective, it is the first line of defense. The diversity of sources of foods, including global market, makes prevention difficult, if not impossible. At the same time, many developing countries lack basic food safety infrastructures and are vulnerable to deliberate acts of sabotage [22].

However, in the mid-1990s, the CDC began to develop the Food-borne Diseases Active Surveillance Network (Food Net) (http://www.cdc.gov/foodnet), to help public health experts be on the alert for food borne illnesses. Several associations and US agencies collaborated to produce a free educational primer on food safety called "Diagnosis and Management of Food borne Illnesses: A Primer for Physicians and Other Health Care Professionals"

Another promising use of technology in food safety is "DNA fingerprinting." This molecular system uses networked computers to identify distinctive patterns and the genetic makeup of *E. coli* and other bacteria and match strains of bacteria from different locations. Pulse Net enables the CDC to determine when people in different locations are becoming sick from a single source of contamination based on the bacteria's specific DNA. If scientists can determine the source of contamination, it may be possible to track down other people who are ill or may become ill [23].

The WHO identifies food-borne disease outbreaks and incidents, including those arising from the natural, accidental and deliberate contamination of food, as major global public health threats in the 21st century. These threats require urgent action, and the WHO recognizes that the building of global public health security rests on solid and transparent partnerships. The Full implementation of the WHO International Health Regulations, cross collaboration within governments, global cooperation in surveillance and outbreak preparedness, alert and response, open sharing of knowledge, technology and materials and capacity building in health security is necessary by Member States [24].

Clearly, the potential health effects of a terrorist attack must be taken seriously by the public health community and by those responsible for assessing and countering terrorist threats [25].

Food-borne disease, whether intentional or otherwise, can also paralyze public health services. While many countries have some form of emergency response plan, they often do not include consideration of terrorist threats to food. This gap in preparedness could lead to misdiagnoses, incorrect laboratory investigations and the failure to identify and detain affected food. This would weaken or even preclude an effective response to a food sabotage incident [26].

7. Food supply resources in Serbia: potential risk and control measures to prevent bio-terrorism incidents

The Republic of Serbia has recently become a candidate to for membership in the European Union. Considering that the agriculture and food industries play important roles in trade between Serbia and EU members, there is a growing need for harmonizing policies in this field. In expanding its membership, the EU declared that it would not compromise food safety by admitting countries with lower food safety standards or with programs that pose additional risk for consumers. The natural advantages such as a favorable climate, fertile terrain and experience in agriculture and food industry place Serbia in a relatively good position, but in the future, with a fully opened market, there will be strong competition and maximum food safety conditions should be provided.

During the 1960s till the 1980s, Serbia was traditionally a country with strong and developed agriculture and food industries. Favorable conditions provided an excess in food production with great opportunities for export, not only to Eastern European markets, but also to Western markets. But, in the 1990s, this situation was brutally changed with almost 10-year-long economic sanctions. The transformation to a market-oriented economy was completed in 2000. That led to the withdrawal of state interventions aimed toward the protection of weakened domestic production. The opened market resulted in introducing the numerous imported products and the rapid decline in domestic share in total trade. Big companies were privatized, often with unpredicted consequences for stakeholders and consumers, while small companies are struggling to keep their traditional food producing and processing procedures in difficult financial conditions.

Harmonization programs for food safety and quality control were started a few years ago. The following steps were made: to become acquainted with the mechanism of the EU, collection and analysis of the EU food legislation, studying the U regulatory system, the establishment of the framework of harmonization and declaration of the methods of harmonization. This will help the competitiveness of Serbian foodstuffs in the market-place, and to prepare the industry for the EU accession giving sufficient time for the economy to study and apply the necessary regulation and changes. Public sector actions to support improved food safety are: policymaking at the national level in order to establish effective food safety regulation, which requires the capacity for assessing food safety risks, the establishment of priorities for policy intervention, and the ongoing monitoring and evaluation of food safety risks; capacity building to participate in the international arena; provision of information by the public sector, which can make it easier for consumers or export buyers to identify and reward safer products (certifying production conditions); direct public efforts to prevent and control hazards, which include additional investments in improving sanitation infrastructure at key points in the food supply chain; and finally, investments in research [27, 28, 29].

According to the WHO the definition of food terrorism as *"An act or threat of deliberate contamination of food for human consumption with chemical, biological of radionuclear agents for the purpose of causing injury of death to civilian populations and/or disrupting social, economic or political stability"*, there was no single attempt of food terrorism in Serbia. As declared in Secufood Report (comprising five countries: Italy, Spain, the United Kingdom, Romania, Denmark, which are selected to be representative of Europe in terms of Mediterranean and continental countries, "new" and "old" EU countries, and with different food regimes) [30], there is no evidence whatsoever of a terrorist attack against the food supply chain (the only episode reported in literature is that which happened in 1989 in Israel with the contamination of grapefruits). Even if, in the period from 1950-2008 there were 450 "suspected" episodes recognized, of which chemical agents were present in 335 cases, biological agents in 10, radiological in 7, physical contaminants in 8 and unknown agents in 3 cases. The large retail and food services were recognized as weak points, because the large risks are assumed in the phase not directly controlled (i.e. wholesale distribution and retailer).

Food terrorism threats are categorized as internal and external, and attackers are grouped into five categories: criminals, protesters, terrorists, subversives and rogue or disgruntled insiders [31]. The attacks are aimed at generating disease and death, and in most cases to induce fear and anxiety. The past experiences proved that even "symbolic" attacks are able to create a public health impact, economic losses or trade disruption, together with social and economic damages.

Are the Serbian agriculture and food industries attractive to such attacks? The risk is estimated as the product of likelihood and consequences. Likelihood is the function of *access availability*, i.e. the probability that the terrorists could access food resources, and *vulnerability*, i.e. susceptibility of infrastructure to such attacks. In addition, consequences are the product of the *effects* (both the physical and psychological health damages), and number of *persons* affected. To produce a huge impact, the terrorists must introduce the contaminants immediately after the processing phase. The most effective attacks hence would be made on farms and during processing. The organization of the Serbian agriculture and food industries considers just a few large companies, where it might be successful. The attack on small farms and factories would not be effective. On the other hand, exposure to symbolic contamination considers the attacks in phases close to the consumers, where the processes are less controlled, therefore a high probability of success is more evident. Past experience indicates that the motives of such attacks are more personal than aimed for general damage. Many food operators are aware of the vulnerabilities in their process, and especially the "negative publicity" caused by the idea that their food can be maliciously manipulated.

As previously mentioned, in Serbia, many foods are imported. Unfortunately, the risk of illegal food import is relatively high, due to unfavorable state position and the well-known situation in the whole south-eastern European region. Like most countries, Serbia established an emergency response system to respond to catastrophic incidents such as earthquakes, floods or disease outbreaks that threaten the health of the population. However, this response system does not include consideration of food as a vehicle for delivering harmful agents by terrorists. The government's role in protecting the safety of the nation's food supply has historically depended on two factors: first, incremental legislation and regulation in response to specific problems, and second, effective coordination and cooperation among regulatory authorities and other public and private stakeholders. Two aspects of the food supply system make it difficult to minimize acts or threats of deliberate contamination. First, the food supply system encompasses a multi-faceted production and delivery system of food products, commonly referred to as a "farm-to-table" or "farm-to-plate" system. Essential system components include the production, processing, preparing, packaging, labeling, distribution, and, of course, consumption of food. At each of these stages, food products may be exposed to various levels of risk. The World Trade Organization (WTO), based on the Agreement on the Application of Sanitary and Phytosanitary Measures (SPS Agreement), resolves trade disputes that involve food safety issues, such as the regulation of hormone use in cattle.

Strengthening national food safety programs requires that national policies and resources to support the infrastructure are in place and that food legislation, food monitoring and surveillance, food inspection, food borne disease surveillance, education and training are adequate and up to date. Proactive risk analysis can reduce vulnerability in the same way as analysis of the risks of inadvertent contamination. The resources allocated need to be proportional to the likelihood of the threat, the magnitude and severity of the consequences and the vulnerability of the system. The possibility of intentional contamination needs to be an integral part of safety considerations, and measures to prevent sabotage should augment, not replace, other activities. Typical food safety management programs within the food industry include good agricultural practice, good manufacturing practice and "hazard analysis and critical control point" (HACCP) and HACCP-based systems.

Industries have shifted away from the traditional focus on end-product testing (where sub grade products are rejected) toward quality management of the production process (where the aim is prevention of quality mishaps before they happen). With regard to food safety, "Hazard Analysis and Critical Control Points" (or HACCP) represent the main strategies. HACCP, a 7-step method developed in the 1960s for controlling microbiological contamination of processed foods for the US space program, has been expanded to cover a range of different types of contamination, in a variety of production circumstances.

In Serbia, this approach resulted in a shift from end-product to process-based regulatory standards. Regulatory bodies are shifting their emphasis from measures targeting outcomes (e.g. maximum tolerance levels for contaminants) to process-based measures (i.e., imposition of specific quality assurance methods). Process-based regulations shift the primary responsibility for safety from the government to the private sector. This is sometimes referred to as a move from a "command and control" approach to one stressing the responsibility of private industry actors.

In the private sector, food safety management comes under the broader rubric of "quality assurance". Private food safety standards are also of great importance, especially in countries like Serbia, with a long-term tradition in this type of food production. Since, in general, PFS include a requirement that all relevant national standards have to be met, these standards are never "less stringent" than official standards. They may sometimes require specific measures that are not suited to the context in which the business operates. Certification to private sector schemes has been shown to provide a driver for improved hygienic practices by food chain operators and it has been shown to create opportunities for developing country producers to access markets that would otherwise not have been open to them. Furthermore, some developed countries are considering ways of integrating private standard certification into overall national systems of food control to strengthen public health protection. A major concern about the standards, however, is that they are disproportionately burdensome to small-scale operators and sometimes unnecessarily so.

In order to prevent standards from being misused as non-tariff trade barriers, the WTO has adopted two agreements: the Agreement on Technical Barriers to Trade (TBT), and the Agreement on Sanitary and Phytosanitary Measures (SPS). TBT measures comprise technical standards, along with regulations on test and inspection procedures and certification. They are developed by organizations such as the International Standard Organization (ISO). Sanitary and phytosanitary standards, as covered under the SPS Agreement, include health and hygiene standards or regulations to avoid the spread of animal and plant diseases and epidemics. These are adopted by the Codex Alimentarius Commission (CAC) of the Food and Agriculture Organization (FAO) and the World Health Organization (WHO), the World Organization for Animal Health, and organizations collaborating within the framework of the International Plant Protection Convention. For the development of their own standards, WTO member countries are encouraged to use international standards where they exist [32].

Regarding the situation in this field in Eastern and Central Europe (including Serbia), there is a consensus that it is necessary to strengthen food safety systems, which will then result in improved safety in prevention and appropriate management of terrorist attacks in food industry. According to previously mentioned issues, the main frame of antiterrorist measures is the harmonization of the national safety regulation with the requirements of the EU. Joining the EU requires countries in this region (including Serbia) to take a number of steps to improve their food safety systems, including: adopting a new food law and improving coordination among the different national competent authorities and institutions responsible for food controls; harmonizing all health legislation in accordance with EU regulations; updating approaches and methods to improve food safety and moving them from mandatory compliance toward risk-based control systems; improving access to laboratories and the quality of laboratory equipment; and increasing laboratory-based surveillance of food borne diseases and epidemiologic investigation of outbreaks, as well as chemical and microbiological food contamination monitoring.

In order to fulfill the strict demands discussed above, the National Parliament of the Republic of Serbia adopted the *Food Safety Law* on May 29, 2009 (published in the Official Gazette of the Republic of Serbia No. 41/09). This Law governs the general conditions for the safety of food and feed, duties and responsibilities of food and feed business operators, rapid alert system, emergency measures and crisis management, food and feed hygiene and quality.

In this Law, the risk of unsafe foods is explained using these terms: *Risk analysis* which represent the process consisting of three interconnected components: risk assessment, risk management and risk communication. *Risk communication* means an interactive exchange of information and opinions through the risk analysis process as regards hazards and risks, risk-related factors and risk identification, among the risk assessment and risk management authorities, consumers, food and feed business operators, scientific and higher education establishments and other interested parties, including the interpretation of risk assessment results and the basis of risk management decisions.

The term *Hazard* represents a biological, chemical or physical factor in food or feed or a state of food or feed, which can potentially be harmful to health, while *Risk assessment* means a scientifically based process consisting of four stages: hazard identification, hazard characterization, exposure assessment and risk characterization. *Risk* is addressed to the factor of probability of a harmful impact on health and the severity of such impact, as a consequence of a hazard, while *Risk management* refers to the process of setting the policies and measures, separately from risk assessment, which includes consideration of possible alternatives for further action, in consultation with interested parties, as well as the implementation of the risk abating measures, based on risk assessment and relevant data.

This Law regulates the principles of risk analysis, precautionary principle, principle of protection of consumers' interests, and principles of transparency. Risk assessment should be based on the available scientific evidence and especially the opinion of the Expert Council for Risk Assessment in Food Safety Area, in an independent, objective and transparent manner. Risk management should be based on the results of risk assessment, precautionary principles and other factors of importance for the case being considered [33].

The safety of food and feed in the territory of the Republic of Serbia is provided for by the operators entered in the Central Register of Facilities and other entities involved in the field of food and feed safety within their responsibilities. The other entities referred to are Ministry of Agriculture, Forestry and Water Management (as the central authority), Ministry of Health and Laboratories.

The Law also regulates the division of competencies, where the duties related to food safety should be performed by the following state administration authorities:

In the primary production stage, for food of animal and plant origin – the responsible authorities are veterinary inspection and phytosanitary inspection, respectively. In the production, processing and wholesale stage, the responsibility is shared between veterinary inspection (food of animal origin), agricultural inspection (food of plant origin and non-alcoholic beverages), and veterinary and agricultural inspections (mixed food).

In the import and transit stage of food of animal origin the main authority is border veterinary inspection, while phytosanitary inspection is responsible for food of plant origin. Both inspections are involved in control of import and transit of mixed food. The same pattern is applied in the export stage, with the addition of agricultural inspection in export of wines and spirits.

Control of novel food, dietetic supplements, food for babies – supplements for mothers milk, dietetic supplements and salts for human ingestion and production of additives, aromatics, enzymatic preparations of other than animal origin and accessories of other than animal origin, as well as drinking water in original packing (table water, mineral water and spring water), as well as water for public supply of drinking water in all stages of production, processing and circulation (wholesale, retail, imports on customs points and exports) is conducted by sanitary inspection;

In the retail stage, food of animal origin in the facilities registered or approved by the Ministry, as well as retail of fresh meat, milk, eggs, honey, fish and wild animals in specialized facilities (butcheries, fisheries and similar) is conducted by veterinary inspection, and regarding wine and alcoholic beverages, agricultural inspection. Control of genetically modified food in all stages of production, processing and circulation is conducted by the phytosanitary inspection, and the veterinary inspection regarding genetically modified feed.

The international obligations in the field of food safety are executed in accordance with the recommendations of relevant international organizations, the WTO Agreement on the Application of Sanitary and Phytosanitary Measures (*SPS Agreement*), international conventions and other relevant international agreements, and information should be exchanged with other national organizations responsible for food safety.

For the purpose of considering issues related to the risk assessment in the field of food safety, the Minister, with the consent of the minister responsible for public health and in accordance with regulations governing state administration, establishes a special working group - Expert Council for Risk Assessment in the Field of Food Safety. Administrative and technical tasks for the needs of the Expert Council are performed by the Ministry. Expert Council applies and uses recommendations, guidelines and information available through the European Food Safety Authority – EFSA in its operation. Expert Council performs the following activities: prepares expert and scientific opinion for the ministries and other state administration authorities, food and feed business operators, consumers, as well as other interested parties, regarding risks related to food and feed; enhancement and coordination of application of the methods for risk assessment; provision of scientific and technical assistance upon request of ministries and other state administration authorities in interpretation and considering opinions on risk assessment; collection, comparison and analysis of scientific, technical data related to the defining and control of risk that have a direct or indirect effect on the food and feed safety; provision of scientific and technical assistance upon request of ministries that implement procedures for managing crisis in the field of food and feed safety; provision of opinion regarding measures that are applied for improvement of the system in the field of food and feed safety; giving information to the general public and interested parties on relevant information from the scope of work of the Expert Council; provision of opinion on the program for managing crises in the field of food and feed safety; preparation of guides for good agricultural, producers and hygiene practice, as well as application of the principle of Hazard Analysis and Critical Control Points (hereinafter referred to as; HACCP) for the needs of the ministry; provision of recommendations for expert specialization and education in the field of food and feed safety; other tasks related to the risk assessment in the field of food safety.

This Law institutes a rapid communication and alert system, as a network for the notification of the direct and indirect risks to health caused by food or feed. The Ministry administers the rapid communication and alert system. The ministry responsible for public health, the Expert Council reference laboratory, participates in the rapid communication and alert system. A central information system is established for the exchange of data with other institutions involved in the risk assessment and management in the Republic of Serbia and relevant foreign institutions. Other interested countries and international organizations may also participate in the rapid communication and alert system, on the basis of agreements concluded with such countries and organizations.

This Law also regulates the emergency measures. If the Ministry and/or the ministry responsible for public health finds that a food or feed, whether of domestic origin or imported, may pose a serious threat to the health of humans, health of animals or the environment, as well as that such risk cannot be eliminated in a satisfactory manner, the Minister and/or the minister responsible for public health orders one or several emergency measures. All participants in the rapid communication and alert system in such situations should promptly notify the Ministry and/or the ministry responsible for public health of the occurrence of the risk, within the scope of their responsibilities.

If the food or feed is of the domestic origin, the following emergency measures may be applied: a temporary ban on placing on the market or the use of food or feed or specifying special conditions for the treatment of the mentioned food or feed. If the food or feed is imported, the emergency measures are: a temporary ban on the import of food or feed from the exporting country or a part thereof or the country of transit or specifying special conditions for the treatment of the mentioned food or feed from the exporting country or a part thereof or the country of transit. Should the risk assessment not confirm the existence of a risk to health, the Ministry and/or the ministry responsible for public health shall revoke the ordered measure.

In the event of direct or indirect risk to the health of humans, health of animals or the environment caused by food or feed, the occurrence of which could not be foreseen, prevented, eliminated or abated to the acceptable level of the prescribed measures, the measures provided by the Crisis Management Program in the Field of Food Safety shall be applicable. The Crisis Management Program in the Field of Food Safety includes in particular: The type of situation in which direct or indirect risk to the human health caused by food and feed exists; measures which have to be implemented promptly once it has been established that food or feed is posing serious a threat to humans or animals, either directly or indirectly through the environment; Crisis management procedures, which include the principle of transparency and communication; and Plan of exercises and simulations for crisis management purposes. The Crisis Management Program in the Field of Food Safety has been adopted by the Government.

For the purpose of the analysis and monitoring of food and feed safety, the Ministry keeps databases in conformity with this Law and makes use of the data in accordance with other prescribed databases, on the basis of special regulations. The databases related to food and feed safety must be linked with the Register of Farms kept by the Ministry. The Ministry established the network of National Reference Laboratories performing the activity in accordance with this Law. The manner of linking the databases, the manner of collecting and using data from other databases, as well as the manner of coordinating and administering the network of National Reference Laboratories are governed by a special regulation enacted by the Minister with the consent of the minister responsible for public health.

8. Conclusions

Food bioterrorism is a serious threat with potential global health, economic and social consequences. Food protection and defense imply the development of effective measures to prevent, detect and respond to a potential bioterrorist attack of the food system.

Cooperative national and international efforts to defend and protect the food supply system may be crucial to the global security in the coming years.

In Serbia, there is an urge for complete harmonization of regulative regarding food safety with EU. The Food Safety Law adopted in 2009 gives a promising perspective. It regulates the obligation of introducing HACCP and other standards in food industry, as well as the tightening of the private food sector regulations. In most countries, full application of these standards provides adequate prevention against terrorist attacks as well.

References

[1] http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5218a3.htm

[2] M.Wheelis, Investigating Disease Outbreaks under a Protocol to the Biological and Toxin Weapons Convention, Emerging Infectious Diseases, 6(2000), 595-600.

[3] PS Mead, L Slutsker, V Dietz, at all. Food-Related Illness and Death in the United States, Emerging Infectious Diseases, 5(1999), 607-25.

[4] World Health Organization, Terrorist threats to food:Guidance for establishing and strengthening prevention and response systems, 2002. http://www.who.int/fsf/documents/terrorism_and_food.en.pdf

[5] www.gao.gov/cgi-bin/GAO-04-259

[6] Taleski V, Food-borne diseases-bioterrorist threat to public health. HACCP Conference, How to make HACCP more efficient in practice?, Morevska Toplice, Slovenia, 2006

[7] DA Ashford, RM Kaiser, ME Bales at all. Planning against Biological Terrorism: Lessons from Outbreak Investigations, Emerging Infectious Diseases, 9(2003), 515-19.

[8] United States Department of Agriculture. Economic Research Service. U.S. Food Imports, 2013. http://www.ers.usda.gov/data-products/us-food-imports.aspx

[9] OA Monastirskiy, Globalization of agricultural production and food safety in Russia/ Food Safety in Russia. Materials of the conference, Moscow State Academy of Veterinary Medicine and Biotechnology, Moscow, Edit House NP, 2005,93–102. http://www.uvao.ru/okno/Prod_bezop.pdf

[10] Report of the Meeting of the States Parties to the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, Geneva, Switzerland, 2005, http://www.opbw.org/new_process/msp2005/

[11] J Sobel, AS Khan, DL Swerdlow, Threat of a biological terrorist attack on the US food supply:The CDC perspective. The Lancet, 359(2002), 874-80.

[12] U.S.Dep't of State, *APEC Food Defense Initiative,*2006 http://www.state.gov/r/pa/prs/ps/2006/75537 (APEC members had met in November of 2006 at a workshop in Bangkok, Thailand)

[13] Chicago, IL: American Medical Association. Diagnosis and management of food borne illnesses: A primer for physicians and other health care professionals,2004

[14] http://www.fda.gov/oc/bioterrorism/bioact.html

[15] Isabelle Benoliel, EU Defending Food Chain Against Bio-Attack, European Affairs 8 (2007), http://www.europeaninstitute.org/2007030297/Spring-2007/eu-defending-food-chain-against-bioattack.

[16] FDA Food Protection Plan, 2007 http://www.fda.gov/Food/FoodSafety/FoodSafety-Programs

[17] Global Food Safety Initiative, *Stakeholder Meeting Report*, 2010, http://www.mygfsi.com/gfsiiles/GFSI_Stakeholder_Meeting_Report_Washington_DC

[18] http://www.fskntraining.org, CC-BY-SA, 2009

[19] K Mitchem, Bioterrorism and the Clinical Laboratory. Labmedica Int., 19(2002), 8-9

[20] E Hartnett, G Paoli, D Schaffner, Modeling the Public Health System Response to a Terrorist Event in the Food Supply. Risk Analysis, 29(2009),1506-1520.

[21] D Trudil, J Tartal, C Trudil, Experience received from the cases of bioterrorism in year 2001. Special symposium on problems of biosafety and bioterrorism (in Russian), St.-Petersburg, 2002.

[22] JP Dudley, MH Woodford, Bioweapons, bioterrorism and biodiversity: potential impacts of biological weapons attacks on agricultural and biological diversity. Rev Sci Tech, 21(2002),125–137

[23] Terrorism and Other Public Health Emergencies: A Reference Guide for Media. http://www.hhs.gov/emergency.

[24] Khan, A.S., Swerdlow, D.L., Juranek, D.D. (2001). Precautions against biological and chemical terrorism directed at food and water supplies. *Public Health Reports, 116*, 3-14.

[25] Center for Infectious Disease Research & Policy, Bioterrorism and food safety: developing an effective national response. University of Minnesota, Minneapolis, 2001

[26] FDLI's 55th Annual Conference. March | April 2012. www.fdli.org/pubs/update

[27] WHO, Department of Food Safety, Zoonoses and Food borne Disease, Clustero on Health Security and Environment. Terrorist Threats to Food – Guidance for Establishing and Strengthening Prevention and Response Systems, 2008.

[28] C Delgado, M Rosengrant, H Steinfeld, S Ehui, C Courbois, Livestock to 2020: The Next Food Revolution, 2020 Vision Discussion Paper 28, Washington, DC: IFPRI, FAO, and ILRI, 1999

[29] LJ Unnevehr, N Hirschhorn, Food Safety: Issues and Opportunities for the World Bank. World Bank Technical Paper No 469,Washington, DC,2000

[30] MJ Alvarez, A Alvarez, A Oses, MC de Maggio, Trombetta M, Setola R. Food Defense: Protection of the Food Supply Chain Against Criminal Manipulation and Terrorist Attack. European Food Supply Chain.Available at: http://www.thei3p.org/docs/events/ifip2010/secufoodpresentation.pdf http://secufood.unicampus.it

[31] E Yoon, CW Shanklin. Food terrorism: Perceptional Gaps Between Importance and Preventive Measures. Journal of Foodservice Business Research, **10**(2007):3-23

[32] M Roberts. Role of Regulation in Minimizing Terrorist Threats Against the Food Supply: Information, Incentives, and Penalties. Minn JL Sci Tech,**8**(2006):199-223.

[33] Food Safety Law (Official Gazette of the Republic of Serbia No. 41/09), 2009

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-190

Potential Vulnerability and Threats of Natural Disasters or Malicious Human Activity to the Water Supply Network: A Case Study of Chernivtsi, Ukraine

Igor WINKLER [a,1] and Alla CHOBAN [a]
[a] *Yu. Fedkovich National University of Chernivtsi, Chernivtsi, Ukraine*

Abstract. The potential vulnerability of the Chernivtsi water supply systems is analyzed in light of some basic shortcomings committed in the general planning, the poor realization of the project and some natural conditions imposing potential threats. Also the potential threat of intentional and unintentional human malicious activity is evaluated. Two potential strategies of mitigation are considered: the deep restructuration of the water supply system and some minor targeted steps aimed at the minimization of the threats. The latter option requires a smaller investment and promises quite reliable results in the short-term prospect.

Keywords. municipal water supply system, vulnerability/risk analysis, mitigation of potential terrorist threat

Introduction

Water supply infrastructure and food chains have suffered regularly from various terrorist attacks, natural disasters and malicious activities since very ancient times. Descriptions of water supply sources contamination during ancient wars or conflicts can be found even in the Bible (Exodus 7:14-25), when it refers to one of the Egyptian Plagues depicting the water of Nile turning into blood. This case can be interpreted as a poetic expression of the water disaster that made the water useless and undrinkable. Besides, the Bible also refers to finding a water well at Marah (Exodus 15:23-25), which was undrinkable because the water was 'bitter' (probably, contaminated?). It is interesting that using an unidentified tree, Moses removed this contamination and made the water 'sweet', i.e. drinkable.

Water supply objects are very appealing for potential malicious activity because they usually occupy significant land areas, which are quite hard to protect. Potential water/food contamination can affect many victims and cause serious devastation at the enemy's side. Comparatively simple and quite feasible actions can cause critical human casualties and/or financial, reputational and other losses. The long-term psychological effects of successful terrorist water contamination also should not be underestimated. Potentially, such kind of terrorist activity can be undertaken by various domestic and international terrorist groups with a wide range of motivation and by 'lone wolves', still with a very wide range of motivation.

[1] Corresponding Author: Dr. Igor Winkler, Yu. Fedkovich National University of Chernivtsi, Chernivtsi, Ukraine, e-mail: wigor@hotmail.com

There are numerous possible attackable targets all along the water supply and transportation system. A terrorist can attack either water supply reservoir/body or contaminate water processing chemicals or equipment, inject the toxic agent at any point along water transportation pipes. Various water pumping or processing equipment can be damaged in order to worsen the drinking water quality and that is equal to its contamination. On the other hand, a range of potential contamination agents is also quite wide and can include any species (or their combinations) of the three groups: biological, chemical or radioactive.

As an example, the following unsuccessful or partially successful water contamination attempts undertaken recently within the USA and can be mentioned [1].

A drinking water supply reservoir was contaminated with poisonous chemicals and some safety caps and valves were found removed in North Carolina in 1977. The malicious actor has not been identified and no serious hazard was inflicted because of the significant dilution of water on its way from reservoir to the end user.

An individual criminal contaminated the water mains with a poisonous weed killer agent in Pittsburgh in 1980. Again, no serious harm was caused because of the significant drop in the chemical concentration on the way to the end user.

These failures probably showed the pointless character of any individual attempt to contaminate a public water supply system chemically. Among other factors, multiple dilution of the drinking water during its production and transportation causes the inefficiency of chemical contamination agents.

Biocontamination was more successful and more than 750 persons suffered from the salmonella contamination of water tanks and food in some cafés performed in Dallas by followers of the Rajneeshee religious cult in 1984.

Radioactive plutonium was identified in the drinking water in New York in 1985. However, its concentration and activity was too low to cause any serious problems. The source of the contamination has not been identified.

As computer technologies become more involved in the water treatment processes and technology, this potential target attracted the attention of malicious groups and specialized computer viruses and spyware were detected in the drinking water production control system in Harrisburg, Pennsylvania (2006). These viruses could potentially lead to uncontrollable release of chlorine at the stage of water disinfection.

A similar approach was employed in Willows, California in 2007. Computer viruses influenced the normal functioning of the water distribution equipments and valves and diverted the water supply from its normal way.

Even though most cases of deliberate intrusion in the water production and distribution processes failed or were left ineffective, a simple attack that causes the disruption in the normal water supply is capable to bring great disorder and, therefore, it remains attractive for the terrorist activity.

Some natural and unintentional contamination of the drinking water sources can also be mentioned [2, 3].

More than 5 million tons of highly concentrated brine was discharged from the Stebnyk (Ukraine) wastewater and slurry storage pond of the local mineral fertilizers plant after heavy rains on September 14, 1983. The brine rushed into small local streams, then – to rivers and reached the river of Dnister. This contamination seriously damaged the local biota and made the Dnister water technologically and agriculturally useless. Several cities including Chernivtsi using Dnister as a source for water supply, were out of drinking water during several days or weeks until the contamination spot passed the water intake area. The brine travelled about 450 km down the river until it reached the Dnister hydropower plant dam (see Fig. 1) and remained in the bottom water layer during several years. Small portions of the brine were pumped out regularly from the bottom area and released across the dam after significant dilution with the river water.

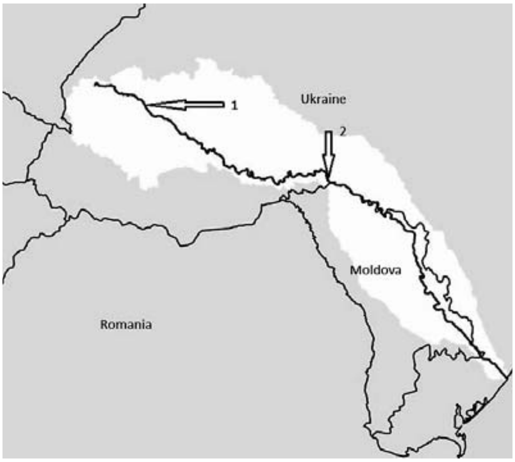


Figure 1. Map of the Stebnyk contamination along the river of Dnister (bold line) from the outbreak point (1) to the hydropower plant dam (2).

Severe contamination of river Tisza happened in 2000 because of a massive outbreak of wastewater containing high amounts of cyanides and heavy metals from a Romanian ore refining factory to one of the Tisza's tributaries, Szamos. About 100 000 m^3 of wastewater containing about 1000 tons of cyanides were discharged to Szamos and formed a 150 km long contamination spot [4]. Initial cyanides concentration in Szamos was 600 times over the maximum permissible concentration, then – 300 times in junction of Szamos and Tisza and then 30 times (on leaving of Tisza from Ukraine) [5]. This contamination also left many settlements out of drinking water for several days or weeks. Of course, serious damage to any fisheries in Tisza lasted several months or years until the complete natural decomposition of cyanides and washing off the heavy metals ions.

Similar but less influencing accidents happened in the Tisza region during next years as well.

Therefore, we believe that a thorough analysis of any water supply infrastructure should be performed in order to find and characterize the weakest points of the system. Then some mitigation activity can be targeted onto the identified critical points in order to enhance the level of their protection.

Such a case study has been performed for the Chernivtsi water supply system.

1. Current structure of the drinking water production and transportation system in Chernivtsi

The drinking water supply system of Chernivtsi is fed mostly from the open sources. Only an insignificant amount of the source water is taken from the ground wells. There are two main sources of the drinking water supply to Chernivtsi: near and under the riverbed water intake trenches at the river of Prut (minor) and open river canal water intake at the river of Dnister (major).

Most water processing, pumping and transportation equipment can be grouped into the four classes:

- water intake installations;
- pumping stations;
- water processing equipment and installations;
- water transportation and distribution network.

The minor Prut water supply plant is located near the city of Chernivtsi and pumps water directly to the city water supply network. The major Dnister water supply plant is located far away from the city and pumps water to Chernivtsi through the 42 km long water main over the 200 meters height difference. Three cascades of the pumping stations were built in order to ensure water transportation across such a complex relief.

There are several technological shortcomings in the Chernivtsi drinking water supply system inherited from the Soviet times when it was developed and put into practice.

1.1. Prut water supply plant

This is a low capacity water intake supplying only about 25 % of the current city needs. Water is partially collected in the near-riverbed trenches and galleries fed by infiltration of the river water. The water quality is considered good, close to the groundwater purity. However, these installations have been flooded several times during high water periods, which are quite often for Prut. As a result, part of the water infiltration installation has been damaged and the direct river water intake was employed to fill in the deficient water balance.

A composition of the surface river water is more unstable and is influenced by the atmospheric precipitations and run-offs. On the other hand, the water processing technology remained unchanged, adjusted to more stable filtered water.

Therefore, a potential threat of the non-intended water supply problems can be identified because of the possible worsening in the river water quality caused by intense storms or the upriver emergency discharges.

Besides, the water treatment technology seems quite outdated. It includes the following stages [6] (see Fig. 2):

- first stage water pumping station (1);
- coagulation reagents storage (2) and mixing (3) equipment;
- flocs formation vortex chamber (4);
- horizontal settler (5);
- filtration equipment (6);
- disinfection reagent equipment (7);
- drinking water reservoir (8);
- city distribution water pumps (9).

Such a technology has been designed for the relatively clean water and it cannot ensure the removal of various chemical pollution agents and some persistent microbes that are usually present in rather polluted water sources today. This is another potential threat of the surface water intake technology. It should be clearly understood that there is a great probability that any deliberate or even non-deliberate bacteriological contamination would not be identified immediately and many persistent microorganisms will travel to the local water distribution system before they can be neutralized. An outdated chlorine disinfection technology no longer uses the chlorine gas but employs less toxic hypochlorite compounds. However, this agent still cannot ensure the safe disinfection level and many hazardous spores and microbes survive after this stage. Besides, a number of toxic products of the organic pollution agent chlorination still can form after application of the sodium hypochlorite technology.

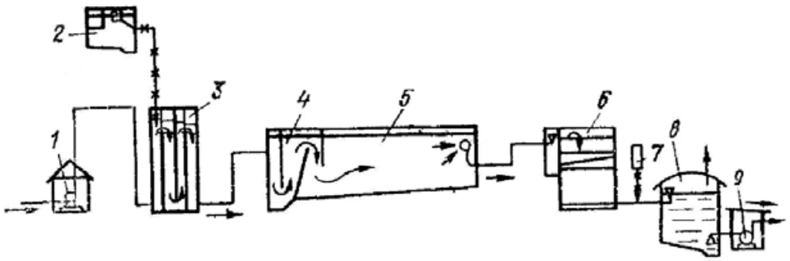


Figure 2. General plan of the 'classical' water treatment stages employed in Chernivtsi. All markings are expressed in the text.

On the other hand, due to the 'hypochlorite method' usage, a potential threat of the highly toxic chlorine gas leakages or emergency discharges is already eliminated.

In our opinion, the fully or partially chlorine-less disinfection technologies can help to lower the above mentioned potential threat of the deliberate or non-deliberate water contamination. Ozonation is an advantageous yet quite costly solution. Many technological and threat-mitigation issues can be resolved by using this method.

The disinfecting ability of ozone is much more effective than that of any chlorination agent. Therefore, no high ozone concentration is required to provide the water cleaning. A wide variety of organic water pollutants are oxidized effectively by ozone and form the poorly soluble products that can be easily filtered out at the next water treatment stages. Byproducts of such oxidation are not so toxic as products and byproducts of the chlorination technologies. Any excessive ozone transforms into oxygen and does not result in any bad odor or taste of the water. Most of the organic pollution agents can be eliminated through the ozonation [7]. Besides, it eliminates even persistent microbes and spores and does not influence the mineral composition and pH of the water. To reduce the high cost of the ozonation technology, it can be combined with the weak chlorination of water before ozonation. In this case, the pre-chlorination technology ensures preliminary disinfection and partial decomposition of the chemical pollutants while the persistent microorganisms and hazardous chlorination products will be destroyed during the next ozonation stage. Such a technology ensures the significant reduction in the ozone consumption and lowers the total cost of the water treatment.

Therefore, the results of many potential threats and malicious activities can be significantly mitigated by the pure ozonation and mixed chlorination/ozonation technologies. Of course, a system of the microbiological and chemical water quality monitoring can also prevent many dangerous situations but not all possible attacks or technical failures. In this context, an introduction of the ozonation stages would ensure the permanent but unspecified protection against these threats.

1.2. Dnister water supply plant

The Dnister water supply plant supplies the major part of the drinking water to Chernivtsi across the 42 kilometer water mains. It consumes the surface river water since the river of Dnister was considered one of the cleanest in Europe at the time of designing and construction of the water supply system (1970s). Unfortunately, the Dnister water condition has seriously worsened since that time and now this water is no longer considered clear enough.

Excessive turbidity and colorization of the Dnister water are the key issues to be solved in course of the drinking water production. Great concern is paid to these water quality parameters because they are caused mostly by excessive silt and clay microparticles content in the water. They effectively adsorb the majority of the water pollution agents including the heavy metals ions.

Some average water quality parameters for the river Dnister near Chernivtsi water intake point are shown in Table 1 [9].

As seen from the data of Table 1, major attention should be paid to the excessive turbidity that can be achieved by the clay particles flocculation and filtration. On the other hand, coloration and COD are close to the required values and no extensive efforts are expected in order to bring them in accordance to the legislation.

Traditionally, aluminum sulfate $Al_2(SO_4)_3 \cdot 18\ H_2O$ is used for the clay/silt coagulation. However, the residual concentration of Al^{3+} ions after the water clearing stage can reach a half of its maximum permissible content or even more (see Table 2) [9]. This problem brings a potential threat of the water chemical contamination resulted by deliberate or non-intentional over dosage/under dosage of the water clearing reagent.

Table 1. Some parameters of the Dnister water vs. actual requirements towards the drinking water in Ukraine

Water category	Turbidity, mg/l	Coloration, degree	pH	Al^{3+}, mg/l	COD, mg O/l
Raw Dnister water	57	27	8.59	-	5.7
Drinking water*	0.58-2**	20	6-9	0.5	<5

* - required by the actual Ukrainian standard “DSanPiN 2.2.4-171-10 – Drinking water: hygienic requirements” [8]

** - depending on the season and region, the limit value of turbidity (0.5 mg/l can be temporarily raised to 2 mg/l) - acting until January 1, 2020

As seen from Table 2, the lowest residual Al^{3+} content can be achieved after application of 30 mg/l of $Al_2(SO_4)_3 \cdot 18\ H_2O$. This amount ensures coloration meeting the “DSanPiN 2.2.4-171-10” requirements and turbidity that partially meets the requirements. However, even this lowest residual content makes more than half of the Al^{3+} maximum permissible concentration. Therefore, in the case of the treatment of water with relatively high natural content of Al^{3+}, it is quite easy to exceed this limit value. Application of 40 mg/l of $Al_2(SO_4)_3 \cdot 18\ H_2O$ makes the turbidity fully compliant with the requirements but in this case the residual Al^{3+} content almost reaches the limit value. On the other hand, under dosage of $Al_2(SO_4)_3 \cdot 18\ H_2O$ is also potentially dangerous because application of 10 mg/l results in the excessive residual content of Al^{3+}.

Table 2. Some parameters of the Dnister water after the application of aluminum sulfate as a clay/silt flocculation agent

$Al_2(SO_4)_3 \cdot 18\ H_2O$ applied, mg/l	Turbidity, mg/l	Coloration, degree	Residual Al^{3+}, mg/l	pH
10	20	25	0.66	7.95
20	3	20	0.46	7.92
30	1.3	10	0.26	7.59
40	0.9	5	0.42	7.50
50	0	5	0.48	7.45

Table 3. Some parameters of the Dnister water after application of Polvak-86 as a clay/silt flocculation agent

Polvak-86 applied, mg/l	Turbidity, mg/l	Coloration, degree	Residual Al^{3+}, mg/l	pH
10	9.8	25	0.19	8.23
20	2.5	15	0.14	8.24
30	0.6	5	0.12	8.20
40	0	0	0.08	8.32

This potential problem can be mitigated by the using of another coagulation reagent instead of the pure $Al_2(SO_4)_3 \cdot 18\ H_2O$. For instance, the special coagulant Polvak-86 proves much higher efficiency. Polvak-86 is a complex aluminum hydroxochloride $Al(OH)_aCl_b$ with a+b=3 and a>1.05. Its efficiency is shown in Table 3. As seen from this Table, the residual contents of Al^{3+} are significantly lower for Polvak-86 and coagulation efficiency is much better comparing to the pure aluminum sulfate. Besides, the acidification effect of Polvak-86 is weaker than that of $Al_2(SO_4)_3 \cdot 18\ H_2O$.

Comparative analysis between the data of Table 2 and 3 proves that 30 mg/l of Polvak-86 provides the required water clearing degree and leaves rather insignificant residual Al^{3+} in the treated water. Therefore, this reagent ensures a better water clearing degree and mitigates the potential threat of the water chemical contamination by excessive aluminum.

Transportation of the drinking water over the 42 km long pipe brings some other security problems.

There are some ground shift-dangerous areas under the water pipe. Several ground shifts has happened and serious pipes ruptures seriously disturbed the water supply regime. To avoid this potential danger, parts of the water main were rearranged within the shift-dangerous areas and placed on the ground instead of the underground construction used previously. A special ‘slipping pier’ construction was designed to ensure security of some small ground shifting under the pipe. This way the water mains become more rupture-proof although its general security decreased. It can be seen that such open parts became an easily available target for any potential malicious human activity directed onto a deliberate break of the water main.

Pumping the water across 42 km mains and over 200 m of height difference requires quite significant energy and powerful, low adjustable pumps. As a result, this regime of the water transportation is highly energy consuming and very vulnerable by the energy supply problems. This is another potential security hole in the Dnister water supply infrastructure.

2. Increasing the stability potential of the entire water supply system of Chernivtsi

Chernivtsi is a city with a rather hilly relief and several intermediate water buffering reservoirs were operated inside the city in order to smooth the water pressure along the supply system. Then they were gradually disconnected and taken out of service in the late 1990s due to financial reasons. As a result, the water supplier had to increase the entrance water pressure up to 6-8 bars to ensure its passing across all parts of the distribution system.

In our opinion this situation is potentially dangerous because any break in the inner city distribution network would (and in fact it did) cause severe water losses and hardly repairable damages. On the other hand, keeping such a high pressure requires additional electricity consumption during the peak period. The intermediate water reservoirs can be filled during the off-peak period and the required water pressure can be lowered to 2-3 bars. This way, significant amounts of the costly high-peak electricity can be substituted with the cheaper off-peak energy and potential ruptures would be less dangerous.

3. Conclusion

The following potential vulnerabilities and corresponding mitigation steps can be identified in the Chernivtsi water supply network:

- vulnerability of the outdated water disinfection technology (fixed partially by the substitution of chlorine gas with the hypochlorite salts and can be fixed completely by switching to the ozone or combined ozonation/chlorination disinfection technology);
- vulnerability of the remote Dnister water intake system supplying most part of the drinking water from the low quality source (fixed partially by application of more advanced coagulants and can be fixed completely by total substitution of the Dnister water with new underground water intakes constructed near the city);
- vulnerability of the water distribution system operating currently under high pressure (can be fixed completely by return to use of the intermediate buffering water reservoirs).

It can be concluded that the above steps would not require any ‘global’ reconstruction of the water supply system, rather minor changes. Therefore, a comparatively low finance investment can ensure its better protection against technical problems, natural disasters and malicious human activities.

References

[1] The potential terrorist risk of drinking water contamination. in: Office of Homeland Security and Preparedness . Intelligence Bureau. Report on January 6, 2009. https://publicintelligence.net/the-potential-terrorist-risk-of-drinking-water-contamination/ Accessed April 04, 2014

[2] Stefanyshyn D (2009) Probability assessment for the river hydroinstallations emergencies caused by extreme weather conditions. Environmental Safety and Nature Management 4:28-48 (In Ukrainian).

[3] Winkler I (2011) Ukraine and Romania: Transboundary environmental security and ecology of shared water resources. In: Hami Alpas, Simon M. Berkowicz and Irina Ermakova (eds) Environmental Security and Ecoterrorism, 157-169, Springer.

[4] Laszlo F, Csanyi B et al (2001) Cyanide and heavy metal accidental pollution in the Tisza river basin: consequences on water quality monitoring and assessment. In: Proceedings of Monitoring Tailor-Made. III International Conference, 65-70.

[5] Toth J (2004) Social responsibility in pollution: the case of the Tisza river. Human Ecology 12:143-147.

[6] A concept of Chernivtsi water supply (1998). Alekto, Klagenfurt. (In Ukrainian).

[7] Papageorgiou A, Voutsa D, Papadakis N (2014) Occurrence and fate of ozonation by-products at a full-scale drinking water treatment plant. Science of the Total Environment 481:392-400.

[8] Directive of Ministry of Public Health of Ukraine: Implementation of the state sanitary regulation of the drinking water quality parameters SanPiN 2.2.4 – 171-10 (2010). http://zakon2.rada.gov.ua/laws/show/z0452-10/page2 Accessed April 11, 2014

[9] Choban A, Kulish V, Choban S (2007) Efficiency of analysis of the water treatment station “Vikno” and search of the new water clearing reagents for the Dnister water. Sci. Bull. Chernivtsi University 364:129-135 (In Ukrainian).

Section 4:
Energy Security as a Key Factor of Critical Infrastructure Protection

This page intentionally left blank

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015

© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-201

Tailor-Made Education: Environmental vs. Energy Security and Sustainable Development Paradigm

Vesna NIKOLIĆ [a,1] and Dejan VASOVIĆ [a]
[a] *University of Nis, Faculty of Occupational Safety in Nis, Serbia*

Abstract. The term security, in the narrow sense, represents the degree of safety in terms of protecting a nation, a people, or individuals from danger, damage, or crime. Structures that raise the security level constitute elements of security as a form of protection in the technical sense. Analysis of relevant scientific sources clearly indicates that a form of protection is where a separation is created between the assets and the threat. Such a definition implies a dual conclusion – that the security level can be raised either by eliminating, i.e. reducing, the threat (technical sense of security) or by eliminating the asset, i.e. by reducing subjective perception of what the asset to be protected is (the threat has no effect if there are no assets to be threatened). The global dimension of environmental problems and sustainability, in particular the seriousness of various risks and security threats to the operation of the critical infrastructure of a state implies the need for new educational approaches and content in this area. In a significant number of European countries, the goals of teaching and education in general have been innovated and redefined by the introduction of tailor-made training modules and courses regarding the abovementioned environmental and energy security. In parallel with socio-economic transitions, countries in transition should also take certain initiatives for change in the education system. In this sense, this paper discusses the problems of environmental and energy security and opportunities offered by formal and informal education within this area. Special emphasis is given to the issues of the tailor-made education of personnel operating within critical infrastructure facilities. Pertaining to this goal, the organization of diverse educational and informational/promotional activities in this field is of equal importance.

Keywords. tailor-made education, environmental security, energy security, sustainable development, formal education, informal education

Introduction

Contemporary lifestyle and production methods lead to the significant usage of all kinds of energy in industrial, agricultural, and other production activities depending on energy-demanding technological systems. Despite the obvious terrorist threats to critical infrastructure, due to the abovementioned requirements, the transportation of energy and other material goods is inevitable. Due to the fact that proper planning and maintenance of different kinds of critical infrastructural elements rely on proper pre-education, a significant series of educational initiatives should be considered as a necessary prerequisite to reduce the risk of terrorist threats, thus directly reducing the potential damage.

[1] Corresponding Author: Dr. Vesna Nikolić, University of Nis, Faculty of Occupational Safety in Nis, Carnojevica 10a, 18000 Nis, Serbia, e-mail: vesnik08@gmail.com

1. Sustainability Concept

Sustainable development is a very complex issue embedding different disciplines ranging from biology, engineering, law, economics, and politics to education [1]. The main pillars of sustainable development: institutional, legislative, and educational development coupled with both socio-economic and environmental development could be significantly enforced by introducing key determinants of modern society's continual manufacturing improvement and corporate education. With regard to the abovementioned tailor-made education process from the discourse of sustainable development, it is necessary to evaluate both the basics of sustainable development and the international legislation and practice in order to make the connection between sustainability, energy security, environmental security, critical infrastructure and the ever-present terrorism threats.

Sustainability has a double binding: for humankind and for the environmental perspective [2]. In relation to humankind, sustainability implies both the quality of life and inter- and intra-generation justice. Contemporary literature analysis shows that sustainable development may be seen as a social ideal which should establish regularity in improving human social status. Observed from the aspect of authors, education and learning for energy and environmental security is not viewed as a practice for the purposes identified by politics and economics [3]. Facts, seeking self-determination in the discussions, in dialogue with the theory and practice of the modern phenomenon of terrorism threats to management, are important for organizational learning and critical infrastructure employees who are subjected to education. The question is whether the debate on sustainable development can draw more than merely cosmetic changes in the forms and topics of learning and teaching. What are the possible directions of development of education in our country? Can we in the present social turmoil be able to find a positive education formula, but also be open to the tendencies of modern society? The sustainable development discourse is perceived as language on the culture turnaround, which is far more subtle than that in which scientific research and the maxims of equity were drivers of the reform. The presented model of tailor-made education promotes sustainable development discourse as a field in which its expression crosses advanced and innovative theories and techniques, values, and cultural trends that will follow the basic principles of sustainable development in the sense of environmental protection and the establishment of a secure culture. From the energy and environmental security perspective, and taking into account the discourse of sustainable development, we can adhere to the following:

- In a particular organization and culture, the problem of education is perceived as an important theme in the discourse about the environment,
- The discourse of sustainability is used to identify people who are interested in education,
- The premises of sustainable development that are important for the educational context are examined,
- New patterns and trends, not just the discourse of sustainable development, should be the basis for the structural reform of education and learning,
- Education increasingly promotes the trend of individuality and the broader participation of stakeholders.

2. Environmental Security Concept

In a narrower sense, environmental security refers to determination and the qualitative and quantitative expression of the connections between environmental determinants and the level of anthropogenic security, particularly between the environmental determinants that can considerably influence the level of security, such as natural disasters that may lead to water shortage and famine and their effect on the security of people and social structures. In a broader sense, the concept of environmental security goes beyond physical security and also encompasses the definition of security attributes, food security, health aspects of security, and environmental safety of other populations. Another, extended, concept has its roots in the dual extension of the definition of military security and the development of new ideas pertaining to the quantification of environmental risks, and in the challenges of the Millennium Project and the aspects of sustainable development. The main concern in such an understanding of environmental security is the potential of environmental degradation, which can lead to violent conflicts, which reflects the military "spirit" of this concept [4]. Such a concept acknowledges and studies the relationship between global changes occurring in the environment and their quantifications by means of various models, which is why it became the focus of scientific research. It is important to bear in mind that nowadays certain parts of the world represent potential critical zones where the level of environmental degradation can be so severe or widespread that it endangers human life and property. The majority of these critical zones are located in Sub-Saharan Africa, the Middle East, and specific parts of southern Asia [5]. The potential for environmentally-induced conflicts is present in these areas, where population displacement is one of the effects of environmental degradation [6].

Bearing the aforementioned in mind, environmental security needs to be interpreted dually in any future research. On one hand, environmental security implies a possible level of hazard to people and property stemming from various environmental occurrences, while on the other hand it represents a level of hazard to the environment stemming primarily from the usual impact of economic activities on conflicts between different nations. Within the Millennium Project, it is possible to find a definition that presents environmental security as the continual sustainability of environmental elements that are fundamental for life preservation, in terms of:

- Prevention or reduction of the environmental impact of military operations,
- Prevention of international conflicts caused by the right to environment,
- Environmental protection as a moral obligation.

When observing the concept of environmental security in the broader sense, it is important to remember the fact that humankind has always been faced with various environmental risks, whether they were natural disasters or anthropogenic industrial-technological accidents. Even though natural disasters are considered to be inevitable, from the aspect of endangering people and property, they can be classified as situations affecting the level of environmental security only if they directly or indirectly endanger people and property. A storm or an earthquake striking an uninhabited area without any material human structures cannot be considered to be causing risk. The situations considered influential in terms of environmental security are exclusively those that in a certain way involve people and property. This category also encompasses all catastrophes caused by a human factor as well as wars. Accordingly, the following could be listed as reasons for a noticeable increase in the number of people and areas afflicted by some sort of hazard (floods, fires, or industrial accidents): change of climatic conditions on Earth that inevitably lead to more frequent and intense natural disasters on the one hand, and increased human settling of the areas that have previously not contained any human settlements, so there are fewer and fewer unsettled areas, to which the term environmental security does not apply (it is unnecessary to assess environmental security when it is not, in fact, an environment but a specific physical space).

3. Energy Security Concept

Energy security is a state associating national security and the availability of energy resources that are to meet national energy needs [7][8]. From the environmental perspective, energy security is the level of protection of energy infrastructure against various environmental influences (e.g. landslides or floods), whereas from the energy infrastructure perspective, energy security is the level of environmental protection against various influences of energy infrastructure (either during regular operation or during emergencies). Considering that energy security implies autonomy, i.e. the least possible dependence on energy import, promotion of the energy security concept includes the promotion of renewable energy sources, as well as more efficient utilization of the existing resources (polygeneration), which is a trend of energy-economic models [9]. Energy security also implies the continuity of energy production and distribution; accordingly, reliance on non-renewable energy sources lowers the level of national energy security [10]. In terms of prices, access to relatively low-cost energy is a pillar of economic development, so a high level of energy security implies low prices but also the absence of price fluctuation [11].

Energy security aspects and the set of energy security indicators can be divided or categorized based on the principle of division [12][13] but the most common categorization is the one involving a dominant share of geopolitical and economic indicators, whereas reliability indicators and environmental (ecological) indicators are less represented, as shown in figure 1.

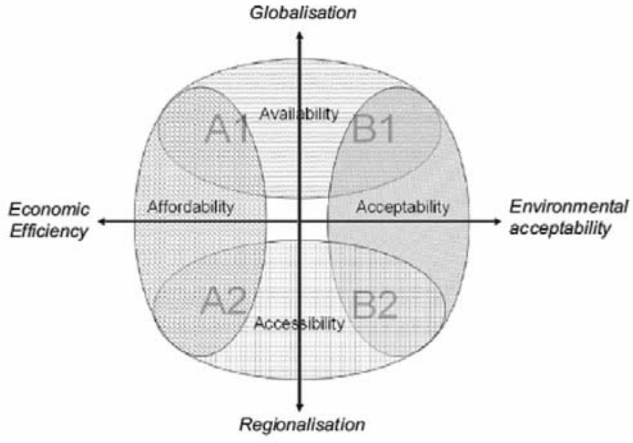


Figure 1. Aspects of energy security [14].

The significance of energy security has also been recognized in a number of scientific publications studying the importance of energy security and energy sector implications at the national and supranational level [15][16]. Figure 2 shows how the energy sector of one country or region is related to other critical infrastructural elements of society, such as water supply, transport, telecommunications, finance, food supply, etc.

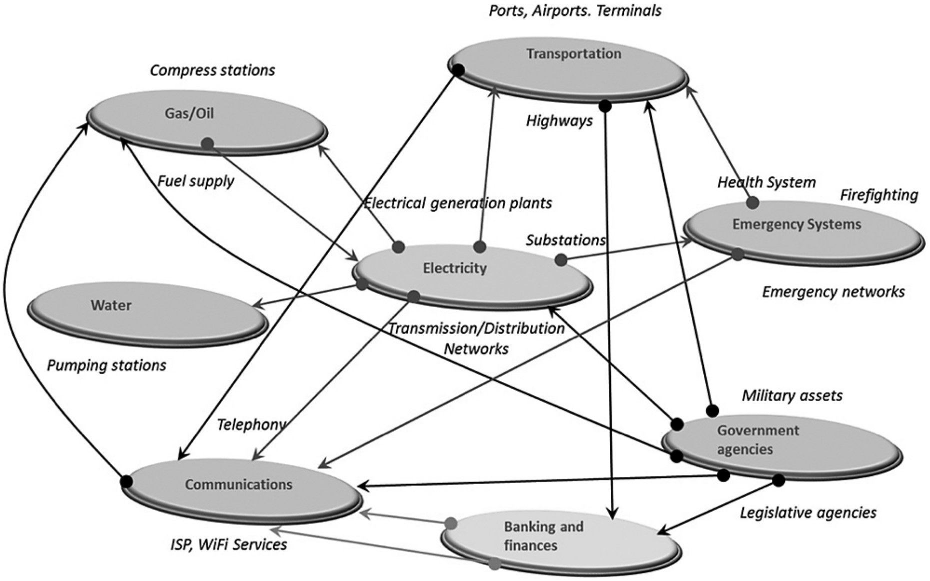


Figure 2. Example of interdependence between energy systems and other critical infrastructure [17]

There are numerous examples of social initiatives to improve national energy security. For instance, many Asian's countries, particularly Japan [18], are implementing intensive programs to promote renewable energy sources and polygeneration, primarily in order to reduce the dependence on energy import but also to obtain energy that will have price continuity [19].

4. Education as an Instrument of Critical Infrastructure Protection and Sustainable Development

4.1. A Review of the Conceptual Definition of Critical Infrastructure

When defining critical infrastructure, the European Union distinguishes between national critical infrastructure and European critical infrastructure. Both terms refer to a property or a system in a Member State that is necessary to maintain key social functions, healthcare, safety, security, and economic and social well-being – the only difference being the ultimate effect. In regards to national critical infrastructure, any destruction of or damage to critical infrastructure would significantly impact the Member State in which it is located, whereas in the case of European critical infrastructure, the impact refers either to two or more Member States or to one state which does not contain the critical infrastructure [20].

So far, no clear criteria for identifying critical infrastructure and no supporting regulatory framework have been established in Serbia. Analysis of Serbian legislation indicates a lack of definitions of critical infrastructure, as opposed to the terms 'infrastructure' and 'infrastructure systems', which are defined in numerous laws pertaining to regulation in specific parts of infrastructural systems (e.g. the Law on Planning and Construction defines linear infrastructure facilities and utility infrastructure, *Law on Planning and Construction, Official Gazette of the Republic of Serbia, No. 72/2009, 81/2009, 24/2011, and 121/2012*) [21]. In the broadest sense, the term critical infrastructure implies instruments and property that are crucial for the undisturbed functioning of the economy and the society. The Law on Defence (*Law on Defence, Official Gazette of the Republic of Serbia, No. 116/2007 and 88/2009*) [22] defines facilities of special relevance for defence, which include certain critical infrastructural facilities, whereas the Law on Emergency Situations makes no mention of critical infrastructure even though it covers the establishment of protection and rescue systems for people and material and cultural wealth (*Law on Emergency Situations, Official Gazette of the Republic of Serbia, No. 111/2009 and 92/2011*) [23]. However, based on the Law on Emergency Situations, the Serbian Government passed the Regulation on the content and elaboration of protection and rescue emergency plans, which, among other things, included the risk assessment for critical infrastructure in terms of natural disasters and other major accidents in the Risk Assessment section. This Regulation thus introduced the term critical infrastructure in Serbia, but still without a clear definition of which elements or areas of infrastructure the term refers to.

The term critical infrastructure is included in the National Strategy for Information Society Development until 2020, where the critical infrastructure protection within information security is listed as a priority. The phrase 'critical infrastructure protection' implies the ability to *prepare, protect, mitigate, respond to, and recover* everything related to critical infrastructure damage or destruction [5].

The EU has made considerable efforts in analyzing critical resources and has adopted a series of documents pertaining to the protection of the critical infrastructure. The European indicative list of critical infrastructural sectors lists eleven sectors whose protection is of special significance for society and civilization: energy; information and communications technology; water; food; healthcare; finances; public and legal order and safety; state administration; transport; chemical and nuclear industry; and space research. For instance, energy system facilities are utilized daily and any interruption of their operation or their destruction can produce severe consequences for people, society, nature, and the environment in general. Energy resources can be endangered by breakdowns, natural disasters, individual sabotage, enemy activity by another country, or acts of terrorism. After an analysis of the importance of the energy system as a part of the critical infrastructure of our country, the significance of education as the basic preventive measure in the system of integral safety and protection against fires, breakdowns, floods, and other catastrophic events on the one hand, and from terrorist attacks, larceny, breaking and entering, etc. on the other hand becomes clear.

4.2. Basic Fields and Goals of Formal and Informal Education

The strategy of education for security and the protection of the critical infrastructure and of the environment in general is viewed and determined within two basic theoretical-methodological and developmental frameworks: the concept of lifelong learning and the strategy of sustainable development. Understood in its essence, education should contribute to the development of capabilities and readiness of each community member for hazard and risk prevention, environmental protection, and sustainable development in the future [24].

Systemically speaking, education for prevention of risks and threats to the security of critical infrastructure and the environment in general has a dual manifestation according to its didactic goals – as environmental protection and, at the same time, as protection of people and property in the working and living environment. Therefore, this activity encompasses a broad educational population from children and youth to adults in all formal and informal types of education. This means that education in this field occurs fairly extensively with more or less intensity, in different group and individual educational forms, and with different pedagogical-andragogical approaches and didactic-methodological modalities.

However, in terms of pedagogical-andragogical differentiation, two basic educational populations stand out: children and youth within a school system and adults in all aspects of social life and work. The framework didactic concept in the implementation and realization of the content of education for environmental security implies the realization of educational goals and tasks in early childhood, directed towards the development of security culture[2] and safe behaviour, whereas acquisition of knowledge and skill development for the prevention and protection of risks, hazards, and threats of different nature and type in the working and the living environment (as well as the terrorist threats, *Author's Note*) should be conducted in the later stages of formal education, especially professional education (secondary vocational schools or higher education institutions) and education through work[3].

Didactic concentration of educational content should be moving from general to particular and individual or from an integral (inter-subjective) to an autonomous (subjective) didactic-methodological type of instructional work. In fact, this framework concept implies curricular changes in order to give a proper place to the issues of security in the educational system. Of course, this raises the question of preparedness and preparation of teachers for both their subject teaching and integral work types (teachers should enrich their syllabi with content from occupational safety, fire protection, environmental protection, and other occupational and environmental safety issues in accordance with compatible content from their subject's content and other educational activities). Current issues also include the determination and modernization of the material, technical, and didactic foundations of education in this field, i.e. appropriate textbooks/handbooks and other informational-advertising material and tools or general educational technology that would help implement this content [25].

[2] In agenda 21, the term 'security culture' implies raising the capabilities of society and individuals to behave adequately in case of accidents and to pre-emptively prepare preventive and recovery measures.

[3] For instance, preschool education includes the following: education and upbringing of preschool-aged children to develop basic health, work, and ecological habits; the acquisition of basic terms and concepts of nature and the environment, of what is dangerous and harmful, good and bad, beautiful and ugly, etc.; the formation and development of ecological and safety awareness, security culture, and safe behavior, particularly during hazards, crises, or emergencies (e.g. in case of fire, flood, earthquake, terrorist and other armed attacks, and the like). Primary education is directed towards the following: health and security culture, work habits, and the development of basic work culture elements (culture of work and behavior); the acquisition of knowledge about nature, the world, ecological problems, various security challenges and threats, and the need for protection of people and natural and material wealth; the development of value relationships of students towards the environment; the development of security awareness and security culture of students, etc.

In order to keep up with the times and technological and other changes, and to respond to (or actually manage) occupational and environmental risks of different nature and type, lifelong learning is necessary. Accordingly, education for security and occupational and environmental safety should be implemented not only through schooling but also through self-education and informal education. These are the three major types of learning (almost equally important in developed countries) that comprise lifelong learning. Since a large portion of education occurs outside of schools, at the places of work or residence of adults, the entire society becomes a "learning society". This particularly applies to countries in transition, which needs to be carried out by the currently active population without waiting for the modern-educated upcoming generations.

In regards to informal education, special importance lies with employee training for occupational safety, fire protection, environmental protection, and behaviour during crises/emergencies in companies and other work organizations [26].

In this respect, educational practice in Serbia contains many weaknesses and flaws (program-related, organizational, didactic-methodological, etc.). In many areas of work, education in this field is overly generalized, traditionally based, undifferentiated goal-wise, and viewed more as a category of employee rights than as an instrument for improving the security level and economic efficiency, the quality of work, and professionalism in general. Of course, a certain number of companies have initiated some changes in this respect, but the essential changes are yet to come.

In addition to organizing education for occupational and environmental safety within human resource management, the new approach to education in this field also includes the founding of internal schools, education centres, or even companies (as parts of larger companies), whose activity would be directed towards providing modern knowledge and the acquisition of skill sets for environmental risk assessment and management (including workplace and work environment risks), or towards the permanent development of employees' competencies, which would affect both their personal safety and the safety of the system, or the efficiency of the organization as a whole (smaller organizations, typical of the post-industrial age, should seek such educational services on the market – with educational service organizations) and, consequently, environmental security. There is a need for permanent education, which is not understood solely as serving environmental protection, but more extensively, as serving further development of employees, training for constructive and anticipatory thinking, problem solving, cooperation, accepting responsibility or forecasting, predicting and managing risks, hazards, and threats of a different nature and type to the working and living environment.

4.3. Development of a Model of Informal Education for Critical Infrastructure Security and Sustainable Development

Conceptual foundations of the modern educational approach imply program orientation and a compliance of educational content with the characteristics and particularities of a given organization, company, job, the nature and type of risks and hazards, and the methods, techniques, and instruments of safety and management. Table 1 shows the concept of the education model based on the need of managing terrorist threats to the critical infrastructure. We chose the energy sector as an example of the critical infrastructure, although the presented model applies to other parts of the critical infrastructure, as well.

Table 1. Timetable of activities within a short, one-semester-long education course that recognizes the need for managing terrorist threats to the critical infrastructure

(1st month)	Energy vs. environmental security	**1st week**
	Display of current critical infrastructure systems	**1st week, 2nd week**
	Analysis of data on terrorist threats	**2nd week, 3rd week**
	Analysis of current critical infrastructure systems - technical, economic and social aspects	**2nd week, 3rd week, 4th week**
(2nd month)	Analysis of available models for energy and environmental security education	**1st week, 2nd week**
	Assessment of the applicability of the model to local conditions	**2nd week, 3rd week**
	Definition of the optimal model of energy and environmental security education	**3rd week, 4th week**
	Energy vs. environmental security workshop: case studies	**3rd week, 4th week**
(3rd month)	Economic aspects of energy and environmental security education	**1st week, 2nd week**
	Necessary organizational and technical changes in the current critical infrastructure systems	**1st week, 2nd week, 3rd week**
	Action plan for the implementation of a new model of energy and environmental security education	**1st week, 2nd week, 3rd week**
	Training programs and training of decision makers and other stakeholders	**1st week, 2nd week, 3rd week**
(4th month)	Program campaign for raising awareness of the need of managing terrorist threats to the critical infrastructure	**1st week, 2nd week, 3rd week**
	Public hearing on the new model of energy and environmental security education	**2nd week, 3rd week, 4th week**
	Final assessment and evaluation	**4th week**

First month: Energy vs. environmental security: introducing course participants to the definition, interpretation, and implementation of the concepts of energy security and environmental security. Display of current critical infrastructural systems: parallel analysis of the term critical infrastructure and the existing technogenic systems that are considered or potentially considered to be elements of the critical infrastructure. Analysis of data on terrorist threats: analysis of available data on the type of current terrorist threats with an overview of previous experiences (definition of terrorism, active terrorist groups and threats, potential threats, motivating factors, objectives, and options for preventive action). Analysis of current critical infrastructural systems – technical, economic, and social aspects: analysis of the current infrastructure in terms of technological, economic, and social significance in a given society; Analysis of potential economic, technological, and social implications of terrorist activities against elements of critical infrastructure.

Second month: Analysis of available models for energy and environmental security education; Identification of advantages and disadvantages; Assessment of the applicability of the model to local conditions: objective assessment of the applicability of existing models within local or national boundaries, bearing in mind the real elements of critical infrastructure and the current practice of terrorist threat management. Definition of the optimal model of energy and environmental security education: modification and creation of an adequate model for energy and environmental security education. Energy vs. environmental security workshop: case studies: application of the defined model of energy and environmental security in case studies.

Third month: Economic aspects of energy and environmental security education: consideration of economic aspects of the adopted model of energy and environmental security education. Economic implications in critical infrastructural elements; Economic implications in society; Necessary organizational and technical changes in the current critical infrastructural systems: analysis of necessary changes and improvements in existing critical infrastructural systems (based on the feedback from the previously conducted case studies). Action plan for the implementation of a new model of energy and environmental security education: defining an action plan with a structural and temporal dimension, done individually by the now well-trained course participants. Training programs and training of decision makers and other stakeholders: final training programs for course participants with testing of the previously acquired knowledge.

Fourth month: Program campaign for raising awareness of the need of managing terrorist threats to the critical infrastructure: with the help of a moderator, course participants conduct various promotional campaigns aimed at raising awareness of the need for terrorist threat management, whereby the target groups primarily include employees at the functional units of the critical infrastructure. Public hearing on the new model of energy and environmental security education: public presentation of the results of the implementation of the model of energy and environmental security education, followed by a final assessment and evaluation, where participants are asked to provide feedback and suggestions and an objective analysis of course successfulness is performed with the adoption of measures representing positive experiences of participants.

In addition to program changes, there is a need for organizational and didactic-methodical innovations in terms of the implementation of (inter)active participating methods and forms of learning and modern educational technologies (modern media, multimedia). Such an approach to education shall create conditions (considering the direction of the educational approach towards individual users of educational services, through achieving individual results and effects in the discovering, perceiving, and recognizing of risks, hazards and threats to critical infrastructural security and in proper individual response and behaviour) for a cumulative effect to be manifested as a realization of set goals and tasks in this field on a systemic level, or for a cumulative effect to contribute to system safety and success of the organization as a whole. All of the above suggests a need for creating and developing an organization that will be capable of meeting the modern demands and needs of our time. This is actually a need to create a “learning organization” [27][28].

Being a result of the need for continuous adaptation to changes, a learning organization does not learn exclusively through a mechanical adaptation to surroundings; in fact, it prefers new and flexible management procedures and mechanisms (with emphasis on knowledge management procedures), which are better suited to handling the surroundings and other unpredictable factors and risks.

In addition to companies and other organizations of work, attention should be given to organizing informational-advertising, cultural-educational, and other types of extracurricular education and learning for the unemployed categories of educational population such as housewives, retirees, the unemployed, or the rural population (e.g. fire protection training during harvest, training for using pesticides and other chemical-biological agents, etc.).

Program- and organization-wise, these activities should involve the proper education and information centres and institutes, but also ecological societies, NGOs, and other associations and stakeholders. Accordingly, it is necessary to closely connect formal, informal, and all other types of learning and education for environmental protection in order to enable the implementation of a philosophy and practice of lifelong learning and to enable lifelong revision and upgrades of knowledge and skills in this field.

Educational system reform implies its decentralization and deregulation, i.e. abandonment of the model in which the functioning of a system is entirely under governmental control through a relevant ministry. By becoming decentralized and deregulated, the educational system is free to include many other subjects.

The establishment of interest-based partnerships generates conditions for everyone interested in a specific educational level, form, or segment to take part in its creation. In the upcoming period, all entities interested in the security issues of the working and living environments must become involved in these activities and thus allow the issues and problems of environmental security, in particular of the critical infrastructural security, to take their proper place in the educational system.

5. Concluding Remarks

Until today, the fate of the environment has never been tied to the tendency to establish global safety, peace, stability, and sustainable development. On the other hand, it is fairly obvious that there is, and there will be, no global or national development, welfare, and stability without the development of the occupational and environmental safety system and, within it, the system for managing different types of risks, hazards, and threats to the functioning of the critical infrastructure. Development of international cooperation, increased possibilities of direct contacts, constant exchange of experiences in crisis/emergency prevention and recovery, and development of scientific research in the field represent undeniable support for the dissemination of scientific results, possible solutions, and knowledge for the establishment and improvement of such a system. In this context, the primary intention, which bears paradigmatic significance, pertains to preventive measures and activities among which education has the invaluable role in realizing the strategy of safe and sustainable social development.

From the primary levels of the educational system, it is of paramount importance to establish the foundation of a proper and respectful relationship towards the issues of security and health. This is achieved through adoption of a knowledge system that will help children and youth understand and perceive that security is a fundamental human right; that security needs to be prioritized in any activity over the results of that activity; that a responsible and disciplined relationship towards security issues in every sphere and field of human work is a guarantee of safety for people, property, and natural and material wealth. In fact, all of this should form a general culture (“security culture”) of children and youth towards security issues and represent the foundation which will be upgraded as needed with further knowledge and habits during the course of education. At the secondary and higher levels of education, the process pertains to the acquisition of specific knowledge and the development of specific psychophysical characteristics, skills, and habits, or professional competencies in keeping with the requirements of cultured and safe behaviour in the occupational and the living environment (in professions and occupations for which students are trained). Naturally, special attention should be given to professional education and to education and permanent improvement of personnel who are directly or indirectly responsible for occupational and environmental safety and for crisis/emergency response.

The organization of the informal education of employees operating within the critical infrastructural facilities of a country poses a number of organizational, program-related, and didactic-methodological dilemmas of education for occupational and environmental safety. Without a new model and approach that connects occupational and environmental safety with the broader issues of managing risks, hazards and threats of different natures and types and with sustainable development problems, informal education will remain neglected with poor stakeholder support, insufficient resources, institutional instability, and limited results.

The concept of education for occupational and environmental safety, especially for the security of the energy system as a part of the critical infrastructure of a country, should rely on the policy of integral environmental quality management and as such needs to be based on the fact that energy is one of the three fundamental elements of life and that energy sources are an integral part of the ecosystem and a key factor of socio-economic development and the quality life of humans. Therefore, environmental quality and energy production and distribution should be managed as an integral part of national socio-economic development by means of a comprehensive analysis of available energy resources, energy needs, the sustainable use of energy, and the preservation of energy resources, especially the renewable ones. In the implementation of this policy, priority should be given to the activities that will first and foremost promote the sustainable use of energy resources but also the protection of the ecosystem in which the energy resources are located. On one hand, there is an interesting fact that an ecosystem knows not of state or regional borders, but on the other hand, there is an interesting fact that energy needs and energy as a resource are clearly or necessarily defined by national boundaries. Bearing all this in mind, from the fundamental goals of integral management of energy resources, sustainable development, energy security, and environmental security, it is possible to define the objectives that need to be met by the education for energy and environmental security:

- Distinction, but also mutual causality of the concepts of energy security and environmental security;
- Understanding of the elements of criticality and vulnerability of the energy infrastructure;
- Learning of the measures to reduce the vulnerability of and to protect the energy infrastructure;
- Learning and development of crisis/emergency, recovery, and rehabilitation plans;
- Planning and management of energy sector capacities and resources at the highest scientific and professional level;
- Avoidance/resolution of conflicts between different stakeholders;
- Raising of awareness about energy infrastructure protection and the involvement of stakeholders and the general population;
- Development of human resources performing jobs and tasks in critical infrastructural systems;
- Strengthening of institutional, financial, and other mechanisms that are supposed to enable the protection and preparedness of the system for the protection of the critical infrastructure or for recovery in case of a crisis/emergency.

The choice of managing activities is closely connected to the adopted approaches to managing energy and environmental security globally (UN and EU conventions, which usually serve as guidelines), regionally, or nationally (national legislation). The management of energy resources, which should proceed nationally, has to be harmonized with the fundamental principles and standards adopted internationally.

The conclusions of the thus-defined concept of education can also be used in other areas of environmental protection, such as food security, water security, military security, etc.

In any case, the identification of risks and threats to the security of the critical infrastructure, as well as sustainable development, dissemination of knowledge, and the exchange and integration of information and data on the possibilities on safety management and prevention of risks and threats of different natures and types form the necessary prerequisites for the development of a security culture and the responsibility of all subjects and factors of a social community to competently and permanently conduct preventive and operative measures and activities in order to prevent risk events, reduce their incidence and severity, and mitigate their environmental impact and effects on humans.

Acknowledgments

The research presented in this paperwork is supported by the projects III 44006 and III 42006, under the auspices of the Ministry of Education and Science, Republic of Serbia.

References

[1] A. Tripon. Innovative technology for sustainable development of human resource using non-formal and informal education. *Procedia Technology 12* (2014), 598 – 603.

[2] A. Ghezloun, N. Oucher, S. Chergui. Energy policy in the context of sustainable development: Case of Algeria and Tunisia. *Energy Procedia 18* (2012), 53 – 60.

[3] L. Wang, L.Y. Xu, H.M. Song. Environmental performance evaluation of Beijing's energy use planning. *Energy Policy 39* (2011), 3483-3495.

[4] O.M. Theisen. Climate clashes? Weather variability, land pressure, and organized violence in Kenya, 1989–2004. *Journal of Peace Research 49* (2012), 81–96.

[5] R. Reuveny. Climate change-induced migration and violent conflict. *Political Geography 26* (2007), 656–673.

[6] L. Roma. Climate change, population drift and violent conflict over land resources in Northeastern Nigeria. *Journal of Human Ecology 23* (2008), 311 – 324.

[7] EC, Green Paper: On a European Programme for Critical Infrastructure Protection. Commission of the European Communities. Brussels (Belgium). 2005.

[8] J.C. Jansen, A.J. Seebregts. Long-term energy services security: what is it and how can it be measured and valued. *Energy Policy 38* (2010), 1654-1664.

[9] M. Protic, D. Mitic, D. Vasovic, M. Stankovic. Renewable energy potentials in Serbia with particular regard to forest and agricultural biomass. Proceedings of Advanced Research Workshop *Energy options impact on regional security*, Split, Croatia, Springer, 307- 324, 2010

[10] V. Costantini, F. Graccevaa, A. Markandyaa, G. Vicini. Security of energy supply: Comparing scenarios from a European perspective. *Energy Policy 35* (2007), 210–226

[11] L. Chester. Conceptualising energy security and making explicit its polysemic nature. *Energy Policy 38* (2010), 887–895.

[12] A. Löschel, U. Moslener, D. Rübelke. Energy security-concepts and indicators. *Energy Policy 38* (2010), 1607–1608.

[13] A. Löschel, U. Moslener, D. Rübelke. Indicators of energy security in industrialised countries. *Energy Policy 38* (2010), 1665–71.

[14] B. Kruyt, D.P. Vuuren, H.J.M. Vries , H. Groenenberg. Indicators for energy security. *Energy Policy 37* (2009), 2166–2181.
[15] C. Le Coq, E. Paltseva. Measuring the security of external energy supply in the European Union. *Energy Policy 37* (2009), 4474–4481.
[16] D. Streimikiene, G. Sivickas. The EU sustainable energy policy indicators framework. *Environment International 34* (2008), 1227–1240.
[17] J.M. Yusta, G.J. Correa, R. Lacal-Arantegui. Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy 39* (2011), 6100–6119.
[18] J.S. Duffield, B. Woodall. Japan's new basic energy plan. *Energy Policy 39* (2011), 3741–3749.
[19] V. Vivoda. Evaluating energy security in the Asia-pacific region: a novel methodological approach. *Energy Policy 38* (2010), 5258–63.
[20] EC, Commission of the European Communities from the Commission on the European Programme for Critical Infrastructure Protection, COM (2006) 786, Final, Brussels (Belgium). 2006.
[21] Law on Planning and Construction, Official Gazette of the Republic of Serbia, No. 72/2009, 81/2009, 24/2011, and 121/2012.
[22] Law on Defence, Official Gazette of the Republic of Serbia, No. 116/2007 and 88/2009.
[23] Law on Emergency Situations, Official Gazette of the Republic of Serbia, No. 111/2009 and 92/2011.
[24] J. McKay.Community responses to flood hazard. *Disasters* (1984), 8-23.
[25] V. Nikolic, N. Zivkovic, N. Occupational and Environmental Safety, Emergencies and Education, Faculty of Occupational Safety, University of Nis, Serbia, 195-263. 2010.
[26] J.H. Sorensen. Knowing how to behave under the threat of disaster: can it be explained? *Environment and Behaviour 15* (1983), 438-457.
[27] C. Argyris., D. Schon. Organizational Learning. Addison – Wesley. Massachusetts. 1978.
[28] M. Dodgson. Organizational learning: A review of some literatures. Sage Publications. Thousand Oaks. 1993.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015

© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-215

The Combined Threat of Terrorism and Organized Crime for and in South East Europe

George X. PROTOPAPAS[1]
Research associate – Analyst with the Research Institute for European and American Studies (RIEAS)

Abstract. The nexus between terrorism and organized crime could be developed into a major threat for South East Europe. Some areas, for instance the Western Balkans, are considered a "safe haven" for Islamists terrorism and criminals. The Critical Infrastructure is considered an important part of the security of the states and could be a target of terrorism and organized crime. The broad definitions of the Critical Infrastructure and energy security show the different views of organizations and states towards national security. The post Cold War era has blurred the dividing lines between internal and external security. Terrorism and organized crime have converged interests in order to finance their operations. NATO could play a leading role in the protection of Critical Infrastructure. NATO could establish a Gendarmerie Force on the model of the European Gendarmerie Force (EGF) and the Italian Guardia di Finanza. NATO could guard against the combined threat of terrorism and organized crime by adopting an effective strategy. It could include military and policing methods, border security, smuggling, safety of financial, economic, judicial and public sectors and cyber -security.

Keywords. critical infrastructure protection, critical energy infrastructure, terrorism, organized crime, security, NATO Gendarmerie

Introduction

Globalization and the technological evolution have considerably undermined the previously tight structures of the global security. The control of the states' borders inevitably becomes more difficult for the law enforcement agencies. The post Cold War era has blurred the dividing lines between internal and external security. The terrorists and organized crime groups are collaborating in order to finance their illegal activities and operations. The Critical Energy Infrastructure (CEI) is an important target for the terrorists and organized crime groups. Accordingly, terrorists may plan to execute a high-impact attack against CEI. However, in law-weak enforcement we observe the cooperation between terrorism and organized crime.

As regards the terrorism factor, we observe that the Islamic terrorism have found a fertile ground to grow up due to some new weaker state institutions, corruption and the deteriorating economy. The surge of Islamic fundamentalist ideology exploited the global war against terrorism and the ethnic tolerance of the Western Balkans and could threaten South East Europe. In view of the above, the transnational organized crime groups also found the preconditions to become a regional threat. Organized crime's

[1] Corresponding Author: George X. Protopapas, MSc, Research associate – Analyst with the Research Institute for European and American Studies (RIEAS), e-mail: rieasgeorge@gmail.com

activities destabilize countries, increase corruption, extortion, racketeering, violence and sophisticated crimes at the local and international levels.

This paper examines the methods that NATO could adopt for an effective Critical Infrastructure Protection strategy from the combined threat of terrorism and organized crime. We approach the issue by: (a) approaching the theoretical aspects of the Critical Infrastructure. The definitions help us to understand the role that the Critical Infrastructure is playing in the functioning of the society and national security; (b) explaining the energy security importance. It is a fundamental factor for the survival of the states. We explain also the role of NATO in energy security; (c) analyzing the threat from the cooperation between the terrorist and organized crimes groups; and (d) proposing the precondition for the creation of a NATO Gendarmerie in order to simultaneously fight the Islamic terrorism and organized crime.

1. Theoretical Aspects of Critical Infrastructure (CI) and Energy Security

1.1. The Definitions of Critical Infrastructure (CI)

The Critical Infrastructure (CI) has become an issue of great importance as it is directly connected to the national security, the economy and well – being of the society. The CI is considered an important aspect of the security issue. A terrorist attack can destroy the interconnected and interdependent critical networks of social and business systems. It can provoke enormous destructive effect on the development of a state. In parallel, the globalization and Information Technology (IT) have increased the interdependency among markets and networks in essential sectors such as energy, information & communications and transportation. The Critical Information Infrastructure (CII) refers to the information and communication technology systems. However, the distinctions between Critical Infrastructure (CI) and Critical Information Infrastructure (CII) have created a debate among the practitioners and academicians. The defining line between CI and CII is far from clear.

The term CI has several definitions that are based on the interpretation in literature and the state policy documents. Nevertheless, CI is generally defined as the basic facilities and services that are vital for the functioning of a community or society. The description of the CI is a necessary step towards understanding its significance in order to protect it, and is used as an indication to detect the national priorities on the security level [1].

In 1996, the American administration of President Bill Clinton defined CI in the concept of national security. The Executive Order 13010 characterizes as infrastructure the framework of interdependent networks and systems comprising certain industries, institutions (including people and procedures), and distribution capabilities that provide a consistent continuation of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole [2].

The European Union defines CI as (a) an asset, system or part thereof located in Member-States, which is vital for the maintenance of vital societal functions, or social well-being of people, and the interruption or destruction of which would have a significant impact on a Member-State (b) European critical infrastructure, or ‘ECI’ means critical infrastructure that the disruption or destruction of which would have a significant impact on at least two Member States. The impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure [3].

The Organization for Economic Co-operation and Development (OECD) includes two interdependent definitions for the CI: (a) the “critical” as the infrastructure that offers a crucial support for economic and social well-being for public safety. The incapacitation or destruction of the infrastructure would result in catastrophic and far-reaching damage, and (b) the “infrastructure” as “the physical infrastructures that regularly comprise intangible assets and/or to production or communications networks” [4].

Nevertheless the word “critical” is the fundamental criterion for the description of an infrastructure as “critical”. The definition constantly changes due to the general views and expanded lists. Nevertheless, Metzger [5] identifies a typology of two different but interrelated approaches of the meaning of “criticality”: (a) Symbolic concept. The infrastructure exists as an essential part of the society (has a role or a function) and (b) Systemic concept. The infrastructure has a structural position in the whole system of infrastructure, especially when it is connected with other infrastructure or sectors.

The CI is a part of interconnected and dependent networks that link systems of communications and information technologies. For this reason a terrorist or cyber-attack could have a destructive impact on the society. The term “interdependencies” means the links among agents from different infrastructure in general system of systems. The interdependencies increase the overall complexity of the system of systems [6].

Although the interdependencies have distinguished characteristics and different impacts on the infrastructure agents, Rinaldi categorizes the interdependencies in four types: physical, cyber, geographic and logical [6]:

- Physical Interdependency: In this case two infrastructures are physically interdependent if the state of each depends on the material output(s) of the other. A physical interdependency is created from a physical connection between the inputs and outputs of two agents.
- Cyber Interdependency: It means that a state depends on information that transmits through the information infrastructures. Cyber Interdependencies are interconnected via electronic and informational links.
- Geographic Interdependency: It takes place when parts of multiple infrastructures are in close spatial proximity.
- Logical Interdependency: It occurs when two infrastructures are interdependent if the state of each depends on the state of the other via a mechanism. The logical interdependency does not have the characteristic of the three aforementioned interdependencies.

The concept of the Critical Infrastructure (CI) should not be separately examined from the concept of Critical Information Infrastructure (CII)). Broadly speaking, the CII is considered a vital part of the CI. The CII includes all the critical sectors and CII can be seen as a subset of a CI [7][8].

OECD characterizes CII as something that the disruption or destruction of which would have a dangerous impact on the health, safety, security, or economic well-being of citizens, or on the efficient functioning of a government or an economy [9].

The CII includes telecommunication networks, management, location-based services for emergency calls; air traffic control, train routing and control, traffic management;

credit card transactions, settlement systems, transaction records, electronic stock /bond trading; and control systems/SCADA (Supervisory, Control and Data Acquisition). However, the internet is not considered CII although the society is based on internet services such as e-commerce, e-banking, e-governments service and telecommunication [8]. The internet is vulnerable to cyber attacks that can disrupt the aforementioned services, provoking instability in the society.

The definitions of Critical Infrastructure from practitioners and academicians are considered the first step that helps the international community to find sufficient ways to protect them.

1.2. The Definition of Energy Security

The energy infrastructure is an essential part of the modern society as energy is an important element for the development of the states. The energy is used in residential, industrial and transportation sectors; it is of great importance for the military (supply for military operation) and is a casus belli because wars have started for the control of the energy resources (World War II). The great powers are desperately looking for access to gas and oil reserves to supply to their economy and populations. Therefore, the energy security is considered a vital factor for the survival of the states and societies. The traditional elements of energy security are the supply sources, demand centers, geopolitics and market structures.

The European Commission defines energy security as the ability to guarantee that future essential energy requirements can be met through adequate domestic resources, worked under economically acceptable conditions or maintained as strategic reserves and by calling upon accessible and stable external sources supplemented where appropriate, by strategic stocks [10].

The International Energy Agency (IEA) defines energy security as “the uninterrupted availability of energy sources at a reasonable price”. The need to increase energy security was the main objective underpinning the establishment of the IEA in 1974. The energy security has many aspects: long-term energy security is mainly linked to timely investments to supply energy in line with economic development and environmental needs and short-term energy security based on the ability of the energy system to react rapidly to unexpected changes in the supply-demand balance [11].

The Global Energy Assessment (GEA) argues that energy security relates to the vulnerability of national vital energy services, which is the first precondition for functioning of the modern states [12].

The Working Group on Asian Energy and Security at the Massachusetts Institute of Technology’s (MIT) Center for International Studies defines energy security based on three approaches: (a) decreasing the vulnerability to foreign threats or pressure, (b) preventing supply crisis from happening and (c) minimizing the economic and military effect of supply crisis once it has occurred [13].

The term energy security also has four different but overlapping dimensions: (a) internal policy dimension: calls for extensive financial acquisitions for the maintenance and extension of energy networks; the emergency planning to face interruption challenges; the energy efficiency or productivity; the need of consuming states to rethink their specific fuel mixes; (b) economic dimension: the sufficient and affordable supply is the main precondition for energy security [14]; (c) geopolitical dimension: it relates to the energy resources that are located in a few regions in the world. The great powers need access to the rich – energy states to maintain their economic development in the high level and to supply their population. The concentration of energy reserves (gas and oil) in a few countries inevitably creates geopolitical implications. The fossil fuels are located in regions that are characterized by political instability or internal conflict (Libya, Iraq).The access to the energy resources is hampered by internal policies, such as the nationalization of energy sectors [15]; and (d) security dimension. It is for the protection of the energy critical infrastructure from terrorism / cyber / piracy attacks.

The Energy Critical Infrastructure (ECI) includes four sectors: nuclear, hydroelectric, petroleum and natural gas. According to Fedorowicz the four ECI have different levels of vulnerability in terrorist attacks [16]:

Nuclear facilities: The fact that the most of them are located in relatively stable and developed states removes the risk of them becoming target of terrorist attacks; hydroelectric facilities: The terrorists have committed attacks on electrical transmission towers (Peru's Sendero Luminoso). There are also examples of large scale blackout (north eastern part of North America in 2003); Petroleum and natural gas facilities. These types of facilities are more exposed to terrorist attacks because they are considered more diverse targets.

The energy security concept differs among the countries because it depends on: (a) the degree to which a state is characterized energy-rich or not (b) the degree to which market forces are able to operate to set prices and (c) the degree to which long – term versus short term planning is used [13].

In the coming years the energy security is bound to face more pressing challenges. The scale of the global trade in energy will grow substantially and the world markets will become more integrated. The energy security will depend much more on the countries' relations (at bilateral or multilateral levels) [17].

Overall, the concept of energy security is a complex and multifaceted issue. It does not have a common definition because its meaning is differently interpreted by different states and organizations. In any event, the energy security generally refers to: the reliability of supply, self-sufficiency, security of infrastructure, stability and diversity of suppliers and diversity of energy carriers.

2. NATO and Energy Security

2.1. Concept and Strategy

Energy security is directly related to the Critical Energy Infrastructure Protection (CEIP) and NATO can play a vital role as a powerful military alliance. The Critical Infrastructures are part of the broader framework of counter – terrorism and civil protection policies. As major threats, the terrorist attacks pose a considerable threat to the energy security as they can undermine and damage energy facilities. A terrorist target would aim at causing the highest possible damage; disrupt supply chains as well as to create a sense of instability for the society.

NATO understands the importance of energy security which does have several implications on Alliance strategies. On this context the energy security challenges involve: the dependency of European continent for oil and gas – especially for Russia; terrorist attacks against energy infrastructures; political instability in numerous transit – states and energy-producing states; territorial conflicts for the control of energy resources and other reserves; the increased energy demands from rising powers (China, India); piracy attacks in vital maritime choke–points; cyber-attacks against energy infrastructure; the need for an energy efficiency for NATO military operations when they deployed far from home [18].

The Atlantic Alliance underlined the importance of the energy security at the Bucharest Summit in April 2008 with the report on "NATO's Role in Energy Security". The report recognized guiding principles and outlines options and recommendations for further activities. The report identified the five following key areas where NATO could significantly contribute: information and intelligence fusion and sharing; projecting stability; advancing international and regional cooperation; supporting consequence management; and supporting the protection of critical infrastructure.

The energy security was officially included in NATO 2010 Strategic Concept of "Active Engagement, Modern Defense" that states to: "develop the capacity to contribute to energy security, including protection of critical energy infrastructure and transit areas and lines, cooperation with partners, and consultations among Allies on the basis of strategic assessments and contingency planning" [19].

However we could say that two Articles of the North Atlantic Treaty (Washington, 4 April 1949) comprised the notion of energy security [20]. Article IV stipulates that "the Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the parties is threatened" [21]. Article V is pertinent as well as because of the nature of many threats: "the parties agree that an armed attack against one or more of them in Europe or North America" [21]. We could agree "Though Article V does not distinguish energy facilities from other targets, and is likely that the nature of the threats to energy infrastructure, no matter the source, may they be from terrorists, pirates and even states, in the end they are likely to be in the form of armed attacks which can be determined to be a cause for invoking Article V" [20].

The NATO 2010 Strategic Concept, the Emerging Security Challenges Division (ESCD) and the NATO Energy Security Center of Excellence (ENSEC COE) prove that energy security is officially a part of the Alliance activities. The NATO Emerging Security Challenges Division (ESCD) within the NATO International Staff was created to deal with a growing range of non-traditional risks and challenges - terrorism, the proliferation of Weapons of Mass Destruction (WMD), cyber defence and energy security. The ESCD provides NATO with a Strategic Analysis Capability to monitor and anticipate international developments that could threaten the Alliance security. The ESCD connect various strands of expertise already existing in different parts of NATO Headquarters. The establishment of the ESCD underscores that NATO pays attention to the importance of the new, non-traditional security challenges [22].

The mission of the NATO Energy Security Center of Excellence (ENSEC COE) is to provide subject matter expertise on the energy security in order to support the transformational and operational requests of the Strategic Commands, the Sponsoring Nations and other Customers. It involves the contribution to the development of energy security related doctrines and standards. The Doctrine & Concept Development Division collects and analyzes knowledge and experience by conducting and attending relevant seminars, workshops and conferences, by contributing to and participating in concept development and experimentation activities. The Doctrine & Concept Development Division is responsible for: development of NATO energy security related doctrines, standards and procedures; development, validation and improvement of NATO Nations and partners standards and procedures with an energy dimension; support and integration of Repositories of Best Practices, lessons identified and lessons learned in cooperation with NATO and National Lessons Learned centres [23].

NATO energy security activities can be categorized into the following fields: raising strategic awareness, participating in the protection of Energy Critical Infrastructure, ensuring energy efficiency in the military [18].

The preconditions for an effective NATO energy security strategy entail measures on the political and military level. On the political level, NATO diplomatic mechanisms could address the problems of energy security involving regular consultations with other players such as Russia, or states in the Middle East, Africa, Caucasus, and Central Asia. Yet, on the military level, NATO could use its military structures to protect the CEI, by preventing terrorist attacks. Perhaps this role can be served by the NATO Response Force (NRF), which could play a basic role in protecting energy facilities from threats [24]. For instance, special operations forces (ground forces) could rapidly be deployed in the center of the crisis that threatens to disrupt or destroy an oil and natural gas pipeline or an LNG facility [25].

Operation Active Endeavour is a naval anti-terrorism operation which also applies to energy security. The NATO maritime forces have been maintaining security for key resource routes in the Mediterranean. Allies also cooperate with partner countries and relevant experts through the Euro-Atlantic Partnership Council (EAPC), the Mediterranean Dialogue (MD), the Istanbul Cooperation Initiative (ICI), NATO's Science for Peace and Security Programme and other frameworks[2].

Therefore, the concept of energy security ought to be a part of NATO's strategy in order to address any kind of threats including the asymmetric ones. However, the realization of the above poses difficulties due to the following theoretical – at least – reasons: (a) the divergent national interests of the Member–States; (b) the increased number of players that are engaged in the energy security chessboard, like the European Union, the IEA, the OSCE and others, as well as the private sector, which may be more concerned in energy security issues; (c) the concern of many countries with regard to overstretching, which NATO might possibly be exposed to and; (d) the fact that NATO is perceived as being more competent to deal with several other threats [26]. In addition to the aforementioned, the Armies of the Member-States are characterized by strategic weaknesses as regards energy supply chains and energy usage [27].

2.2. NATO and South East Europe

South East Europe became part of NATO's strategies and activities after the end of the "Cold War", when ethnic-conflicts of the Western Balkans threatened the security of the entire region. South East Europe remains a basic priority for NATO's strategy due to its

[2] NATO forces have hailed over 115,000 merchant vessels and boarded some 162 suspect ships. By conducting these maritime operations against terrorist activity, NATO's presence in these waters has benefited all ships traveling through the Straits of Gibraltar by improving perceptions of security. Keeping the Mediterranean's busy trade routes open and safe is critical to NATO's security. In terms of energy alone, some 65 per cent of the oil and natural gas consumed in Western Europe pass through the Mediterranean each year, with major pipelines connecting Libya to Italy and Morocco to Spain. For this reason, NATO ships systematically carry out preparatory route surveys in "choke" points as well as in important passages and harbours throughout the Mediterranean. Operation Active Endeavour, Available at: http://www.nato.int/cps/en/natolive/topics_7932.htm

geopolitical importance – it partly covers the Eastern Mediterranean, Central Eastern Europe and the Black Sea.

NATO's involvement started with the dissolution of the Former Yugoslavia which unleashed ethnic–sectarian differences provoking political fragmentation and armed conflicts. In August 1995, NATO carried out its first military intervention in Bosnia and Herzegovina in order to impose peace and security (Operation Deliberate Force). At the beginning, in December 1995, the Alliance deployed a multinational peacekeeping Implementation Force (IFOR) in Bosnia and Herzegovina with a one year mandate. After that NATO created the Stabilization Force SFOR, a continuation of IFOR which deployed in Bosnia and Herzegovina from January 1996 until December 2005.

NATO continued to play active role in the maintenance of security and peace in Western Balkans when it started in March 1999 military operations against the Federal Republic of Yugoslavia because of the Kosovo War. As a result, in June 1999, NATO deployed the Kosovo Force (KFOR) into Kosovo to secure peace and freedom of movement for all citizens irrespective of their ethnic origin[3].

NATO included at the Washington Summit 1999 the South East Europe Initiative (SEEI) which included programmes and initiatives for the regional cooperation and security- focusing in Bosnia and Herzegovina, Croatia and the Former Yugoslav Republic of Macedonia (FYROM).

The maintenance of the long – term stability and security in the South East Europe are one of NATO's priorities. Thus the Alliance established the Partnership for Peace (PfP) and the Science for Peace and Security Programme (SPS) in order to enhance the dialogue with partner - states of SEE, to support military reforms and to help them to fulfil the standards which need to acquire NATO membership.

The Partnership for Peace (PfP) is a programme of practical bilateral cooperation between individual Euro-Atlantic partner countries and NATO. It gives the opportunity to partner-states to build up an individual relationship with NATO, choosing their own priorities for cooperation. The aim of PfP is to increase stability, diminish threats against peace and build strengthened security relationships between individual Euro-Atlantic partners and NATO, as well as to enhance the cooperation among the partner countries. The activities of the PfP include defence-related work, defence reform, defence policy and planning, civil-military relations, education and training, military-to-military cooperation and exercises, civil emergency planning and disaster response, and cooperation on science and environmental issues[4].

The Science for Peace and Security Programme (SPS) was created in order: to enhance the cooperation and dialogue with all partners; to contribute to the Alliance's core goals; and, to address the priority areas for dialogue and cooperation. The SPS facilitates the collaboration between experts from NATO member-states and partner-

[3] KFOR derives its mandate from UNSCR 1244 of 10 June 1999 and the Military-Technical Agreement (MTA) between NATO and the Federal Republic of Yugoslavia and Serbia. KFOR is operated under Chapter VII of the UN Charter and, as such, is a peace enforcement operation, which is more generally referred to as a peace support operation. See more NATO's role in Kosovo. Available at: www.nato.int/cps/en/natolive/topics_48818.htm

[4] Over the years, a range of PfP tools and mechanisms have been developed to support cooperation through a mix of policies, programmes, action plans and arrangements. At the Lisbon Summit in November 2010, as part of a focused reform effort to develop a more efficient and flexible partnership policy, Allied leaders, decided to take steps to streamline NATO's partnership tools in order to open all cooperative activities and exercises to partners and to harmonise partnership programmes. See more The Partnership for Peace (PfP). Available at: www.nato.int/cps/en/natolive/topics_50349.htm

countries through the Euro -Atlantic Partnership Council (EAPC), the Mediterranean Dialogue (MD), the Istanbul Cooperation Initiative (ICI) and NATO-Ukraine. The SPS key priorities are : (a) to facilitate mutually beneficial cooperation on fields of common interest, including international efforts to meet emerging security challenges (including Counter-terrorism, energy security, cyber defence, defence against CBRN agents, environmental security; (b) to enhance support for NATO-led operations and missions; (c) to enhance awareness on security developments including through early warning, with a view to prevent crises (security-related advanced technology, border and port security, mine and unexploded ordnance detection and clearance, human and social aspects of security related to NATO's strategic objectives) [5].

Furthermore, the SEE is connected to energy balance of power of the European continent. The SEE can play a vital role to the European energy security and can contribute to the reduction of the European energy dependence on Russian gas. In the past years the Russian–Ukraine gas crisis disclosed the energy vulnerability of the SEE when the gas supplies were interrupted in winter of 2008 – 2009. Russia uses the energy as a tool to deepen Europe's dependence on energy supplies. The so-called "*pipeline diplomacy*" increases Russia's economic and geopolitical influence on the European states.

The European Union is looking for supply alternatives in order to reduce its energy dependence on Russian gas, particularly after relations between the West and Russia deteriorated following the current Ukraine crisis. Greece, Albania and Turkey – NATO member-states will be used as transit-countries to transfer gas of Caspian Sea to Europe bypassing Russia. The proposed Trans Adriatic Pipeline (TAP) to transport natural gas from the Azerbaijan starting from Greece via Albania and the Adriatic Sea to Italy and further to Western Europe[6].

NATO has understood that the energy security of the SEE cannot be neglected because it will divide alliance between vulnerable and non-vulnerable members [28]. NATO strategies and actions focus on the need to reduce Europe's dependence on Russian oil and gas, to protect energy infrastructures and to guard the political stability.

3. The Nexus Between Terrorism and Organized Crime in South East Europe

The actions of organized crime and terrorists groups could develop in to a significant threat for the security of the region of South East Europe. The "Balkan route" serves the illegal activities of the aforementioned two groups. It is also well known that organized crime and terrorism usually develop links and interdependencies that increase the level of asymmetric threat. The interests of the organized crime may be connected with the aims of terrorists. For example, organized crime groups may finance criminal or terrorist operations. On those grounds, energy facilities - such as refineries, pipelines could become potential targets of terrorist as well as of organized groups.

[5] The SPS includes: Counter-Terrorism, Energy Security, Cyber Defence, Defence against CBRN Agents, Environmental Security, Enhance support for NATO-led operations and missions, Security-related Advanced Technology, Border and Port Security: Border and port security technology, Mine and Unexploded Ordnance Detection and Clearance: The Science for Peace and Security Programme (SPS), available at: www.nato.int/cps/en/natolive/topics_85373.htm?

[6] The TAP pipeline would be supplied by natural gas from the second stage of the Shah Deniz gas field development in the Azerbaijani section of Caspian Sea through the South Caucasus Pipeline and the planned Trans Anatolian Pipeline (TANAP).

The connection between terrorism and organized crime has been facilitated by globalization, communication and the end of the "Cold War". In this context, organized crime offers to terrorists the much needed channels, such as crime routes and access to weapons, thus enabling them to challenge public security as well as armed forces [29].

According to UNODC Report "South-Eastern Europe has long represented a crucial stage of the "Balkan route"; a well-worn heroin supply route that travels westward by land from Afghanistan to reach the lucrative destination markets of Western and Central Europe. The continued importance of the "Balkan route" is evident in large seizures at key stages of the route. Large single seizures of heroin upstream and in destination markets suggest that while large shipments are moving through South-Eastern Europe, there appears to be less such actionable information being generated in the region itself. This is an area of vulnerability in the context of disappearing internal borders resulting from European Union (EU) accession and accelerating regional integration" [30].

Several spots in the Balkans are operationally used as important shipment points for illicit trafficking due to the high flows of regional road traffic which favor illegal shipment to move undetected from the authorities of law enforcement. These activities are facilitated by the increased illegal migration flows [31]. The Western Balkans are not only deemed as a transit region but also as a significant source of firearms trade on the international weapons market, drug precursors (ephedrine) as well as ready synthetic drugs. Moreover, the weapons' trade continues to supply international criminal markets. The Western Balkans is expected to remain a key source of heavy firearms trade into the EU, due to the large illicit stockpiles of the countries of the region [32]. We can assume that large quantities of weapons and armaments from the conflicts of the 1990s remain out of the control of local law enforcement and security authorities. Furthermore, money laundering prevails in the region through investment in real estate and in commercial companies [33]. The Western Balkans region is considered a "safe haven" for a bundle of war profiteers, career criminals and Islamic fundamentalists due to the weak governmental structures and deteriorating economies [34].

The transport networks in the Balkans are used also by militant Islamic groups for logistical support. The Islamist militants can enter the Schengen area through Croatia or Serbia which are open to the European Union's member-states. For instance, it is reported that the Al Qaeda of the Islamic Maghreb uses the heroin trade via West Africa en route to Europe. Moreover, the militant Islamic groups participate in the criminal actions in order to gain financial and logistical support. They are encouraged by the need for self-finance and the requirement to independently organize their terrorist operations. The defining characteristics of the alliance between terrorism and organized crime consist of, but is not limited to: (a) access to specialized knowledge (e.g. money laundering), (b) access to specialized services (e.g. counterfeiting), (c) operational support and (d) financial support [31].

The "Balkan route" is primarily used by the militants who come from Afghanistan and Pakistan and recently from Syria. The Islamic fundamentalism could become a major threat for the Balkan (imported mainly from the Middle East) as it finds a fertile ground because of most countries have large Muslim majorities [35].

In addition, the civil war in Syria poses another serious threat for the South East Europe. The counter terrorism agencies have expressed concerns that the Islamists from Balkans in Syria could become more radicalized and receive combat training. Some of them might return to their home as part of a global jihad [36]. According to international media 159 individuals from the Western Balkans have been associated with Islamists foreign fighters in Syria. A data analysis based on the roles attributed to these individuals shows that 125 are foreign fighters, 18 are facilitators, 10 are identified as the wives of foreign fighters, and the role of six people could not be clearly identified. The majority of the persons listed are male (94%) with a small number of females (6%). Moreover the identity of their nationality shows that 70 individuals were from Bosnia-Herzegovina, 42 from Kosovo, 25 from Albania, nine from Serbia, five from FYROM, and two from Montenegro. The data reveals a number of dual nationals including one from Algeria / Bosnia, two from Egypt / Bosnia, one from Lebanon / Bosnia, one from Syria / Bosnia, and one from Switzerland / Bosnia. With the exception of the Swiss / Bosnian, all Islamists are ex-members of the el-Mujahid group (was operational during the former-Yugoslavia conflict in the 1990s [37].

The level of cooperation between terrorists and organized crime is determined in many cases from the nature of geographic region. According to Study of the European Parliament, "in transitional states, the nexus includes the operational and conceptual plane, with evidence of convergent motivations dominating groups operating in regions such as the Balkans. Historically, poor border security, weak law enforcement, corrupt public officials and established smuggling networks have facilitated the emergence of hybrid groups that simultaneously sought political aims and profit maximization. This was epitomized by the Albanian mafia and the KLA through the mid-1990s, each benefiting from an interchangeable membership and recruitment base" [31].

The links between Islamic terrorist cells and organized crime groups raise serious concerns for the European law enforcement authorities. Although they are different types of criminal activities and their actions are driven by different incentives, terrorism and organized crime cannot be examined as isolated and unrelated entities. The organized crime and terrorism operate on a global level and don't recognize nationality and borders. The groups are only motivated by the rule of supply and demand which involves the strategies and tactics of an effective marketing [38].

The threats of organized crime and terrorist groups have been underlined by the European Union's law enforcement authorities. A document from EUROPOL, EUROJUST and FRONTEX which was sent to the Council of the European Union, concludes that "organized crime and terrorist groups are increasingly mobile, exploiting existing transport infrastructure and establishing new routes to penetrate the internal security of the EU. Key hubs in and around the external border of the EU have developed as principal staging posts for the inward flow of illicit goods and people from other parts of the world; border security is compromised by groups exploiting vulnerabilities in the transport sector, including through corruption and the use of counterfeit, forged and fraudulently obtained documents, which are indispensable facilitators for illegal migration, trafficking in human beings, identity fraud, and terrorism" [39].

4. NATO Proposed Actions and Considerations

The post-Cold War era has blurred the dividing lines between internal and external security. As Lutterbeck points out, security thinking and analysis are categorized as challenges to a state's internal security and threats to its external security [40].

While the nexus between international terrorism and transnational organized crime constitutes a considerable threat for the global security and peace, the traditional strategy thinking fails to anticipate these significant changes. In this context the protection of CEI becomes vital not only for the good functioning of the society but for NATO's operations, as they too depend on uninterrupted supply chain. Undoubtedly, the Alliance could strengthen its role in the CEI protection creating a Gendarmerie that could incorporate the mission of the European Gendarmerie Force (EGF) and perhaps adopt the standards of the Italian Guardia di Finanza (GdF).

The creation of a new force, such as Gendarmerie based on NATO rules for the peacekeeping operations, could be a good option in order to protect and to maintain the peace and security. The North Atlantic Treaty does not explicitly provide for the creation of such force. Yet, we believe that since a Gendarmerie would aim in fulfilling the purpose of protection of the member and/or cooperation States [41], perhaps a supplementary Protocol or Agreement for its creation would suffice. During the post- Cold War the Strategic Concepts and Cooperation Agreements gave NATO a wider and more flexible role to face the new challenge and threats. The NATO Strategic Concept 1999 predicts the serious effects of instability on NATO stating the need for pre-emptive activities stating "some countries in and around the Euro-Atlantic area face serious economic, social and political difficulties. Ethnic and religious rivalries, territorial disputes, inadequate or failed efforts at reform, the abuse of human rights, and the dissolution of states can lead to local and even regional instability. The resulting tensions could lead to crises affecting Euro-Atlantic stability, to human suffering, and to armed conflicts. Such conflicts could affect the security of the Alliance by spilling over into neighbouring countries, including NATO countries, or in other ways, and could also affect the security of other states" [42]. The modernized NATO Strategic Concept 2010 became more specific when it stated: "it commits the Alliance to prevent crises, manage conflicts and stabilize post-conflict situations, including by working more closely with our international partners, most importantly the United Nations and the European Union" [19].

The rules and responsibilities of a proposed NATO Gendarmerie - will combine the duties of European Gendarmerie Force (EGF) and the Italian Guardia di Finanza (GdF)- which is not prescribed in NATO provisions as we propose a force with military and policing duties. A NATO Gendarmerie should be focused on border security, trafficking, the narcotics trade, illegal weapons trading, the protection of the financial, economic, judiciary and public sectors and cyber -security.

The framework of the European Gendarmerie Force (EGF) and the GdF are a useful tool to understand their roles in the safeguarding of security. The EGF is a multinational initiative of six EU Member States - France, Italy, The Netherlands, Portugal, Romania and Spain – established in 2006 with the mission to strengthen international crisis management capacities and contribute to the development of the Common Security and Defense Policy. The members of the EGF have national Gendarmerie - France (Gendarmerie Nationale), Portugal (Guarda Nacional Republicana), The Netherlands (Koninklijke Marechaussee), Italy (Arma dei Carabinieri), Romania (Jandarmeria Română), Spain (Guardia Civil) and experience to accomplish gendarmerie duties. The EGF structure does not envision a standing force. However, a force can be generated and deployed on an ad hoc basis, mobilizing a maximum of 800 gendarmes within 30 days, including if needed, a deployed Headquarters in the field. The EGF can be considered as an integrated police tool designed to carry out police missions in different theatres, including destabilized ones, in support of the European Union, the United Nations, the Organization for Security and Cooperation in Europe (OSCE), the North Atlantic Treaty Organization (NATO), or possible ad hoc coalitions [43].

Likewise, we indicatively suggest the example of the Italian Guardia di Finanza as it is a law enforcement agency under the authority of the Italian Ministry of Finance, while it is part of the Italian Armed Forces. It is focused on the prevention of tax evasion, financial crimes, smuggling, money laundering, international illegal drug trafficking, illegal immigration, customs and borders checks, copyright violations, anti-Mafia operations, credit card fraud, cybercrime, counterfeiting, terrorist financing, maintaining public order, and safety and of the protection of Italian territorial waters and borders.

The proposed NATO's gendarmerie could be rapidly deployed – as any military force – and be logistically sufficient as support entity for peacekeeping troops. The EGF could cooperate with NATO Gendarmerie as all the EGF members are NATO member-states. In this case the European and NATO could establish joint command for independent actions or by assisting peace-keeping forces. It is implied, of course, that this type of action will have the necessary legitimacy and jurisdiction deriving from international conventions. This combined new force could easily be deployed on rogue areas or conflict regions, where local Police and enforcement agencies are in need of assistance, either very ineffective or disabled.

In this way a gendarmerie can assist both UN and NATO armed forces as well as local institutions. The benefits are many; indicatively, we can mention improvements in intelligence and law enforcement in micro and wider levels. For example, the gendarmerie forces could become the liaison of intelligence management between the local authorities (if any exist) the troops and the law enforcement agencies in the Member States. Likewise, gendarmerie may work together with the local Police, gendarmerie or military forces for planning, command and control, training and exercises [44]. The Gendarmerie forces are considered the most suitable units to stabilize a country, secure CEI, and advise on mixed law enforcement and military operations, based on its ability to carry out policing in all circumstances [44].

On a practical level, NATO must first start with a comprehensive strategy for the protection of the CEI. This strategy should be focused on emergency needs, accordingly the overall management should include more comprehensive organization capabilities encompassing law enforcement properties for accomplishing the following: (a) Warning: the identification of imminent threats; (b) Prevention: the detection, identification and control of threats that could threaten the national security in the short-midterm; (c) Protection: the concurrent security and safety of people, critical infrastructure, goods and economy; (d) Response: the management of measures and actions in order to encounter terrorists acts, natural disasters, accidents and (e) Recovery and rehabilitation: the plan of state authorities and private sector to re-establish public service structures and functioning after terrorist attacks and other accidents [45].

As regards the intelligence gathering and assessment, the same is considered a vital element of the Alliance's strategy. The security of CEI is based on the realistic identification of domestic and international risks of the energy (product and supply) chain. In this case, it is of paramount importance to establish advanced intelligence-sharing between civil and military agencies [46]. The threat assessments of national intelligence agencies often translate to a threat level indicator. The intelligence should focus on: identifying critical infrastructures (what must we protect); determining threats (what threatens the things we must protect); determining vulnerabilities (how those things are vulnerable); determining risk (what risk is there of disruption); taking countermeasures (if risk of disruption is unacceptable, what action can be taken to mitigate or eliminate the vulnerability) [47]. The surveillance of CEI is also a practical element to be taken into account and involves the use of unmanned aerial vehicles (UAV), networked sensors or radar systems [46].

5. Conclusion

The Critical Energy Infrastructure plays a vital role in the national security, economic and well–being of the society. The terrorist attacks can be prove very damaging as precious energy is used in residential, industrial and transport sectors, as well as the armed forces. The risk against CEI becomes increasingly dangerous as the correlation between terrorists and organized criminal may seriously undermine the level of security within the states. The post-Cold War era has created an environment where countries of the Euro-Atlantic pact face security threats from non-state and transnational actors [40].

South East Europe includes some regions which are considered vulnerable to terrorist attacks and the activities of organized crime. In particular, the Western Balkans is characterized as a "safe haven" for war profiteers, career criminals and fundamental Islamists due to their weak governmental structures and deteriorating economies. This situation may pose risk for the public security and order in the South East Europe and the wider Europe.

NATO should adopt a strategy that would focus on the parallel fight against terrorism and organized crime. The creation of a NATO Gendarmerie could be considered an appropriate mechanism to face the combined threats of Islamic terrorism and organized crime groups. The Alliance has the assets, capabilities and experience in military and peace-building operations. A NATO Gendarmerie should have the mission of border security, eradicating smuggling, the safety of financial, economic, judicial and public sectors and cyber-security. The Gendarmerie could be an independent authority on NATO headquarters and could be generated and deployed on ad hoc basis. NATO Member-States can dispatch forces, personnel and experts for staffing the NATO Gendarmerie.

The fighting of the Islamic terrorism and organized crime requires from NATO the adoption of an effective strategy that would combine counter-terrorism and anti-crime strategies. In particular its scope should be focused on:

(a) prevention: fighting radicalization and recruitment of terrorists by identifying their methods, propaganda and instruments used by them; the coordination of the national policies; sharing information; raising awareness of the reality and consequences; developing techniques to deter people from continuing in serious and organized criminality; establishing an effective offender management framework to support work on 'Pursue and Prevent', (b) protection: coordinating actions for border security, transport and other cross-border infrastructures; improving protective security in the private sector; people at risk of becoming victims; improving anti-corruption systems; strengthening systems for establishing identity, (c) pursuit: haunting terrorists to put an end to sources of terrorist financing by carrying out inquiries, freezing assets and impeding money transfers; establishing strong, effective and collaborative organizations capabilities; attacking criminal finances, ensuring that effective legal powers are available internationally; improving the capabilities and cooperation with others (d) response: exchanging the operational and policy information [48].

References

[1] NATO Parliamentary Assembly (2007) 162 CDS 07 E rev. 1, Annul Session, The Protection Of Critical Infrastructures, retrieved 30 March 2014 from www.nato-pa.int/default.asp?SHORTCUT=1165

[2] Moteff J. and Parfomak P. (2004), Critical Infrastructure and Key Assets: Definition and Identification, CRS Report for Congress, retrieved 27 March 2014 from www.fas.org/sgp/crs/RL32631.pdf

[3] European Council Directive (2008) /114/EC, retrieved 30 March 2014 from eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[4] OECD (2008) "Protection of 'Critical Infrastructure' and the role of investment policies relating to national security", retrieved 27 March 2014 from www.oecd.org/daf/inv/investment-policy/40700392.pdf

[5] Metzger J. (2004). The concept of Critical Infrastructure Protection (CIP), in Bailes, AJK and Frommelt, I. (Eds): Business and Security: Public – Private Sector Relationships in New Security Environment, Oxford, retrieved 30 March 2014 from books.sipri.org/files/books/SIPRI04BaiFro/SIPRI04BaiFro17.pdf

[6] Rinaldi S.M., Peerenboom J.P., Kelly T.K. (2001), Identifying, understanding, and analyzing Critical Infrastructure Interdependencies, IEEE Controls Systems Magazine, retrieved 29 March 2014 from www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf

[7] Dunn Myriam (2005), The socio-political dimensions of critical information infrastructure protection (CIIP), Int. J. Critical Infrastructures, Vol.1, Nos 2/3., p.262, retrieved 30 March 2014 from www.environmentalexpert.com/Files%5C6471%5Carticles%5C6388%5Cf412118326107915.pdf

[8] Haemmerli B. and Renda A. (2010), Protecting Critical Infrastructure in the EU, Regulatory Policy, CEPS Task Force Reports, retrieved 27 March 2014 from www.ceps.eu/book/protecting-critical-infrastructure-eu

[9] OECD (2008) Recommendation of the Council on the Protection of Critical Information Infrastructures, retrieved 30 March 2014 from www.oecd.org/sti/40825404.pdf

[10] Bahgat Bawdat (2006), Europe's energy security: challenges and opportunities, International Affairs 82: 5, p.965

[11] International Energy Agency (IEA) Energy security, retrieved 30 March 2014 from www.iea.org/topics/energysecurity/

[12] Cherp A. and Jewell J (2011)The three perspectives on energy security: intellectual history, Disciplinary roots and the potential for integration, Current Opinion in Environmental Sustainability 2011, 3:1- 11, retrieved 29 March 2014 from www.exeter.ac.uk/energysecurity/documents/publications/Cherp_and_Jewell%202011.pdf

[13] Von Hippel D.F, Suzuki T, Williams J.H., Savage T., Hayes P. (2011), Evaluating the energy security impacts on energy policies, in Sovacool B. K. (eds) The Routledge Handbook of Energy Security, Routledge: New York 2011, p.75

[14] Bauman Florian (2008), Energy Security as multidimensional concept, Center for Applied Policy Research (C·A·P) Policy Analysis, No1, retrieved 30 March 2014 from doc.vifapol.de/opus/volltexte/2009/784/pdf/CAP_Policy_Analysis_2008_01.pdf

[15] Metais Raphaël (2013), Ensuring Energy Security in Europe: The EU between a Market-based and a Geopolitical Approach, EU Diplomacy Papers 3/2013, retrieved 27 March 2014 from www.coleurope.eu/sites/default/files/uploads/page/edp_3_2013_metais.pdf

[16] Fedorowicz J. K. (2007), The Ten-Thousand Mile Target: Energy Infrastructure and Terrorism Today, Canadian Centre of Intelligence and Security Studies (CCISS), Critical Energy Infrastructure Protection Policy Research Series, No. 2, retrieved 30 March 2014 from: www3.carleton.ca/cciss/res_docs/ceip/fedorowicz.pdf

[17] Yergin Daniel (2006), Ensuring Energy Security, Foreign Affairs 85(2), retrieved 27 March 2014 from www.un.org/ga/61/second/daniel_yergin_energysecurity.pdf

[18] Ducaru Sorin (2014), NATO and Energy Security: Current Achievements and Future Challenges in Energy Security: Operational Highlights, NATO ENERGY SECURITY CENTRE OF EXCELLENCE, retrieved 9 August 2014 from www.enseccoe.org/en/news/energy-security-operational-gjqd.html

[19] NATO Strategic Concept 2010, "Active Engagement, Modern Defence", retrieved 29 March 2014 from www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

[20] ThessiMun (2013) "NATO's role in energy security: The uprising energy security challenge", retrieved 7 August 2014 from thessismun.org/2013/wp-content/uploads/2012/11/NAC-1st.pdf

[21] North Atlantic Treaty 1949, retrieved 8 August 2014 from www.nato.int/cps/en/natolive/official_texts_17120.htm

[22] NATO ESCD 2010, "New NATO division to deal with Emerging Security Challenges", retrieved 5 August 2014from www.nato.int/cps/en/natolive/news_65107.htm

[23] ENSEC COE 2014, “Doctrine & Concept Development”, retrieved 30 March 2014 from www.enseccoe.org/en/about-us/doctrine-concept-development.html

[24] NATO Response Force (NRF), retrieved 30 March 2014 from www.nato.int/cps/en/natolive/topics_49755.htm

[25] Sloan Elinor (2007), NATO Approaches to Energy Security: Future Options, Challenges and Directions, Canadian Centre of Intelligence and Security Studies (CCISS), Critical Energy Infrastructure Protection Policy Research Series, No. 1, retrieved 30 March 2014 from www3.carleton.ca/cciss/res_docs/ceip/sloan.pdf

[26] Niglia Alessandro (2013) Critical Energy Infrastructure Protection (CEIP): The role of EU and NATO, Police Brief of The Atlantic Treaty Association (ATA), retrieved 30 March 2014 from www.ata-sec.org/publications/policy-briefs

[27] Milstein Dan (2012), Energy security and NATO: a view from Washington, NATO Review Magazine, retrieved 30 March 2014 from www.nato.int/docu/review/2012/Food-Water-Energy/Energy-Security-NATO/EN/index.htm

[28] Garibaldi Ida (2008), NATO and European Energy Security, European Outlock (The American Enterprise Institute), No1, March 2008, retrieved 12 August 2014 from www.aei.org/files/2008/03/28/20080402_EuONo1_g.pdf

[29] Schori Liang C. (2011), Shadow Networks: The Growing Nexus of Terrorism and Organized Crime, Geneva Centre for Security Policy (GCSP) Policy Paper N° 20, retrieved 29 March 2014 from gcsp.ch/Resources-Publications/Publications/GCSP-Publications/Policy-Papers/Shadow-Networks-The-Growing-Nexus-of-Terrorism-and-Organised-Crime

[30] UNODC (2014), United Nations Office on Drugs and Crimes, The illicit drug trade through South Eastern Europe, p. 5, retrieved 30 August 2014 from www.unodc.org/documents/data-and-analysis/Studies/Illicit_DT_through_SEE_REPORT_2014_web.pdf

[31] European Parliament Study (2012) Europe’s Crime-Terror Nexus: Links between terrorist and organized crime groups in the European Union, Directorate General for Internal Policies of European Parliament, retrieved 29 March 2014 from www.europarl.europa.eu/document/activities/cont/201211/20121127ATT56707/20121127ATT56707EN.pdf

[32] OCTA - Europol (2011), EU Organized Crime Threat Assessment, retrieved 29 March 2014 from www.europol.europa.eu/sites/default/files/publications/octa2011.pdf

[33] SOCTA - Europol (2013), EU Serious and Organized Crime Threat Assessment, retrieved 29 March 2014 from www.europol.europa.eu/sites/default/files/publications/socta2013.pdf

[34] Arsovska Jana and Basha Dimal (2012), Globalizing the Western Balkans: Transnational Crime, Fundamental Islam and Unholy Alliances, Etudes Caribeennes, retrieved 30 March 2014 from http://etudescaribeennes.revues.org/5871#ftn18

[35] Hide Enri (2014), Islamic Extremism in the Balkans as a Geopolitical Instrument, Mediterranean Journal of Social Sciences, Vol 5 No 6,p.377

[36] Bakker Edwin, Paulussen Christophe, Entenmann Eva, (2013) “Dealing with European Foreign Fighters in Syria: Governance Challenges & Legal Implications”, ICCT Research Paper 2013, retrieved 8 August 2014 from www.icct.nl/download/file/ICCT-Bakker-Paulussen-Entenmann-Dealing-With-European-Foreign-Fighters-in-Syria.pdf

[37] Holman Timothy (2011) Foreign Fighters from the Western Balkans in Syria, The Combating Terrorism Center (CTC), retrieved 30 August 2014 from www.ctc.usma.edu/posts/foreign-fighters-from-the-western-balkans-in-syria

[38] Arvanites Nikos. (2012), Media 1996 – 20011, Athens: N.D.A. Arvanites, p.60

[39] Council of the European Union (2010), 9359/10 JAI 390, COSI 29, retrieved 8 August 2014 from www.statewatch.org/news/2010/aug/eu-council-eurojust-europol-frontex-int-sec-9359-10.pdf

[40] Lutterbeck Derek (2004), Between Police and Military The New Security Agenda and the Rise of Gendarmeries, Cooperation and Conflict: Journal of the Nordic International Studies Association Vol. 39(1): 45–68, retrieved 29 March 2014 from ftp://budgie3.ethz.ch/gcsp/e tilljune06/publications/CM_Peacebuilding/Peacebuilding/Academic_Papers/Lutterbeck_CAC.pdf

[41] See: “Articles 5 & 6” of the North Atlantic Treaty 1949

[42] NATO Strategic Concept 1999, retrieved 8 August 2014 from www.nato.int/cps/en/natolive/official_texts_27433.htm

[43] European Gendarmerie Force (EGF), retrieved 27 March 2014 from www.eurogendfor.org/organization/what-is-eurogendfor

[44] De Weger Michiel (2009), The Potential of the European Gendarmerie Force, Netherlands Institute of International Relations Clingendael, retrieved 29 March 2014 from www.clingendael.nl/sites/default/files/20090400_cscp_gendarmerie_weger.pdf

[45] Gacic Jasmina (2012), New Conception of Critical Infrastructure Vulnerability in Contemporary Terrorist Attacks, Journal of Defense Studies & Resource Management, September 07, 2012, retrieved 30 March 2014 from www.scitechnol.com/2324-9315/2324-9315-1-e105.php

[46] Borchert Heiko and Forster Karina (2007), The European View: EU and NATO must work together to guarantee energy infrastructure security and to define the role of soft vs hard power, Security Europe, March 2007, retrieved 29 March 2014 from www.atlanticcommunity.org/Energy%20Infrastructure%20Security%20and%20EU-NATO%20Cooperation1.pdf

[47] AFCEA (2008), Intelligence Support to Critical Infrastructure Protection, White Paper of The Intelligence Committee of the Armed Forces Communications and Electronics Association (AFCEA), retrieved 29 March 2014 from www.afcea.org/signal/articles/articlefiles/1783FallIntel08_WhitePaperweb3.pdf

[48] European Council (2005), European Union Counter-terrorism Strategy (2005) Prevent, Protect Pursue, Respond, 14469/4/05, retrieved 26 March 2014 from register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204 and Serious and Organized Crime Strategy (2013), Policy Paper of UK Government, retrieved 30 March 2014 from www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf

This page intentionally left blank

Section 5:
National Approaches to Critical Infrastructure Protection

This page intentionally left blank

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-235

Protection of the Critical Infrastructure from Terrorism: Case Study of the Republic of Croatia

Jadran PERINIĆ and Robert MIKAC [1]
National Protection and Rescue Directorate, Croatia

Abstract. Critical infrastructure represents a medium of national and international importance whose destruction, temporary or permanent disruption in process activities, would seriously endanger or weaken national and public safety, economic and social prosperity. Beside the internal threats, critical infrastructure is exposed to natural, technical-technological and anthropogenic threats, where terrorism is recognized to be one of the most unpredictable and dangerous sources of threats to the critical infrastructures. For that reason countries are responsible for the implementation and improvement of the critical infrastructures' protection and resilience to ensure survival, the development and advancement of individuals' and the social community, domestic and foreign economic subjects on their soil and, in partnership, achieving stability and safety of other countries. The goal of this work is to analyze how the Republic of Croatia has, so far, legally, regulatory and operationally developed protection and resilience of the national critical infrastructure, and give recommendations with regards to necessary steps in the continuation of the said process.

Keywords. the critical infrastructure, terrorism, protection and resilience, Republic of Croatia, regional context

Introduction

Critical infrastructure and terrorism represent two terms that are frequently used in the contemporary world. One is used in the positive and the other in the negative context. Their interaction is in the fact that many of those who deal in the area of critical infrastructure are trying to protect the said from terrorism. Many authors consider terrorism to be the leading threat to critical infrastructure while Elsa Lee goes even further and believes that terrorists' main targets in the United States of America (USA) and the most of the western countries are critical infrastructure [1]. Official policies of many countries and organizations in the field of critical infrastructure protection have been formed in the same way. But the said approach has certain cracks, starting with the inadequate terminological distinctness, conceptual underdevelopment of the critical infrastructure protection system, all the way to the inadequate national and international cooperation in the critical infrastructure protection. The mentioned phenomena are especially visible within the countries that are deficit with the normative frame of the critical infrastructure protection, are lacking main strategic documents in the area of national security or they are not updated, or are in certain measures unstable, whether from internal or external reasons.

[1] Corresponding Authors: Dr. Jadran Perinić, General Director, National Protection and Rescue Directorate, Croatia, E-mail: jadran.perinic@duzs.hr; Dr. Robert Mikac, Head of Sector for civil protection and Commander of civil protection of the Republic of Croatia, National Protection and Rescue Directorate, Croatia, E-mail: robert.mikac@duzs.hr.

The purpose of the article is to show the trends in the development of the critical infrastructure protection with special emphasis on the threats from global terrorism through the model existing in the European Union, to the regional context in Southeastern Europe, with the special review on the Republic of Croatia. The case study on the example of the Republic of Croatia will be shown as a part of the overall activities of the organizations to which Croatia belongs and through the individual efforts within the national frame.

In this work we represent the following hypothesis: (1) the critical infrastructure represents the important condition of the successful functioning and development of any society and country, and as a country is more advanced it is that much more dependent on critical infrastructure and more susceptible to the risks to their continuous functioning; (2) of all the threats to the functioning of the critical infrastructure terrorism represents one of the greatest and the most unpredictable; (3) Republic of Croatia, even though it has laid the normative frame for the critical infrastructure's protection, it is only just at the beginning of this comprehensive process. The methodological frame applied through the research comprises of the analysis of the strategic, normative and implementing documents in the area of the critical infrastructure's protection, discussions with the experts in the said area as well as the description of the processes in which the authors are part of themselves.

1. Challenges in critical infrastructure protection

The importance of critical infrastructure grows with the country's level of industrial development and its dependency on unobstructed functioning of critical infrastructure on its own territory as well as on foreign soil. The contemporary world has become extremely dependent on certain sectors of critical infrastructure, like the energy sector, communications, roads and the transportation systems, finances, Internet and public services and where every disruption in their functioning leads to serious halts and difficulties, from individual, through society and economic subjects to the functioning of the country.

Challenges in the critical infrastructure's protection are numerous. For the countries that are only beginning the formation of the critical infrastructure protection concept the challenges are manifested in understanding the importance of how the mentioned is important, developing the normative frame, identification, the designation of the sector and individual critical infrastructure, establishing adequate quality/cost measures of protection. Then, through the process of the designation of critical infrastructure the most important factors are of critical and national importance, so that it wouldn't come to pass that within the concept of critical infrastructure there are some ranked as such even though they, realistically, are not, so there may come to clogging in the very beginning. The next challenge is regarding the number of critical infrastructure and their interdependency and criticality as well as the dependency on the functioning of critical infrastructure on foreign soil. An additional challenge is the potential limitation of the institutional capacities and available knowledge for the mentioned activity which greatly hinders the overall approach to critical infrastructure protection. In the context of the critical structure protection a special challenge lies in internal and external threats. Elsa Lee groups the threats towards critical infrastructure functioning regarding to importance in the following categories: terrorism, sabotage, violence in the workplace, theft, espionage, explosives threat and IT threats [2]. The Centre for European Policy Studies Task Force on Critical Infrastructure Protection from the organizational aspects of the critical infrastructure protection challenges sees in: relationship between the public and the private sector; unbounded, specifically in the case of critical information infrastructures there are no physical barriers or political boundaries; increasingly networked; complex; dependency on decisions brought by people and vulnerability [3]. As we can see, the challenges in the protection of the critical infrastructure are multi layered, to which we must add the relationship between the public and the private sectors in the management and protection, the influence of the open market demands and the free flow of capital within the nationally sensitive economic branches, never sufficiently developed mechanism for the exchange of sensitive information between all the participants of the critical infrastructure protection system.

The challenges on the EU level in the process of identification, designation and protection of critical infrastructure are multidimensional because it is necessary to harmonize the Europe of "several speeds", harmonize different national policies and in all that to identify and create the Union identity in this area. While certain countries such as the Great Britain, Sweden, Switzerland, the Netherlands, Germany and France have advanced in the development of the national policies of critical infrastructure protection, in the area of public policies the EU is still searching for its place and role. The European Commission is striving to promote the importance of the mentioned topics, ensure cooperation between the countries, accelerate the exchange of knowledge and experience and direct the member countries in their endeavors. The Centre for European Policy Studies Task Force on Critical Infrastructure Protection deems that, even though the Commission has brought many political initiatives in this area, there still exist four major problems: ''First, member states are at varying degrees of maturity with respect to the development of a comprehensive and effective critical infrastructure protection policy. Second, there are islands of cooperation across the EU member states but no overall concept of operations at the EU level. Third, partnerships and relationships are scattered across countries (each individual country has and will maintain unique relationships with private sector owner operators and global companies that enable them). Fourth, critical EU infrastructure is also scattered across many different countries'' [4].

In the area of the Southeastern Europe, especially in the countries that have come to be through the process of the disintegration of Yugoslavia and are still not the part of the EU and NATO, still struggling with another set of priorities, the conceptual and normative field of critical infrastructure protection is still undeveloped. The Republic of Croatia, although it has achieved two of the main foreign policy goals after independence (admittance to NATO and the EU), is hurriedly endeavoring to implement the overall spectrum of activities and norms of the organizations in which it has been admitted including the area of critical infrastructure protection. Although it has, to a certain extent, in the recent years tried to standardize the question of national critical infrastructure, the mentioned has only been completed in 2013 by the assumption of the *Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* in the national legislation. Croatia still has a long road to the overall solution that will satisfy the needs of society, economy, state and assumed international obligations. Continuing the started activities – primarily for its self and then the partnership relations obligations within the organizations it is a member of, if it wants to keep the role of a leader in the region (however small that region may be) – the Republic of Croatia has to progressively continue to develop the field of critical infrastructure protection.

2. Terrorism as a global threat of the contemporary age

Terrorism in the contemporary world has been marked as one of the key challenges to peace, stability and security throughout the world. Although it represents the danger, equal danger represents the ignorance on what lies in the core of the phenomenon, what causes it and who it represents. The authors of the book *International Encyclopedia of Political Science* think that the definition of terrorism is routinely used outside its analytical frame to describe any act of the subjects that have been labeled as terrorists by the state elite and certain circles. What and who is labeled terrorism i.e. terrorist is molded by a political context, all for the reason of delegitimizing opponents and their actions and to justify special actions against them. That is why the term is more a politically-normative tool than a useful analytical concept [5]. According to Mirko Bilanđić ''[e]xactly that's why those different, politically motivated views on terrorism are one of the sources of terrorism's power" [6].

Terrorism is hard to define because often the starting views of the experts involved in a discussion are very different. The best proof of that fact is the many times quoted thought of the renowned international law professor Mahmoud Cherif Bassiouni that *what is terrorism to someone is a fight for freedom to other.* This attitude is considered as a cliché and untrue by Brian Michael Jenkins – because a terrorist to one is a terrorist to all people [7]. For Jenkins the terrorism is ''violence or the threat of violence calculated to create an atmosphere of fear and alarm – in a word, to terrorize – and thereby bring about some social or political change.... [H]allmark of terrorism are acts intended to produce psychological effects beyond the immediate physical damage" [8]. Alex Schmid in the book *Political Terrorism: A Research Guide* has analyzed 109 existing definitions of terrorism and has concluded – as many before and after him have – that it is impossible to define terrorism and that the only possible thing is to mark the most significant characteristics that separate it from other forms of felonies [9]. It is primarily separated by its political background and is, as Bruce Hoffman states, first of all a political concept [10]. Frank Ferudi also thinks that terrorism is impossible to define because, apart from being an objective analytical term, it is at the same time a multi-polar and extremely complex phenomenon and represents a moral judgment on behavior where the usual and most frequent moral judgments are brought by those who have a certain sort of authority for that [11].

Events on September 11th 2001, the terrorist attacks on New York and Washington have been labeled as the turning point in the contemporary understanding of security, challenges and threats to national and global security as well as choice of mechanisms to respond to the threats of terrorism. It is a consequence of the cumulative effect of all that happened that day and in the days that followed and the intensive media video coverage of the terrorist act itself and creating the 9-11 myth that followed. Terrorism has instantly become a global strategic security challenge and threat in many areas including critical infrastructure protection. The USA has proclaimed the "global war on terrorism" and has initiated worldwide international initiatives against terrorists. They have put themselves in the role of the leader in the "global war on terrorism" regardless of all logical, conceptual and implementing implications of the discourse. They have put aside all previous measures to suppress terrorism and responses to the terrorist acts and has have insisted on initiating military operations. Through counter terrorism operations Enduring Freedom and Iraqi Freedom, Afghanistan was quickly attacked and in 2003 Iraq. Parallel with these in Afghanistan the operation International Security Assistance Force started, which was taken over by NATO in 2003 and whose purpose is to help Afghani law representatives and security forces in the processes of the stabilization and reconstruction of the country. Within the corps of the included allies significant contribution came from European countries whether through NATO membership and/or European Union, but also certain countries from Southeastern Europe, which put them all in a position to become potential targets for the certain groups which do not agree with their policies and engagement in the "global war on terrorism".

3. Development of the critical infrastructure protection policy regarding the threat from terrorism

Critical infrastructure as a platform for the development of a society, economic subjects, countries, multinational corporations and organizations is getting more and more attention and significance with the growing requirements, widening of values and new needs of those to whose purpose they serve or contribute to. With the widening of the area of interest the number of sectors in which critical infrastructure is identified and determined is growing as well. The US Congressional Research Service says that the critical infrastructure in the US primarily used to be one necessary for military and economic needs. With time the number of critical infrastructure sectors has grown (today it is 17 sectors) and has, according to the criteria of criticality, spread from the area of national defense, through economic security to public health and in the end to the area of national morality (especially important monuments and public events). Along with the mentioned, the combination of the very fluid definition of critical infrastructure, the large number of sectors and nationally significant areas, it has overall become a great challenge for those who are related to critical infrastructure protection [12].

The leading countries of the world (outside Europe) in the area of critical infrastructure and its protection – USA, Canada and Australia – rather similarly define the above mentioned as the main challenges that are threatening them. The USA has started developing the area of critical infrastructure protection in the mid-1990s and in the 1998, in Presidential Decision Directive/NSC-63, defined critical infrastructure as ''physical and cyber-based systems essential to the minimum operations of the economy and government" [13]. Under the influence of the terrorist attacks on New York and Washington on September 11th 2001, immediately after the attack, Congress passed the *Patriot Act* in which critical infrastructure is defined as ''systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [14]. With the mentioned act the activities of the USA in the area of critical infrastructure protection are strongly tied with the defense against terrorism. Canada defines critical infrastructure as the: ''processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic wellbeing of Canadians and the effective functioning of government" [15]. Of all the risks to which the Canadian critical infrastructure is exposed to, terrorism is mentioned in the first place [16]. Australia defines critical infrastructure as ''those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defense and ensure national security" [17]. Australia views the term and the implementation of critical infrastructure protection exclusively through the prism of actions and measures that need to be implemented to prevent or reduce the threat of terrorism, but when it considers all of the risks then it uses the term critical infrastructure resilience.

The European Union, under the strong influence of the terrorist attack on the USA in 2001, the global war on terrorism that followed and serious terrorist attacks in Europe (2004 in Madrid, 2005 in London), has tied its initial discourse and critical infrastructure protection to the defense from terrorism. The European Commission in 2004 passed *Communication on Critical Infrastructure Protection in the fight against terrorism* in which the recommendation for what Europe should do to prevent terrorist attacks on critical infrastructure, raise its resilience and develop the ability to answer the attack were laid out [18]. A year later the Commission passed *Green Paper on the European program of Critical Infrastructure Protection* in which the solutions for establishing a program for the critical infrastructure protection and creation of information alert network in case of threats to critical infrastructure were proposed [19]. Then, in 2006, the Commission passed *European program of Critical Infrastructure Protection* in which all the dangers to critical infrastructure were considered, but terrorism has remained the primary focus and concern [20]. The Council of the European Union in 2007 made a decision on establishing a special program, *The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risk*, as a part of the General program of security and protection for the period from 2007 to 2013. The program recognizes numerous risks tied with security and in the middle there is a part dedicated to the support of member states' efforts to prevent terrorist attacks, prepare for protection and protect the people and critical infrastructure from risks related to terrorist attacks [21]. After that the Council passed the current key document in the area of critical infrastructure in Europe, *Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, which is no longer primarily focused on the threat of terrorism, but is endeavoring to completely set up the process of critical infrastructure protection on the level of the member states as well as the Union as a whole [22]. According to the Directive, critical infrastructure means ''an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions". The European critical infrastructure means ''critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure" [23]. As can be seen, the Union has focused its initial discourse primarily on the defense against terrorism. In time the other risks were more and more acknowledged and considered, but terrorism has remained declared as the main threat.

NATO presented the definition of critical infrastructure on the annual meeting of the Committee for the civil protection NATO/EAPC in 2002 in Brastov, Romania. According to the definition, critical infrastructure consists of adequate national capacities, services and IT systems which are of such vital importance that their inability to function or damage inflicted upon them could have direct influence on the national security, national economy, public health, public security and efficient functioning of the government [24]. NATO considers that critical infrastructure protection is not a separate area but that it is fitting in the wider frame of anti-terrorist policies and civil protection which are mainly directed to build a resilience of the civilian society against natural disasters, technological incidents and terrorist attacks and generally rely on multilayer strategies that include the prevention of terrorist threats; protection of people and infrastructure from the natural disasters, technological incidents and terrorist attacks; preparedness and consequence management; response and recovery.

The transitional countries in Southeast Europe, generally with a lack of strategic documents in the area of national security or their lack of updates, have difficulties in a sense that they haven't even terminologically determined what for them is critical infrastructure and what is the relationship between public-private partnership in management and critical infrastructure protection. It is worth to mention the opinion of the group of authors from Serbia who view the complexity of the protection problem through three prisms: ''1) cases of severe economic crime within critical infrastructure; (2) absence of public-private partnerships in protecting critical infrastructure; and (3) dramatically politicized management" [25]. The public-private partnership is the key link in the implementation of critical infrastructure protection policies because most of such infrastructure is private property, all are dependent on it, and no company in the world is able to protect its own property by itself from all the possible risks that are potentially threatening it without the cooperation of the public sector. Developed countries with developed policies of critical infrastructure protection view a public-private relationship as a necessary and extremely important element of the overall activities in the area of critical infrastructure protection. However, the transition countries are during the process – beside the lack of strategic frame for the public-private partnership in critical infrastructure protection – meeting with open questions of identifying, determining, ways and models of protection, but also the property of the critical infrastructure.

The Republic of Croatia has through its strategic documents approached critical infrastructure from different discourses. In *National strategy for prevention and suppression of terrorism* from 2008, critical infrastructure has been approached from the aspect of protection against terrorist threats [26]. *National strategy and Action plan for suppression of proliferation of the weapons of mass destruction* from 2013, as a special goal states critical infrastructure protection and public protection from crises caused by weapons of mass destruction [27]. *Assessment of vulnerability of the Republic of Croatia from natural and technical-technological disasters and large accidents* from 2013 views critical infrastructure in the wider light of protection from natural and anthropogenic threat sources [28]. *Protection and rescue plan for the Republic of Croatia* from 2010, as the most important document for the planning of the actions of the operative protection and rescue forces and the response system, views critical infrastructure in the context of the overview of the obligations of the participants included in the implementation of the protection and rescue measures [29]. Although the interest for critical infrastructure protection is clearly visible in the various strategic documents, none of them has given an overall solution, the first of the reasons being that it wasn't their main goal. With the passing of the *Critical infrastructure act*, by which the legislation of the Republic of Croatia assumed aquis communitare of the Union contained in the Directive 2008/114/EC, critical infrastructure protection has been approached from the all hazard approaches. National critical infrastructure has been defined as: ''the systems, networks and objects of national importance whose disruption in operation or interruption in the delivery of the goods can have serious consequences for national security, health and lives of people, property or environment, security and economic stability and continuous functioning of the government''. Under the term, protection has been defined as ''activities whose goal is to secure the functionality, uninterrupted operation and delivery of services/goods of critical infrastructure and prevent threats to critical infrastructure'' [30].

4. Strategic frame for the prevention and suppression of terrorism

Until 2001 terrorism was a challenge and a problem dealt with by the countries themselves in cooperation on many bases. The terrorist attack on the USA has, in a way, united the world on the question of terrorism. The UN Security Council that same year passed Resolution 1368 and 1373 (2001) by which it condemned terrorist attacks of any sort and called the members countries and the entire international community to prevent and suppress terrorism [31, 32]. Many regional organizations and countries, in their security strategies, and for the first time created strategies for prevention and suppression of terrorism, as well as the accompanying action plans, have expressed terrorism as the most significant danger of the contemporary age. The UN, as the organization of the member countries, in its documents and resolutions expectedly mentions responsibility, the need for action and the member countries' obligations. In the *Global Counter-Terrorism Strategy* from 2006 it called the countries to mutual cooperation and cooperation with the private sector in the prevention and suppression of terrorism, especially in the areas of security protection of ports and in maritime and civilian air transport. As especially important the exchange of the best practices between all of the involved in the prevention and suppression of terrorism and the development of the public-private partnership in this area has been accentuated [33].

The European Union has passed various security strategies and action plans regarding the prevention and suppression of terrorism (*European Security Strategy* in 2003, *Declaration on combating terrorism* in 2004*, EU Action plan for combating terrorism* in 2004*, Counterterrorist strategy* in 2005*, Internal Security Strategy for the European Union* in 2010, *Action plan for the implementation of the Internal security strategy* in 2010). *European Security Strategy* from 2003 out of five key challenges to the security of Europe places the threat of terrorism on the top [34]. *Report on the Implementation of the EU Security Strategy,* which was made five years later, mentions terrorism in high second place of threats to Union, its citizens and values for which the Union stands and defends [35]. *Internal Security Strategy for the European Union* from 2010 places terrorism in any form back to the first place of threats the Union must protect itself from [36].

NATO sees terrorism as a direct threat to the security of the citizens of the NATO member countries, international stability and development and considers terrorism to remain a significant threat in the years to come. After the terrorist attacks on September

11th 2001, all the NATO members agreed upon the activation of article 5 of the Washington agreement (for the first time in the history of the Alliance) which is a central clause of the agreement of the NATO fundamental charter, which says that the armed attack on one member is considered an attack on all the members. The NATO members have passed a series of measures on October 4th 2001, by which they supported the American fight against terrorism. Those measures included the exchange and cooperation in the field of intelligence, allowing the flight over their territories and access to the maritime and air ports for the US Forces and their allies in their operations against terrorism. Although they activated Article 5, not all members were ready to accept the inevitable operations in the field. It was questionable in what part certain members were willing to participate in the military forces in Afghanistan. NATO involved itself in those years in numerous measures and activities in the fight against terrorism. Also, the Alliance through several years on many occasions discussed the models for the prevention and suppression of terrorism and, at the Summit in Chicago in 2012, passed Policy guidelines on counter-terrorism. There have been set certain goals, principles and key areas of action of the Alliance in combating terrorism.

On a similar path are the strategic documents of the Republic of Croatia. The *Strategy of national security of the Republic of Croatia* (2002) recognizes terrorism as a global threat to common values, goals and means of the contemporary world and the Republic of Croatia completely supports the efforts and goals of the International antiterrorist coalition lead by the USA. Global terrorism has, with other security challenges, been rated a threat that can directly and indirectly influence the national security of the Republic of Croatia. The document states that the Croatian security concept of action is based on the assumption of the active involvement of all social components in the strengthening of security capacities and development of the resiliency to security risks and threats [37]. In the *National strategy for prevention and suppression of terrorism* (2008) the general frame of Croatia's initiatives in combating terrorism has been determined, giving guidelines for improvement of the existing and the development of new measures, mechanisms and instruments for the prevention and suppression of terrorism [38]. The *Action plan for prevention and suppression of terrorism* (2011) indicates that the response to terrorism demands the involvement and the continuing coordination and cooperation of the national and other society components [39]. The *National strategy and the Action plan for suppression of the proliferation of the weapons of mass destruction* (2013) reminds that the Republic of Croatia accepts all its obligations that result from its membership in the EU and NATO which regard the prevention and suppression of terrorism [40].

As the main coordinating body of all public administration bodies involved in the fight against terrorism, by the decision of the Croatian Government an Inter-Ministerial working group for the prevention of terrorism based at the Ministry of Foreign and European Affairs was established, and it is composed of representatives of the most important departments in this area. Inside the criminal legislation the Republic of Croatia has taken into consideration, in the content of legal rules which regulates questions of sanctions against terrorist behavior, the provisions which regulate this matter in accordance with all international conventions in the field of the prevention and suppression of terrorism and generally accepted principles of international criminal law. In addition to active participation in the various activities of the UN, EU, NATO, Interpol and Europol, it is worthwhile to point out that the Republic of Croatia in the period of 2008-2009 was a non-permanent member of the United Nations Security Council and chaired the Security Council's Counter-Terrorism Committee. It is worthwhile to point out that in the Republic of Croatia the last offense of terrorism was recorded in the year 1995.

The question arises what is the level of threat from terrorism in Europe and apart from that threat what are the specific security challenges present in Southeastern Europe? Especially for the reason that all different security challenges and threats represent the strong direct and indirect danger to the functioning and protection of critical infrastructure, especially to the weak transition countries in Southeastern Europe. According to the latest available Europol estimates for 2012 it is plain that the number of recorded terrorist attacks and arrests connected with terrorism have increased in relation to the preceding years. According to Europol the threats from terrorism are strongly present in Europe [41]. The area of Southeastern Europe, apart from the occasional terrorist incidents, has been marked by: recent wars and unsolved questions as the consequences of those wars, challenges of (un)recognizing of the political statutes and borders, open questions on the statutes and rights of ethnic minorities in other countries, the proximity of the crisis centers in the Middle East and departure of the people to the conflicts there and challenges upon their return, weak state institutions, porous borders, strongly present trans-border groups of organized crime, the smuggling Balkan route, the presence of people in certain countries that have been recognized by the official government representatives as persons who represent threats to national security (in Bosnia and Herzegovina).

5. The concept of protecting critical infrastructure in the Republic of Croatia

In the period of the creation of the proposal of the *Critical infrastructure act* and the passing of the Act different opinions could be heard on the current state and way of forming the concept of critical infrastructure protection in the Republic of Croatia, which are worth mentioning to get a clearer picture of the current and the coming challenges for the Republic of Croatia. Zvonko Orehovec, as the challenges for the Republic of Croatia on all levels, emphasizes that the Armed Forces and the subjects of internal security in parallel "protect the elements of critical infrastructure and no one cares that the potential enemy needn't cross the border with armed force to disturb the integrity, sovereignty and the territorial wholeness of the Republic of Croatia, but is quite enough and legal to become the owner of the elements or all of critical infrastructure" [42]. In regard to the lack of the strategic frame for the state of the overall national security of the Republic of Croatia, Ante Orlović thinks that "the state isn't on the satisfactory or the expected level, and can be regarded as a state of *strategic insufficiency*. It consists of *strategic confusion* – regarding the economic crime, *strategic rudimentary* - regarding national critical infrastructure and *strategic lack of focus* – regarding the mutual reciprocity of the two strategic frames" [43]. According to the portal Svijetsigurnosti.com at the roundtable "Protection of critical infrastructure: Challenges for NATO, EU and Republic of Croatia" (''Zaštita kritične infrastrukture: Izazov za NATO, EU i Republiku Hrvatsku''), held in 2013 within the *Croatian Security Days conference*, participants were "Ines Krajčak, Assistant minister for the Internal Affairs of the Republic of Croatia, Vlatko Cvrtila, dean of the Vern University and Dragan Kovačević, President of the Board of JANAF. The participants came to an agreement that the *Critical infrastructure act* is lacking, first of all because it assigned the National Protection and Rescue Directorate the task of implementing the critical infrastructure protection. Namely, in most of the European countries a much higher state body is assigned for such tasks, with access to all the security information, necessary for the adequate critical infrastructure protection. National Protection and Rescue Directorate simply has other tasks…" [44].

By passing the *Critical infrastructure act*, apart from assuming aquis communitaire contained in the Directive 2008/114/EC in the legislature of the Republic of Croatia, the first step to the establish the concept of critical infrastructure protection in the Republic of Croatia was made. By that Act the rights, authorities and obligations of the Government of the Republic of Croatia, its state bodies of administration and the owners, i.e. administrators of critical infrastructure in identifying, determining and protecting national critical infrastructure and securing their uninterrupted functioning have been determined. In the same way, the Law determines the definitions of national and European critical infrastructure, sectors of national critical infrastructure, management of the critical infrastructure, creating Risk Analysis, owners/administrators Security plans, security coordinator for critical infrastructure, handling sensitive and classified data and supervision over the implementation of the Act. The Act represents the basis for the initiation of the multi sectorial process of cooperation in identifying, designating and protecting national critical infrastructure and cooperation with neighboring countries and bodies of the European Union in determining and protecting critical infrastructure on the territory of the Republic of Croatia and other countries [45]. On the basis of the Act, the Government of the Republic of Croatia passed the *Decision on designation the sectors from which the central state administrative bodies identify national critical infrastructure and lists of the order of the sectors of critical infrastructures.* In total eleven sectors have been determined from which the central administrative bodies can identify the national critical infrastructure. Those sectors are: 1. Energy, 2. Communications and IT technology, 3. Transport, 4. Public health, 5. Water management, 6. Food, 7. Finances, 8. Production, storing and transport of hazardous materials, 9. Public sector, 10. National monuments and valuables, 11. Science and education [46]. As the last step in the implementation of the initial normative frame for identifying, designating and protecting the national critical infrastructures, the General Director of the National Protection and Rescue Directorate brought the *Rules on the methodology for drafting business risk analysis of critical infrastructure* [47], which determines the guidelines, criteria and measures for identifying critical infrastructure and management risk analysis of critical infrastructure. After bringing the normative frame the conditions were created for the process of the overall action in protecting, strengthening resiliency and reducing the negative effects in case of threats to critical infrastructure. By the normative frame the Republic of Croatia has set the presuppositions for the forming of the system that will be competent for the protection of critical infrastructure, domestic and European should they be marked territory, alike. Until the whole system and policy of critical infrastructure protection is established a lot of time is required, as well as efforts and learning from those that are ahead of us in that area.

6. Recommendations for the improvement of critical infrastructure protection in the Republic of Croatia

The Republic of Croatia started the process of critical infrastructure protection just before becoming a member of the EU by implementing Directive 2008/114/EC in the national legislature. The Directive isn't primarily focused on the threat of terrorism, like the documents the Union bodies have brought before, but is trying to comprehensively set the process of critical infrastructure protection on both the Union and member country levels. The Republic of Croatia is taking the all hazard approach to critical infrastructure protection, where, as we have seen from the strategic documents from the area of national security, it is absolutely aware of the dangers of terrorism to values, interests and goals which it protects, critical infrastructure among them.

As one of the initial steps that could be useful to initiate is the organization of the education of all the security coordinators and their deputies in the implementation of the regulations of the *Critical infrastructure act*. After that it would be wise to start the education of the security coordinators at owners/operators who will manage certain critical infrastructure so everybody would have the common initial basics on criticality, national importance, inter-dependability of various infrastructures and ways of functioning of the concept of critical infrastructure protection. In this initial phase of the Croatian model of critical infrastructure protection it is crucial to invest in the knowledge of those that will perform the said task for the State and in the name of the owner/operator of critical infrastructure. We feel that the said initiative and the initial impulse must be initiated from the national level. In countries with the developed systems of critical infrastructure protection there is a great attention to education and there are wider possibilities than in the Republic of Croatia, so it is important to realize the internal capabilities and the most acceptable possibilities of education from domestic and foreign experts and to creating a Croatian model of training the key personnel for their tasks and roles.

In the phase of the designation of critical infrastructure, special attention should be placed to the attributes of criticality and national importance so there wouldn't come a situation where certain sectors aspirations', to show their importance within the whole system of the national administration and the area of critical infrastructure, would propose to the Government to bring a decision on designation to large a number of critical infrastructure. Such an approach can potentially crate administrative difficulties in data processing and the analysis of the criticality of the management of certain infrastructures and slow the whole process. At the same time the challenge will certainly come from designating the level of classification of certain infrastructures and data. If a large number of them should be classified as Secret and Top secret that will most certainly slow the flow of information between participants in the system and the functioning of the whole system. The recommendations in this part certainly go in the direction that it is necessary to be careful in the classifying the secrecy levels and, at least at the start, for every object to consult the national security agency – Office of the Council for national security. Additionally it would be recommended to take care of the transparency principle versus too much secrecy. Besides that, after the designation of critical infrastructure in the Republic of Croatia, it will be necessary to recommend to the Government of the Republic of Croatia to prioritize critical infrastructure with a decision because not every critical infrastructure or even all their parts are not equally important and not all require the same level of protection. The said will have a positive impact within the public and private sectors.

One of the key questions of the successful functioning of the critical infrastructure protection is the establishment of the public-private partnership in the said area. The private sector owns and operates most of the critical infrastructure in the more developed democratic countries and Croatia is following in that direction. The private sector, apart from being the owner and administrator, has the responsibility and the obligation to protect them. It cannot do that efficiently and cost effectively without the quality cooperation with the public institutions. Here many questions open, like: building of trust, developing common procedures, sharing confidential information and data, the exchange of experiences and practices. Great work lies ahead of the Republic of Croatia in this area. In this part it is necessary to establish a mutually acceptable model of cooperation, counseling and exchange of knowledge and information. We suggest that it be organized as one of the functionalities of the Center for critical infrastructure protection.

Such a center does not exist in the Republic of Croatia and we feel it is necessary. There is publicly available information on quality examples of such centers functioning in the world, it is necessary to analyze their activity and take the best for the Republic of Croatia. Forming the Center would be possible either by establishing the new body of, as we suggest, by expanding the authorities and responsibilities to one of the existing operative-communication centers, increasing its manpower and materiel resources and to promote it to the center of excellence that would be operational 24/7 every day of a year as an administrative unit, control point and operational segment for the exchange of information between all of the relevant domestic and international subjects, and implementing measures important to critical infrastructure protection. The center should have support in advanced software solutions for following elements of all critical infrastructures in the Republic of Croatia and IT tools as decision support. As a platform for the successful functioning of the system for critical infrastructure protection there should be established a protected IT network for the exchange of information between the most important elements in the system. Besides all of that, the Center must have an educational role, must be capable that through its own experts of organizing simulation exercises and additional education of the subjects with whom it cooperates. The creation of such a center is a long and complex task, which can be partially funded out of the EU funds, but it shouldn't be viewed as a problem but a challenge if there exists a vision of what the Republic of Croatia wishes to accomplish in the critical infrastructure protection today, tomorrow and in ten years' time.

7. Conclusion

Through research we have shown and confirmed the hypothesis on the attitudes of the relevant subjects that the critical infrastructure represents the condition for the successful functioning and the development of any society and country and that as the country is more advanced it is all the more dependent on critical infrastructure as well as more susceptible to the threats for their continuous functioning. To the primary focus, among the great number of threats to the continuous functioning of the critical infrastructure, we've put the threat of terrorism and have shown that terrorism presents a global threat which, beside its destructive power, also presents a threat because of differing positions on what it is, what it represents and how to successfully counter it. The central position in the review of the founding of the framework for the protection of the critical infrastructure is given to process in the Republic of Croatia, as well as the recommendations for the continuing said process. In the methodological framework we have started from the global actors in the critical infrastructure protection – the USA, Canada and Australia – following with the conditions at the European Union level and, through the Southeastern Europe region, the discussion has led to the Republic of Croatia.

Critical infrastructure and its protection, primarily from threats of terrorism, represent the area of intensive activities from global, through regional to national levels. That has been recognized in many documents of various hierarchical levels, but always the question of the implementation arises. It is necessary to differentiate the countries that have normatively regulated the area of critical infrastructure protection from those that haven't. The ones that haven't protected their infrastructure with a spectrum of different normative and operational measures and arrangements. But the system and the implementation of the protection measures are certainly more recognizable and better regulated if there is a normatively regulated definition and established phases of the identifying, designating and protecting of critical infrastructure. The Republic of Croatia has paid certain declaratory attention to critical infrastructure in some strategic documents until its acceptance in the EU, but has never established the rounded normative frame of the initial laws and subordinate regulations so the process could be initiated. By passing the *Critical infrastructure act* and, based on it, the subordinate regulations, Croatia has formed the necessary initial normative frame out of which, in the period that follows, the critical infrastructure will be identified by sectors, through the Government Decision determined and the Decision will be submitted to the owners/operators of the critical infrastructures for implementation. In the said process there are a lot of open questions that will be answered as we go, so that we can, in time, build the optimal system of the national and the European critical infrastructure protection on the territory of the Republic of Croatia.

References

[1] Lee, E. (2009) *Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection*, Boca Raton, Taylor & Francis Group: Auerbach Publication.

[2] Ibid.

[3] Heammerli, B. and Renda, A. (2010) *Protecting Critical Infrastructure in the EU,* Brussels: Centre for European Policy Studies, http://www.ceps.eu/ceps/dld/4061/pdf (cited 5 February 2014).

[4] Ibid, page 3.

[5] Badie, B., Berg-Schlosser, D. and Morlino, L. (Ed.) (2011) *International Encyclopedia of Political Science, Volume 8.* Los Angeles, SAGE Publication, Inc., page 2591.

[6] Bilandžić, M. (2010) *Sjeme zla: Elementi sociologije terorizma.* Zagreb: Plejada d.o.o. i Synopsis d.o.o., page 80.

[7] Jenkins, B. M. (1980) ''The study of terrorism: Definitional problems'', The Rand Corporation, December 1980. California, Santa Monica, http://www.rand.org/pubs/papers/2006/P6563.pdf (cited 2 February 2012), page 2.

[8] Jenkins, B. M. (1985) ''International Terrorism: The Other World War'', The Rand Corporation, November 1985. California, Santa Monica, http://www.rand.org/content/dam/rand/pubs/reports/2005/R3302.pdf (cited 2 February 2012), page 2-4.

[9] Schmid, A. P. (1984) *Political Terrorism: A Research Guide*. New Brunswick, N.J.: Transaction Books.

[10] Hoffman, B. (2006) *Inside Terrorism*. New York: Columbia University Press.

[11] Ferudi, F. (2009) *Poziv na teror: rastuće carstvo nepoznatog.* Zagreb: Naklada Ljevak.

[12] Moteff, J., Copeland, C. and Fischer, J. (2003) *Critical Infrastructure: What Makes an Infrastructure Critical?,* Congressional Research Service, The Library of Congress, http://www.fas.org/irp/crs/RL31556.pdf (cited 9 Febraury 2014).

[13] White House (1998) *Presidential Decision Directive/NSC-63,* Washington, https://www.fas.org/irp/offdocs/pdd/pdd-63.htm (cited 3 February 2014).

[14] United States Congress (2001) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (The USA PATRIOT Act),* 26.10.2001., http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (cited 3 February 2014), page 401.

[15] Government of Canada (2009) *National Strategy for Critical Infrastructure*, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf(cited 3 April 2014), page 2.

[16] Government of Canada (2014) *Action Plan for Critical Infrastructure (2014-2017)*, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf (cited 3 April 2014).

[17] Commonwealth of Australia, National Counter-Terrorism Committee (2011) *National Guidelines for Protection Critical Infrastructure from Terrorism,* Business Law Branch, Attorney-General's Department, http://www.nationalsecurity.gov.au/Mediaandpublications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf (cited 4 February 2014), page 3.

[18] European Commission (2004) *Communication on Critical Infrastructure Protection in the fight against terrorism,* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702 (cited 5 September 2013).

[19] European Commission (2005) *Green Paper on the European program of Critical Infrastructure Protection,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576 (cited 5 September 2013).

[20] European Commission (2006) *European program of Critical Infrastructure Protection,* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786 (cited 5 September 2013).

[21] Council of the European Union (2007) *The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007D0124 (cited 6 September 2013).

[22] Council of the European Union (2008) *Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Brussels, 2008/114/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:18:03:32008L0114:HR:PDF (cited 1 February 2014).

[23] Ibid, page 174.

[24] Toth, I., Čemerin, D. and Vitas, P. (2011) *Osnove zaštite i spašavanja od katastrofa*, Velika Gorica: Veleučilište Velika Gorica, page 135.

[25] Davidović, D., Kešetović, Ž. and Pavičević, O. (2012) ''National Critical Infrastructure Protection in Serbia: The Role of Private Security'', *Journal of Physical Security*; 6(1), 59-72, Argonne National Laboratory, http://jps.anl.gov/Volume6_iss1/Davidovic.pdf (cited 15 February 2014), page 69.

[26] Government of the Republic of Croatia (2008) *Nacionalna strategija za prevenciju i suzbijanje terorizma,* Official Gazette, No: 139/2008.

[27] Government of the Republic of Croatia (2013) *Nacionalna strategija i Akcijski plan za suzbijanje širenja oružja za masovno uništenje.*

[28] Government of the Republic of Croatia (2013) *Procjena ugroženosti Republike Hrvatske od prirodnih i tehničko-tehnoloških katastrofa i velikih nesreća,* http://duzs.hr/download.aspx?f=dokumenti/Clanci/PROCJENA_web_20.03.2013..pdf (cited 5 February 2014).

[29] Government of the Republic of Croatia (2010) *Plan zaštite i spašavanja za područje Republike Hrvatske,* http://duzs.hr/download.aspx?f=dokumenti/Stranice/PlanZiSzapodrucjeRepublikeHrvatske.pdf (cited 8 March 2014).

[30] Croatian Parliament (2013) *Zakon o kritičnim infrastrukturama*, Official Gazette, No 56/2013.

[31] United Nations (2001) *Security Council resolution 1368 (2001) Threats to international peace and security caused by terrorist acts,* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement (cited 14 February 2012).

[32] United Nations (2001) *Security Council resolution 1373 (2001) Threats to international peace and security caused by terrorist acts*, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement (cited 14 February 2012).

[33] United Nations (2006) *The United Nations Global Counter-Terrorism Strategy,* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/504/88/PDF/N0550488.pdf?OpenElement (cited 14 February 2012).

[34] European Council (2003) *A Secure Europe in a Better World: European Security Strategy,* http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf (cited 5 May 2011).

[35] European Council (2008) *Report on the Implementation of the EU Security Strategy,* http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf (cited 5 May 2011).

[36] Council of European Union (2010) *Internal Security Strategy for the European Union: Towards a European Security Model,* http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf (cited 5 May 2011).

[37] Croatian Parliament (2002) *Strategija nacionalne sigurnosti Republike Hrvatske*. Official Gazette, No: 32/2002.

[38] Government of the Republic of Croatia (2008) *Nacionalna strategija za prevenciju i suzbijanje terorizma,* Official Gazette, No: 139/2008.

[39] Government of the Republic of Croatia (2011) *Akcijski plan za prevenciju i suzbijanje terorizma.*

[40] Government of the Republic of Croatia (2013) *Nacionalna strategija i Akcijski plan za suzbijanje širenja oružja za masovno uništenje.*

[41] European Police Office (2013) *The EU Terrorism Situation and Trend Report (TE-SAT),* https://www.europol.europa.eu/sites/default/files/publications/europol_te-sat2013_lr_0.pdf (cited 3 April 2014).

[42] Orehovec, Z. (2013) ‘’Stara strategija nacionalne sigurnosti u zaštiti kritične nacionalne infrastrukture od novih sigurnosnih ugroza’’. In: Nove sigurnosne ugroze i kritična nacionalna infrastruktura. Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska Akademija, page 228-236.

[43] Orlović, A. (2013) ‘’Gospodarski kriminalitet i nacionalne kritične infrastrukture – strategijski okvir u Republici Hrvatskoj’’. In: Nove sigurnosne ugroze i kritična nacionalna infrastruktura. Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska Akademija, page 237-253.

[44] Portal Svijetsigurnosti.com (2013) ‘’Hrvatska kritična infrastruktura sada je dio europske i zato ju treba kvalitetno štititi’’, http://www.svijetsigurnosti.com/blogs/3089-hrvatska-kriticna-infrastruktura-sada-je-dio-europske-i-zato-ju-treba-kvalitetno-stititi (cited 2 April 2014).

[45] Croatian Parliament (2013) *Zakon o kritičnim infrastrukturama*, Official Gazette, No 56/2013.

[46] Government of the Republic of Croatia (2013) *Odluka o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura,* Official Gazette, No: 108/2013.

[47] National Protection and Rescue Directorate (2013) *Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura*, Official Gazette, No: 128/2013.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015

© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-251

Terrorist Threats to Critical Infrastructure in BiH and Protection Measures

Mile ŠIKMAN [a,1] and Nevenko VRANJEŠ [b]
[a] *Police College, University of Banja Luka, Banja Luka*
[b] *Faculty of Political Science, University of Banja Luka, Banja Luka*

Abstract. Terrorism, as a global negative threat, endangers not only the security of individual countries, but also of the international community. Still, individual countries and protected values (the life and health of people, assets, etc.) are predominantly affected by it. Terrorist threats pose special danger to critical infrastructure. The risk from endangering critical infrastructure is on the rise, considering "the domino effect" of endangering critical infrastructure. The domino effect does not only imply the negative consequences within the borders of a country, but it also has a wider influence (a regional and even international dimension). Of course, the entire critical infrastructure system is at risk from terrorist activities, in particular cyber terrorist offences, which can endanger the key infrastructure of the country, burden communication systems, and even cause serious consequences for the security system within the country. Bosnia and Herzegovina is not an exception. In that sense, the list of critical infrastructure sectors poses a potential target for terrorist attacks, but also for cyber terrorism. Thus, it is extremely important to identify the sectors of critical infrastructure, and create adequate measures for their protection. In that regard, the paper points to some key European standards for the protection of critical infrastructure, and concrete antiterrorist and counterterrorist activities for their protection.

Keywords. terrorism, critical infrastructure, antiterrorism, counterterrorism, Bosnia and Herzegovina

Introduction

Terrorism, as a form of violence, has become an increasing threat to both homeland and international security in the contemporary world. The analyses of terrorist activities show that terrorism threat is at a high global level, considering the fact that the number of countries endangered by terrorism is high, that there are many terrorist organizations, and that there are attacks with a significant number of casualties and material damage. This points to the threat from all forms of terrorism, including suicidal terrorism and a terrorist threat to the world with the weapons of mass destruction, whereby the international community has no adequate protection system against terrorism [1]. Terrorism is a difficult word to define because it is a "contextual concept" so there is often a discrepancy between political, legal and social sciences in defying the term. The lack of a universal definition of the term 'terrorism' is brought about by a large number of incompetent authors who have proclaimed themselves experts on the theoretical interpretation of modern terrorism; the double standards of some great powers on the definition and meaning of terrorism or, in the modern sense called – the politics of terrorism [2]. In this paper we will use the NATO definition of terrorism: "The unlawful use or threatened use

[1] Corresponding Author: Dr. Mile Šikman, Police College, University of Banja Luka, Banja Luka, e-mail: msikman@teol.net

of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives" [3].The rising transnational, i.e. contemporary postmodern terrorism, enriched with new forms of manifestation and personified with extreme radical religious, particularly pan-Islamic fundamentalism, took on a global character and turned into the most serious threat to the world's security at the end of the XX century[2] [4].

When it comes to terrorism, Bosnia and Herzegovina is no exception. Numerous factors have contributed to the occurrence of terrorism in BiH, in particular those factors that give terrorism in BiH its international connotation. Available data point to the presence and establishment of contacts between suspicious foreign persons who are linked with international terrorism, or with other persons abroad from the same milieu, and possible misuse of Bosnia and Herzegovina as a transitional country for terrorist activities[3]. Equally, based on the available data it can be said that the earlier trend of aggressive and provoking activities of particular individuals and groups from some legal organizations and associations of national and religious character, which are active on the territory of Bosnia and Herzegovina, is still present. The last period has been marked, and in some cases it has intensified, with the activities of particular members of radical religious groups in Bosnia and Herzegovina and the region. These activities are colored with the spreading of radical religious movement and ideology, i.e. gaining of new followers. Some of them, through intensive activities (mostly verbal in nature) on religious and ideological levels, negate the constitutional-legal order, and regulations and laws of the state in general [5]. As a relatively new phenomenon in Bosnia and Herzegovina, the last period has been marked with the misuse of cyber technology, primarily the Internet, by differentiated extreme-radical security interest subjects (persons, groups, organizations, associations and alike). The common characteristic of the abovementioned structures is that they use cyber technology (primarily the Internet) for mutual communication, the spreading of radical ideology, the indoctrination of declared and potential sympathizers, the distribution of various contents (propaganda activities aimed at supporting global terrorist organizations and movements via chat, web forums and websites), the gathering and exchanging of data and information (documents, brochures, books, audio and video materials), raising funds, the recruitment, drafting, mobilization and training of new members, the interconnection and connection of the cells and the members, planning, coordinating and controlling of activities, and execution of IT and psychological war. Some website analyses show that virtual attacks are not just sporadic individual initiatives, but that they are becoming coordinated activities[4] [5]. Aside from the aforementioned, Bosnia and Herzegovina has been a home to legal procedures against the suspects and accused of terrorism[5], which has resulted in some court rulings.[6]

The negative effects of terrorism are manifested through at least three dimensions of state and social life: human, economic and security (in the narrow sense); the human dimension is related to the violation of human rights of many direct and indirect victims of terrorism. The problem is even greater since many of these countries still do not have prescribed special strategies for prevention of and combating terrorism, i.e. for the protection of human rights of potential and current victims, which usually leads to their victimization; the economic dimension implies the effects of terrorism which further deepen unfavorable factors of economic transition, which are, among other, one of the causes and conditions of its manifestation and the security dimension which is concerned with the threats to national security by slowing down the democratic processes of the so called "transitional societies", by undermining democratic institutions and ruling of the law and creating numerous social-economic problems [6]. Potential terrorist attack targets in BiH, unfortunately, are diverse, ranging from the safety of aircraft flights, power plants, the transportation and communication infrastructure, diplomatic facilities and facilities of special importance for BiH and the international community, to the point of mass gatherings such as schools, hospitals, public transportation, city squares and alike. Actually, the entire list of the critical infrastructure sectors, drafted by the European Commission in 2005, poses a possible target for terrorist attacks [7].

Taking into consideration the aforementioned we can give a general hypothesis: terrorism poses a serious threat to the critical infrastructure in Bosnia and Herzegovina, and it is necessary to develop modern methods of protection. Terrorism can be perceived as a direct threat to the security of citizens and their property, international security, as well as a threat in the future. The terrorism attacks against critical infrastructure also have a cross-border influence. Therefore it is argued that terrorism acts are endangering the entire critical infrastructure system. Cyber terrorism poses a special threat to critical infrastructure. In that sense, critical infrastructure represents a potential terrorist target, therefore it is necessary to build an adequate system of protection, including antiterrorism elements, but also concrete counterterrorism measures. Available referential data are used in this paper. The content analysis method is used to determine the seriousness of terrorist threat to the critical infrastructure in Bosnia and Herzegovina, the forms of its manifestation, and protection measures. Further, the current system of protection is scrutinized, including some European standards, and measures and activities for the improvement of institutional and organized frame of counterterrorist protection are suggested. In the end, by summarizing and consolidating data, the authors give the final analysis and conclusions on the terrorist threat to the critical structure in Bosnia and Herzegovina. Limitations and difficulties in this research relate to data collection, hence they imply standard difficulties deploying qualitative and quantitative methods, such as content analysis method, comparative method and other methods used in the research. The main limitation is that the case study is very complex and it is not possible to view here all the aspects of terrorist threats to the critical structure in Bosnia and Herzegovina. The research results bring about to better understanding of the police and policing in multiethnic environment, and its practical implications. Based on collected data and new data resulting from this research, it will be possible to formulate suitable propositions with the aim of improving the critical structure in Bosnia and Herzegovina. Accordingly, the purpose of this paper is to point to the ways of further development and improvement of protection of the critical infrastructure, and thus the security of citizens, property, as well as regional and international security in broader sense.

1. Terrorism Threats to Critical Infrastructures

The term Critical Infrastructure came into use during the mid 90s[7] [8][9]. Critical infrastructure has been defined in various ways over time, but generally consists of "those physical or cyber-based systems essential to the minimum operations of the economy and government". Critical infrastructure can be widely defined as a set of assets, systems and services that sustain economic, political and social life of a country, and whose partial and complete endangerment can cause human losses, threaten national security and functioning of economy, i.e. it can seriously threaten a part of the community or the entire state community[8] [10]. Therefore, Critical Infrastructure includes many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services. Some critical elements in these sectors are not strictly speaking 'infrastructure', but are in fact, networks or supply chains that support the delivery of an essential product or service. Namely, the threat to critical infrastructure is on the rise, both from the aspect of the way of threatening critical infrastructure and from the aspect of potential target attacks. The damaged caused by a terrorist attack can be seen in the form of a direct attack on particular segments of critical structure (e.g. an attack on industrial plants, government facilities, etc.) or an attack on particular segments of critical infrastructure that other segments depend on, which leads to "the domino effect" in terms of consequences (a typical example would be an attack on power plants or the water supply system).

The first European interpretation of what is considered critical infrastructure was given in the COM Report[9] (2004) 702 "Critical Infrastructure Protection in the fight against terrorism" [11], accepted on 20 October 2004. Critical infrastructures include[10]:

- Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system),
- Communications and Information Technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet),
- Finance (e.g. banking, securities and investment),
- Health Care (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services),
- Food (e.g. safety, production means, wholesale distribution and food industry),
- Water (e.g. dams, storage, treatment and networks),
- Transport (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems),
- Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials),
- Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments).

The criteria for determining the factors that make a particular infrastructure or element of a critical infrastructure need to be studied. These selection criteria should also be based on sector and collective expertise. Three factors might be suggested for identifying potential critical infrastructure: Scope - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, provincial/territorial or local; Magnitude - The degree of the impact or loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which could be used to assess potential magnitude are: (a) Public impact (amount of population affected, loss of life, medical illness, serious injury, evacuation); (b) Economic (GDP effect, significance of economic loss and/or degradation of products or services); (c) Environmental (impact on the public and surrounding location); (d) Interdependency (between other critical infrastructure elements); and (e) Political (confidence in the ability of government); Effects of time - This criterion ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other). However, in many cases, psychological effects may escalate otherwise minor events.

On 17 November 2005 the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection [7] which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network. The responses received to the Green Paper emphasised the added value of a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged. The importance of the key principles of subsidiarity, proportionality and complementarity, as well as of stakeholder dialogue was emphasized. In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection ('EPCIP') [12] and decided that it should be based on an all-hazards approach while countering threats from terrorism as a priority. Under this approach, man-made, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority. This directive sets up a procedure for identifying and designating European critical infrastructures (ECIs). At the same time, it provides a common approach for assessing these infrastructures, with a view to improving them to better protect the needs of citizens. In April 2007 the Council adopted conclusions on the EPCIP in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European critical infrastructures ('ECIs') and the assessment of the need to improve their protection. Directive 2008/114/EC [20] on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, from 8 December 2008, by the Member States and the Commission shall continue on an ongoing basis the process of identifying potential ECIs [11]. The cross-cutting criteria referred to all comprise the following: (a) casualties criterion (assessed in terms of the potential number of fatalities or injuries); (b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects); (c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services). The cross-cutting criteria thresholds shall be based on the severity of the impact of the disruption or destruction of a particular infrastructure. The precise thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the Member States concerned by a particular critical infrastructure. Each Member State shall inform the Commission on an annual basis of the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds.

2. Antiterrorism and Counterterrorism Strategy

Given the fact that terrorism is an expressed form of endangering the security of particular countries, regions, and even the international community, the importance of the prevention of terrorism arises. Antiterrorism includes all defensive and preventive measures taken to reduce the vulnerability of forces, individuals and property to terrorism. Such measures include protective and deterrent measures aimed at preventing an attack or reducing its effect(s) [3]. The prevention of terrorism implies an organized form of social prevention, criminal prophylaxis as the basic function of criminal policy. It is implemented through formal and informal forms of influences on etiological factors of delinquency, by suppressing the processes and phenomena that lie in its core. Combating terrorism implies the knowledge of criminal phenomena, political, economic, social causes and conditions which lead to them. It is implemented through the preventive activity of the authorities and social institutions, and is supported by political, social, economic, pedagogical and other measures aimed at eliminating the factors of delinquent occurrences, terrorism included. Modern terrorist sources and forms threatening to the practice and values of the state call for a high material-technological level of preparation of the state authorities, their efficient organization, a more developed area for the implementation of the results of natural and social sciences in the realization of their role and tasks as a professional service of the social system and its corresponding security system as a social subsystem. What is more, terrorist organizations today are equipped with cutting edge weapons and equipment, the fact that many scientists from different fields (biology, physics, etc.) work for them, that they are both materialistically and financially well secured, in some cases even better than the security services [1]. Protection against terrorism is the state's obligation as its basic function for securing the conditions for a peaceful and safe life of its citizens, free of violence and fear, democratic, tolerant, creative and prosperous, respectful to the order and the law. Any terrorist attack against Bosnia and Herzegovina would pose a serious and impermissible threat to its fundamental values and interests, since it involves a threat to the security and life of its citizens. Therefore, the priority of Bosnia and Herzegovina is the development of universal measures – national and international – preventions and protections against all forms of terrorist threats, which should be efficient enough to, aside from its immediate benefits, yield and strongly prevent any form of terrorist threat that could threaten Bosnia and Herzegovina[12] [14].

As an explicit security threat, terrorism has become an unavoidable subject of national security strategies, national strategies for the fight against terrorism and laws on national security, which make up an important framework in combating terrorism. The realization of these measures and the activities in the fight against terrorism involve the participation of all the subjects of national security, primarily national intelligence-security systems, the police, police-security formations, the military, etc. The reasons for this are multiple, primarily since terrorism in not seen and defined as a simple phenomenon, which was pointed out when we tried to define the term terrorism, especially international terrorism. Nevertheless, terrorist threats have forced countries over time to find a consensus and define the mechanism in the fight against violent terrorist acts within international frameworks. The largest scopes in this regard were accomplished within the public international law [15]. Such terrorism prevention entails unique engagement on both the homeland and international levels. The identification of trends as indicators of terrorist activities can help the policy creators in many areas, including (1) a priority against terrorism resources; (2) identifying terrorists and terrorist activities with the aim of preventing terrorist offences and (3) showing the fight against terrorism with positive outcomes [16].

Depending on terrorist strategies, the country will also take a stand on a "firmer" or a "softer" antiterrorist plan of action, and implement a reconciliation strategy (the making of special concessions to terrorists in exchange for the withdrawal or termination of terrorist activities), negotiation strategies (immediate or mediate negotiation with terrorist, which do not necessary imply concession) or incompliant strategies (dealing with the situation by denying the terrorists' demands or without any negotiation). The latter is known as the military-police antiterrorist strategy (depriving terrorists of their freedom and the release and protection of victims, mostly hostages by using adequate force means – the release strategy), while the retaliation strategy towards the terrorists is its variant deployed after the terrorists have committed an act of violence, and rarely "escaped justice" (the so called revenge strategy). Preventive strategies are primarily based on the intelligence activity, and rarely on the so called preventive wars. Generally, all these strategies can be classified into two ways of combating terrorism, subsequently antiterrorism[13] [2][17], which is a system of (defensive – preventive and repressive) measures, actions and procedures undertaken by the country with the aim of protecting persons and assets against terrorism on its territory, and counterterrorism, which entails the implementation of offensive measures with the aim of diverting, preventing and suppressing of modern terrorism outside its borders [18]. The term counterterrorism implies all offensive and defensive measures and actions whose carriers are the forces and subjects of the security system, and which are aimed at the complete neutralizing of the carriers and effects of a terrorist attack, in all its dimensions (organizational, functional, economic, psychological and other) [19].

3. Protection Measures

Protection measures include all offensive measures taken to neutralize terrorism before and after hostile acts are carried out. Such measures include those counterforce activities justified for the defence of individuals as well as containment measures implemented by military forces or civilian organizations [3]. The methods for counterterrorist actions are: propaganda; military response; Special Forces activities; police methods which include: territory control, blockades and searches and attacks on terrorists. References often mention offensive and defensive measures in the fight against terrorism. Defensive measures and actions are: propaganda, educational measures and actions, measures and actions of immediate protection. Offensive measures and actions include: combat actions, measures and activities of subduing and neutralizing of terrorists and terrorist groups. The main difference between these two sets of methods and counterterrorism actions is that defensive measures and actions are undertaken as preventive forms, prevention against terrorist actions, whereas defensive measures and actions are repressive in their nature and are deployed after a terrorist attack [20]. Preventive and repressive measures are, therefore, two ways of action which can, as complementary segments, give results in combating socially hazardous ways of behavior in our complex social, political and cultural surrounding. However, it needs to be mentioned that state repressive measures are less implemented and lose their social purpose and justification if the inner social strength is stronger and more united, homogenous and stable and if asocial and antisocial forms of behavior are regarded as an attack on the society in general, which will be able to deal with them and eliminate them due to its hegemony, compatibility in a safe and unique way with the help of modern and trained units for counterterrorism actions. In modern terms, terrorist activities are seen as an integral part of a single attack on the whole territory, rather than isolated actions on some facilities by the enemy. Regardless of the fact when terrorist attacks will commence (before, during or after the completion of war), it is safe to say that they will be synchronized with other events in the region, especially in terms of elections and distribution of action facilities. Most countries regard their special military forces as forces of strategic importance [21].

Surely, these preventive measures against terrorism which imply risk assessment from terrorist threats are important. In that context, it is necessary to mention the presence of the two-way connection between terrorist threats and the vulnerability of the system. Namely, one of the characteristics of identifying terrorist threats, considering the system, is the presence of the two-way connection between: (1) vulnerability of the system in regard to terrorist threats and (2) amount of anticipated damage if the threat is successfully realized. This characteristic can be further divided into several segments, given the fact that it supplies additional possibilities for reducing the risk of terrorism.

The formula for the assessment of risk from natural disasters or endangerment from other technical-technological accomplishments can be presented in the form of a simplified formula [22]:

$$\boldsymbol{R_C = P_{IV}\, x\, P_{(NU/IV)}\, x\, U_{(damage/IV\ \&\ NU)}}$$

Here, ***PIV*** represents a threat to the system, expressed as a probability of extreme attack initiations (the failure of specific elements, exceeding the permitted levels of risk factors, extreme natural phenomena and so on). $\boldsymbol{P}_{(NU/IV)}$ represents the vulnerability of the system in case of an initiated attack, expressed as a conditional probability of damage in case of an attack. $\boldsymbol{U}_{(damage/IV\ \&\ NU)}$ stands for the damage to the system in case of an attack. Therefore, for traditional and natural disasters, technical-technological phenomena, vulnerability determines specific threats, but the consequences depend on both types of threat and vulnerability of the system to these threats. It is important to mention that this method does not contain the two-way connection (because the probability of a spontaneous event is difficult to predict, so the system is unable to react to such threat) or dependence on the danger of consequences (for the same reason).

On the other hand, if a terrorist attack has been initiated, the interactions between different factors included in the equation for risk assessment are more complex. Similar to the equation above, the risk from terrorism is shown in the following equation [22]:

$$\boldsymbol{R_T = P_A\, x\, P_{(NU/A)}\, x\, U_{(damage/A\ \&\ NU)}}$$

$\boldsymbol{P}_A$ stands for a terrorist threat considering the system, shown as a probability that a specific form of terrorist attack will be realized.

$\boldsymbol{P}_{(NU\ /)}$ represents the vulnerability of the system from a terrorist attack depending on the type of terrorist attack, shown as a conditional probability of damage in case of an attack.

$\boldsymbol{U}_{(damage/\ \&\ NU)}$ represents the damage to the system in case an attack is realized.

In these situations the two-way connection between the terrorist attack and the vulnerability of the system takes place. In fact, reduction of the vulnerability of the system significantly reduces terrorist threats to persons and facilities.

The important fact here is that efficient counterterrorist actions directly influence the reduction of terrorist activity.

These strategic assumptions can be divided into several important stances:

- A unique approach and an established critical and value relation towards terrorism as a phenomenon is the first step towards the formulation of strategic assumptions.

- The building of a unique and consistent categorical and conceptual system of defining terrorism, which would enable the systematization of the activity and the actions for its elimination. It is important to have unequivocal definitions of terrorism, as a universal social phenomenon, terrorist actions, as a form of special destruction of the society and the state, and terrorist action, as an economic form of target-oriented violence through the use of weapons and other means for the destruction of people and material goods. It is only then that we will be able to define counterterrorism.
- Eliminating different problematic approaches to the content of counterterrorist action at the strategic level (state level). This would generate objective conditions for the systematization of authority, essential forms of action and activities, as well as time-defined contents according to dynamics. Thus, it would be possible to develop a strategy of national security and all system elements which would lead to its realization.
- A definite homeland normative-legal regulation, which is in accordance with the international legal provisions from the field.
- The implementation of affairs and specifying the jurisdiction of the authorities and special forces which are involved in counterterrorist actions.
- Unequivocal determination and establishment of factors essential for efficient counterterrorist activities. Their establishment in the spheres of basic and given factors would contribute to the explicit conception and formation of the spatial, structural and functional organization of the system for efficient actions. Experience shows that only such system can give final positive results in the fight against terrorism.
- The principles for counterterrorism actions determined by the strategic plan should be: determination, continuity, sufficiency and secrecy. Thus defined, they would secure the necessary notions for the successful preparation and execution of actions.

The creation of objective opportunities for the implementation of actions (preparation and execution of counterterrorist actions) is a necessary condition which implies full situational harmonization, and a positively oriented, operational and efficient environment. This should secure full information, a spatial, structural and functional organization, the capacity and moral segment of counterterrorist activities [19].

4. Challenges for Protection against Terrorism in BiH

Based on the analysis of the above relevant documents, in the spirit of global fight against terrorism, with the aim of making BiH, including the Republic of Srpska, even safer, allowing its citizens to live in freedom, safety and justice, respecting human rights, as well as global strategic aims [23] which can be adopted in our country, we cite the following perspectives and references for the protection against terrorism, which can be viewed as follows [17]: (1) Prevention of terrorism, (2) Protection against terrorism, (3) Detection and investigation of terrorist acts and (4) Response to terrorism.

The prevention of terrorism should include activities aimed at the identification of conditions and causes which lead to radicalization and enable the recruitment of potential terrorists[14] [24] in BiH with the aim of influencing these etiological factors in order to prevent further recruitment for terrorist purposes. Aside from that, special measures need to be undertaken in the area of training the authorities and other bodies for law enforcement, as well as in the sphere of education, culture, informing, the media and raising the public's awareness with the purpose of preventing terrorist attacks and their consequences. Likewise, measures for improvement and development of cooperation between the agencies for law enforcement in BiH are also necessary with the aim of preventing terrorist attacks and their negative consequences, *inter alia*: a) exchanging information, b) improving the physical protection of persons and their property and c) enhancing training and coordination plans for emergencies. Also, it is necessary to promote tolerance, dialogue in BiH, encourage interreligious and intercultural dialogue, including, when possible, NGOs and other elements of the society with the aim of lowering tensions which can lead to the increase in radicalization of specific ethnic groups. Furthermore, it is necessary to raise the public's awareness about the existence, causes, seriousness, as well as threats from terrorist attacks and to encourage the public to help the authorities and thus prevent terrorist attacks. Simultaneously, it is necessary to create conditions for combating terrorism through measures of social prevention, social, economic, crime policy, culture, informing and alike.

Protection against terrorism implies measures and actions used to protect the citizens and the infrastructure against terrorism, in order to decrease our vulnerability in case of terrorist attacks, including physical and technical protection measures, as well as enhancing the security of critical infrastructure. Of course, a strategic assessment of the risk from a terrorist threat is also necessary for Bosnia and Herzegovina, including the strategic analysis of a terrorist threat with the purpose of identifying the areas which are most susceptible to terrorist actions. A necessary condition for the exercise of strategic analyses in terms of terrorism as a social phenomenon or operational analyses regarding the execution of concrete terrorist offences is possessing relevant data bases. Today, these bases are computerized with software comparative analyses which are based on given terms or key words [25]. Protection of the citizens and critical infrastructure in BiH, aside from physical and technological protection of the citizens and critical infrastructure, protection of the traffic infrastructure, including highway, railway, air and waterway transport, should result in adopting guidelines and minimal standards for the purpose of protecting the citizens and critical infrastructure, as well as making publications and publications for protection against terrorism in critical zones (critical destinations).

The detection and investigation of terrorist acts implies measures and actions of penal prosecution of terrorists, including detection of planned terrorist acts, prevention of connecting terrorists into a terrorist network, cutting off financial support for terrorist acts, and detecting specific terrorist acts. Collecting information, the analysis and exchange of information on operational capacities of terrorist organizations (leaders, members, weapons, funds, communication, propaganda materials and other resources), as well as developing and improving of the system for data collection on terrorist acts is necessary. At the same time, it is necessary to develop and improve technical capacities for the monitoring and analyzing of open information sources related to terrorism activities, as well as mutual exchange of information between agencies for law enforcement within BiH, and agencies from other countries, including exchange of information with international organizations (Europol, Interpol, SELEC Center, etc.), and look into the possibilities for formation of joint research teams. The prevention of movement and activities of terrorists should be realized by undertaking criminal-tactical measures and actions, as well as actions of detection and special investigation activities according to the operational capacities of terrorist organizations. Equally, more effort should be put on hindering financing of terrorist acts by cutting off the terrorists' access to financial and other economic resources, developing criminal-intelligence capacities for the purpose of data collection on terrorist financing, overseeing the work and financing of the NGOs labeled as the sponsors of terrorist activities, developing methods for enhanced monitoring of financial flows of terrorists conducted through informal banking sectors or NGOs, etc. In particular, it is necessary to work on further prevention of access to weapons and explosives, and illicit trafficking in arms and explosives which can be misused for terrorist purposes.

Combating terrorism includes measures and actions directed at the preparation of managing and minimizing the consequences of terrorist attacks with the emphasis on the coordination of all subjects of the society on dealing with the consequences and helping the victims. Primarily, it is necessary to enhance all institutional capacities in BiH in order for them to be optimal and efficient in the fight against terrorism, but also the formation of special organizational units for the fight against all forms of terrorist activities. It is necessary to secure the expertise and constant specialization of judicial, prosecutorial and police personnel in the fight against terrorism, including their constant education and professional development in the fight against terrorism. Along with the strengthening of institutional capacities, there is also a need for the development and improvement of legislative capacities in the fight against terrorism. This implies monitoring and insisting on a complete ratification of international charters and conventions in defining a legislative response to terrorist threats, as well as taking into consideration necessary amendments of the existing legal provisions in the sense of the implementation of international agreements (first of all the resolutions and conventions of the UN and Council of Europe, as well as obligations prescribed by the Agreement on Stabilization and Association to the EU). Furthermore, more work needs to be put on the improvement of regulations which will be more efficient in the fight against terrorism, whereby there is a need for the Law on the fight against and financing terrorism as "lex specialis", which should include the protection, help and amends to the victims of terrorism attacks, special short investigation activities, witness protection, etc. Combating terrorism also implies the strengthening of civilian capacities in the fight against terrorism (healthcare, the media, school system, etc.), training and education for actions in cases of terrorist attacks, and dealing with the possible consequences of such attacks.

5. Conclusion

Not engaging in a detailed analysis of a multidisciplinary approach to the study of terrorism (sociological, political, security, etc.), terrorism is considered a criminal phenomenon with all its essential features: a terrorist act (as an individual phenomenon), terrorist (as a perpetrator of a terrorist act), a victim of terrorism (direct and indirect), terrorism as a mass phenomenon, and finally response (community and government) to terrorism. As such (criminal phenomenon) terrorism can be classified based on legal criteria (usually as a form of political crime), or based on motives (e.g. ideological, religious, etc.). In this context, it is necessary to examine the relationship of terrorism with other forms of crime, and especially organized crime and corruption. Finally, the reaction (of the society and the state) to terrorism can be viewed primarily in terms of criminal-law treatment of this issue and to answer the questions what constitutes terrorism offenses in terms of criminal law and how to react to such behavior. Protection of critical infrastructure is the key segment in the fight against terrorism. This segment is as important as intelligence protection, as well as criminal investigations.

Based on the research results, and their thorough analysis, the following can be concluded:

- Terrorism represents a clear threat to the security of state, and to international stability and prosperity more broadly and will remain a threat for the foreseeable future, and terrorists have demonstrated abilities of organizations and actions outside the borders of their states,
- Modern technology increases the potential impact of terrorist attacks employing conventional and unconventional means, particularly as terrorists seek to acquire chemical, biological, radiological or nuclear (CBRN) capabilities and cyber abilities. Critical infrastructure is particularly susceptible to terrorist attacks,
- Instability or conflict can create an environment conducive to the spread of terrorism, including by fostering extremist ideologies, intolerance and fundamentalism, which can have negative consequences on Bosnia and Herzegovina,
- It is necessary to find new and apply the existing standards for protection of critical structure against terrorism. In that sense, antiterrorist and counterterrorist actions become prominent, and their connection on the regional and international level, in order to respond to terrorism accordingly,
- It is necessary to develop all four segments of response to terrorism: prevention of terrorism, protection against terrorism, detection and investigation of terrorist activity, as well as a universal response to terrorism,
- It is necessary to use the resources of international organizations when it comes to combating terrorism. For example, NATO serves as a forum to develop non-binding guidelines and minimum standards as well as to exchange best practices and lessons learned for such eventualities to improve preparedness and national resilience. NATO has developed ‘Guidelines for first response to a CBRN incident’ and organises ‘International Courses for Trainers of First Responders to CBRN Incidents’ in six regional training centres. Providing timely information to the public is also a key component of consequence management, so NATO has developed guidelines to advise national authorities on warning the general public and alerting emergency responders.

If we compare the given conclusions with the hypothesis that terrorism poses a serious threat to the critical infrastructure in Bosnia and Herzegovina, and that it is necessary to develop modern measures of protection, it is clear that the hypothesis is confirmed.

Endnotes

[2] Emphasizing of fanatical extremism, as one of the most important elements of terrorism at the beginning of the XX century, points to the phenomenon of a new rebirth of nationalism and religious fanaticism. Compared to the XX century when terrorism was inspired by different ideologies and orientations (national-extreme, right, left and similar), the new millennium has brought major changes [4].

[3] For a number of former foreign citizens of Bosnia and Herzegovina, out of which some still reside in Bosnia and Herzegovina, earlier findings show that they pose a threat to the national security and as such have been deprived of the BiH citizenship so they are in the process of being deported.

[4] There are findings which show that there are several websites in Bosnia and Herzegovina whose contents encourage or invite to intolerance and even hatred. These are mostly sites which are not registered in Bosnia and Herzegovina, but mainly in European countries (Austria, Germany, Norway and other). It is regarded that the free distribution of such contents via the Internet, which openly invite to violence and retaliation significantly stimulate and motivate the users of such contents to manifest intolerance and hatred and contribute to the spreading of a negative atmosphere and insecure the overall situation in Bosnia and Herzegovina. Among other, these sites are used by individuals to show a verbal support to some global terrorist organizations and movements through showing of particular video contents which are sponsored by Al-Qaeda. Some of the video contents openly invite to violence and retaliation against coalition forces in Iraq and Afghanistan. What is some more, the Internet is also used to incite national intolerance, discord, and intimidation of other ethnic and religious groups. The Internet, as a true virtual training camp, is taking over the role that the Al-Qaeda camps used to have in Afghanistan and Pakistan. More and more young people create their own websites and advocate the formation of autonomous extreme cells, the making of explosive devices from substances that are freely purchased and organize individual terrorist attacks (e.g. the Bektašević case and other) [5].

[5] In 2009 the Prosecutor's Office of BiH charged five persons with complicity between November 2007 and November 2009, as an organized group which acted on the territory of Bosnia and Herzegovina, for a terrorist attack on one of common identified objects, i.e. specified targets with the aim of seriously intimidating the population and causing serious destabilization to basic constitutional, political, economic and social structures. The processing of this group in the BiH Court is an ongoing activity. In August 2006 an explosive device was planted in Sarajevo under the grave of the former president of Bosnia and Herzegovina, Alija Izetbegović. The act was considered a terrorist attack. The gathered information so far shows that this act might have had some political, national or religious background or all of them combined. The perpetrator or perpetrators of this act are not yet familiar [5]. In March 2008 a group of people was arrested (who were in custody at that moment) led by R.R. from Sarajevo, in whose quarters, as well as in the quarters of his contacts, in Sarajevo and Bugojno the BiH authorities found and confiscated a considerable amount of weapons and mine-explosive devices during the search. They are being held in custody at the BiH Court. In a shopping mall Fis Vitez, on 9 October 2008 an explosive device was planted and went off resulting in one person's death, one person was seriously injured and several slightly injured. Three persons were charged for this act, one person was suspected of a criminal act of terrorism according to Article 201 of the Criminal Code of Bosnia and Herzegovina and directly linked to the offence at FIS Vitez. The second person was accused of a criminal act of terrorism for the production and possession of explosive devices which can be linked to terrorist activities and suspicion of a possible terrorist act, while the third person was accused of a criminal act of terrorism. The trial, which will give an epilogue to this criminal offence, is an ongoing process [5].

[6] The first instance verdict of the BiH Court found Mirsad Bektašević guilty of a terrorism offence (Article 1, Paragraph 1, in accordance with the Paragraph 4, Item f) of the CC BiH, and was sentenced to imprisonment for a term of 15 years and 4 months. On 21 May 2007 the Appellate Panel to the Court reached a final ruling which partially took into consideration the appeals of the Defense Counsel, so the verdict was changed into the imprisonment for a term of 8 years and 4 months for the accused Mirsad Bektašević. Also, on 20 November 2013 the Appellate Panel to the BiH Court found the accused Mevlid Jašarević guilty of a terrorism offence (Article 201, Paragraph 1 in accordance with Paragraph 5, Item a) and sentenced him to imprisonment for a term of 15 years. The accused Mevlid Jašarević was found guilty because he was as a member of the so called Vehabia community in Gornja Maoča, municipality Srebrenik, in which, with the aim of, through his actions towards the institutions and the authorities in Bosnia and Herzegovina, and the institutions and the authorities of other countries with embassies in Bosnia and Herzegovina, by expressing dissatisfaction with the status of that community and similar brotherhoods and Muslims in the country, Europe and the world, and thus influencing the change of the status of the same, and extorting concessions from the authorities demanding from the NATO forces to leave Afghanistan, threatening USA and German citizens, intimidating people, preparing and executing actions which are regarded as criminal according to the Criminal Code of Bosnia and Herzegovina, decided to, taking into consideration the aforementioned, execute a terrorist attack. On 28 October 2011 at 4.30 pm the accused Jašarević executed a terrorist attack on the American Embassy by firing 105 bullets from an

automatic rifle caliber 7.62 mm for around 50 minutes at the Embassy and also at the officers of the Directorate for Coordination of Police Bodies (DCPB) in charge of securing the USA Embassy, during which an DCPB officer got shot in both legs, causing severe injuries. The accused was also threatening the USA Embassy's employees until he was contained and apprehended by the members of a SWAT team with the MoI of the Canton Sarajevo. In the same manner, the BiH Court after the main search on 20 December 2013 reached a first instance verdict which found the accused Haris **Čaušević** guilty of a terrorist offence. In that regard, the Court sentenced the accused Haris **Čaušević** to imprisonment for a term of 45 years. The accused Haris **Čaušević** was found guilty because during 2010 he met on numerous occasions with to him known persons in Bugojno and contemplated a terrorist attack on 27 June 2010 in the early morning hours by planting a prepared an improvised explosive device on the back wall of the building of Bugojno Police Department (Bugojno PD) and by activating it – lighting a lighter of a slowly burning cords thus causing an explosion. During the explosion one police officer was killed, another one got severe life-threatening injuries, and several officers were slightly injured. The explosion also caused severe damage to the Bugojno PD and the surrounding block of flats, office buildings and a large number of vehicles. By executing such an act the accused Haris **Čaušević** wanted to force the BiH authorities to do something, as well as to seriously intimidate the population and destabilize basic political, constitutional and social structures in BiH. See more: *Presuda Suda BiH*, broj X-K-06/190, od 10.01.2007. Sud BiH, Sarajevo, 2007.; *Presuda Suda BiH*, broj X-KŽ-06/190 od 21.05.2007, Sud BiH, Sarajevo, 2007.; *Krivični predmet Suda BiH*, broj S1 2 K 007723 13 KŽK – Melvid Jašarević i dr, Sud BiH, Sarajevo, 2013.; *Krivični predmet Suda BiH* broj S1 2 K 002596 10 K - **Čaušević** Haris i dr, Sud BiH, Sarajevo, 2013.

[7] Namely, The United States had the strongest military and the largest economy; these two factors were both reinforcing and dependent on each other. The meteoric increase in cyber communications linked the infrastructures that were vital to the defense and economy of the United States. In 1996, President Clinton formed a commission to study the vulnerabilities of the infrastructures critical to the United States. The commission was formed with representatives from within the government as well as several from outside the government, as many infrastructures are owned and operated by the private sector. The critical infrastructures reviewed included telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply, emergency services. The threats were broken into two categories, physical threat (damage to the tangible property) and threat to the electronic/computer-based systems (cyber attack). While the committee researched the vulnerabilities to the United States' infrastructures, the Infrastructure Protection Task Force (IPTF) was formed within the Department of Justice, chaired by the FBI. The initial charter of the IPTF was to: 1. Provide expert guidance to critical infrastructures to detect, prevent, halt or confine an attack and to restore service; 2. Issue threat and warning notices; 3. Provide training and education on methods of reducing vulnerabilities and responding to attacks; 4. Coordinate with law enforcement during/after an attack to facilitate any investigation [8]. See more: G. Sikich, *Critical Infrastructure Vulnerability: An Overview Of The Report To The President From The Commission On Critical Infrastructure Protection*, Center for Crisis Management Studies, Highland, 2008.

[8] It is important to mention that most definitions of critical infrastructure have an institutional character. Theafore, The USA Patriot Act defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". The European Union definition of critical infrastructure is: 'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions; European critical infrastructure or 'ECI' means critical infrastructure located in Member States, the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure. In Australia critical infrastructure is defined as: "those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security". See more: *The USA Patriot Act* (Public Law No.107-56, Section 1016(e)) Available.http://www.whitehouse.gov/homeland/book/sect3-3.pdf. Accessed 18 March 2014; COM (2006) 786.; Council Directive 2008/114/EC of 8 December 2008.; *National Guidelines For Protecting Critical Infrastructure From Terrorism*. Commonwealth of Australia, National Counter-Terrorism Committee, 2011.

[9] Same Communication, The European Council of June 2004 asked the Commission and the High Representative to prepare an overall strategy to protect critical infrastructure.

[10] Europe's critical infrastructures are highly connected and highly interdependent. Corporate consolidation, industry rationalization, efficient business practices such as just-in-time manufacturing and

population concentration in urban areas have all contributed to this situation. Europe's critical infrastructures have become more dependent on common information technologies, including the internet and space-based radio-navigation and communication. Problems can cascade through these interdependent infrastructures, causing unexpected and increasingly more serious failures of essential services. Interconnectedness and interdependence make these infrastructures more vulnerable to disruption or destruction [11].

[11] Member States must go through a process of identifying potential ECIs, with the help of the Commission if required. Member States should make use of a series of criteria to identify these potential ECIs. The cross-cutting criteria take into account possible casualties and economic and public effects, while the sector criteria consider the specificities of each ECI sector. This directive currently concerns only the energy and transport sectors and their subsectors. This Directive constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, *inter alia*, the information and communication technology ('ICT') sector [13].

[12] Bosnia and Herzegovina recognized the potential dangers and this is why it emphasizes in the Security policy document from 2006 the readiness for the fight against terrorism in the form of the following regulations: "Within the realization of inner policy the subjects of the security system of Bosnia and Herzegovina will direct their actions on the fight against terrorism, organized crime and corruption – by strengthening the control mechanism of control discipline. Combating terrorism will be a factor of cooperation of all subjects, and the cooperation in the fight against terrorism functionally and institutionally developed in accordance with constitutional legal solutions and implementation of adopted international relations" [14]

[13] There are different interpretations of the term "antiterrorism" in references. According to Radoslav Gaćinović, "Antiterrorism is a set of measures, actions and procedures executed by the United Nations and state institutions on its territory with the aim of timely identifying and eradicating modern terrorism, by implementing the strategies of deterrence and fighting back [2]. This is a very complex process which demands a preventive, repressive and combat action of the state security structures accompanied by the implementation of the international legal acts adopted by the United Nations.

[14] According to the Article 6 of the Council of Europe Convention on the Prevention of Terrorism from 2005, "recruitment for terrorism" means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group. See more: CETS No.: 196.

References

[1] M. Šikman, *Terorizam*. Fakultet za bezbjednost i zaštitu, Banja Luka, 2009.

[2] R. Gaćinović, *Terorizam u politčkoj i pravnoj teoriji*, Medija centar Odbrana, Beograd, 2011.

[3] *Nato Glossary Of Terms And Definitions* (English And French), North Atlantic Treaty Organization, 2008.

[4] S. Mijalković & M. Bajagić, *Organizovani kriminal i terorizam*, Kriminalističko-policijska akademija, Beograd, 2012.

[5] Strategija Bosne i Hercegovine za prevenciju i borbu protiv terorizma (za period 2010-2013. godina, Ministarstvo bezbjednosti BiH, Sarajevo, 2010.

[6] R. Milašinović, & S. Mijalković, Terorizam kao savremena bezbednosna pretnja. In: M. Šikman, & G. Amidžić, (Eds), *Suprotstavljanje terorizmu – međunarodni standardi i pravna regulative,* Visoka škola unutrašnjih poslova, Banja Luka, 2011.

[7] COM (2005) 576.

[8] *DCSINT Handbook No. 1.02, Critical Infrastructure Threats and Terrorism,* U.S. Army Training and Doctrine Command, Fort Eustis, VA: Public Affairs, 2006.

[9] G. Sikich, *Critical Infrastructure Vulnerability: An Overview Of The Report To The President From The Commission On Critical Infrastructure Protection*, Center for Crisis Management Studies, Highland, 2008.

[10] *The USA Patriot Act* (Public Law No.107-56, Section 1016(e)) Available.http://www.whitehouse.gov/homeland/book/sect3-3.pdf. Accessed 18 March 2014; COM (2006) 786.; Council Directive 2008/114/EC of 8 December 2008.; *National Guidelines For Protecting Critical Infrastructure From Terrorism*. Commonwealth of Australia, National Counter-Terrorism Committee, 2011.

[11] COM (2004) 702.

[12] COM (2006) 786.

[13] Council Directive 2008/114/EC of 8 December 2008.

[14] *Sigurnosna politika Bosne i Hercegovine*, Predsjedništvo Bosne i Hercegovine, Sarajevo, 2006

[15] M. Bajagić, *Osnovi bezbednosti,* Kriminalističko-policijska akademija, Beograd, 2007.

[16] R. Perl, *Combating Terrorism: The Challenge of Measuring Effectiveness*, Congressional Research Service, Washington, 2007. COM (2004) 702.

[17] M. Šikman, Zaštita od terorizma u BiH – stanje i perspektive. In M. Talijan, D. Jovičić, M. Daničić, (Eds), *Bezbjednost i zaštita u Republici Srpskoj i Bosni i Hercegovini – stanje i perspektive*, Fakultet za bezbjednost i zaštitu, Banja Luka, 2008.

[18] M. Kotovchevski, Bozinovska, S. *English-Macedonian Dictionary of Intelligence Terminology*, Faculty of Philosophy Studies, Skopje , 2007.

[19] M. Mijalkovski, *Terorizam i protvteroristička borba*, Vojna akademija, Beograd, 2003.

[20] U. Pena, & G. Amidžić, *Policijske operacije*, Visoka škola unutrašnjih poslova, Banja Luka, 2007.

[21] R. Ilić, Odbrana od terorizma, *Vojno delo, br. 2/2007,* (2007*),* 111.

[22] G.E. Schweitzer, *Countering Terrorism: Biological Agents, Transportation Networks, and Energy Systems, Summary of a U.S.-Russian Workshop*, The National Academies Press, Washington DC, 2009.

[23] The Bucharest Plan Of Action For Combating Terrorism, OSCE, MC(9).DEC/1 4 December 2001; The European Union Counter-Terrorism Strategy (14469/05 LIMITE JAI 423 ECOFIN 353 TRANS 234 RELEX 639 ECO 136 PESC 1010 COTER 72 COSDP 810 PROCIV 174 ENER 172 ATO 103), Council Of The European Union, Brussels, 15 November 2005; Implementation of the Action Plan to combat terrorism (9809/1/05 REV 1 LIMITE JAI 208 ECOFIN 187 TRANS 114 RELEX 293 ECO 71 PESC 481 COTER 35 COSDP 371 PROCIV 82 ENER 91 ATO 60), Council Of The European Union, Brussels, 15 10 June 2005.

[24] Council of Europe Convention on the Prevention of Terrorism, No.: 196., Article 6, 2005.

[25] B. Simonović, *Kriminalistika*, Pravni Fakultet, Kragujevac, 2004.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-267

Challenges in Defining Critical Infrastructure in Montenegro

Milan BIGOVIĆ [a,1], Ana RAKOČEVIĆ [b]
[a] *Ministry of Defense of Montenegro*
[b] *Ministry for Information Society and Telecommunications of Montenegro*

Abstract. Many theoretical analyses today commonly define critical infrastructure as a set of physical and virtual systems and resources that allow society's smooth and stable functioning, and the destruction or damage of that which would endanger the stability or even the security of modern society or the state. The aim of this article is to define the importance of national critical infrastructure from the standpoint of safety, as well as to show some elements of critical infrastructure in Montenegro. This article analyzes the phenomena and processes that have in recent years contributed to the protection of critical infrastructure, threats to critical infrastructure of Montenegro from cyber space, the importance of defining critical infrastructure from the standpoint of the defense system, as well as the importance of the private sector to protect critical infrastructure. Given that Montenegro has not yet defined the critical infrastructure at the national level, the article gives suggestions of steps that need to be implemented in order to define the critical infrastructure in Montenegro.

Keywords. critical infrastructure, Montenegro, cyber threats, cyber space, protection of critical infrastructure, defense system

Introduction

Major changes in the international environment in the political, security, defense, social and environmental fields and globalization in the 21st century have brought on new opportunities and challenges in the field of security. All of this requires the responsibility of a national security policy and national security system to establish an effective response to a changing security environment. Modern threats are complex, interconnected and transnational and they require an immediate response in order to avoid the domino effect. Today we are faced with threats to the physical and virtual worlds, which are quite real, dangerous and can have potentially deadly consequences. Threats of one country or nation pose a potential threat to others. Identifying threats and timely responses to them becomes an increasingly important factor of safety management. Security threats such as terrorism, IT, environmental, economic, crime, medical, military and other threats in terms of research and practice are important because of their potentially lethal effect on humans and basic social infrastructure [1].

Globalization, in terms of rapid development and expansion of information technologies is a contemporary reality of international relations which rapidly changes the international security environment. The boundaries are not so hard line and on the national level it is much more difficult to control the flow of goods, people, and

[1] Corresponding Author: MSc. Milan Bigović, Ministry of Defense of Montenegro, e-mail: milan.bigovic@mod.gov.me

information, which implies that the traditional concept of security is no longer a key instrument in addressing security issues. While a traditional approach to security points out military threats as the greatest danger to society and a country, nowadays safety challenges and risks come from a completely new field - informatics. The concept of national security is redefined and the military, intelligence and business operations of the international community depend on cyber security.

Constant and rapid changes in international relations, the increase of security challenges of risks and threats, as well as security deficit reflect that the global security picture becomes complex while critical infrastructure gets new dimensions and the increasing importance on the national and international level. As the critical infrastructure has become an important segment of national security, the protection of critical infrastructure began to be developed and today it is one of the main priorities of each country.

The development of information technology influences major changes on the field of protection. To recover from the consequences in new circumstances, new elements of answers are required, as well as a new system of protection. Although (with small differences between different countries) it is defined what is meant by the elements of critical infrastructure (networks of electricity, oil, gas, transportation infrastructure, water supply, food supply, health, banking and financial systems, communication etc.), it is obvious that all these elements are highly dependent on information technologies. In this regard, weaknesses in the information systems occur, which can damage and endanger the safety of critical parts of the infrastructure. Information security, infrastructure systems and networks pose serious challenges for the people who manage them [2].

It is of great importance for Montenegro, as well as for any other developed society, that the supplying of energy goods, food, reproduction materials, medical supplies and all other goods are carried out regularly, for economic and other reasons. Any interruption in the supplying of goods and services (due to natural disasters, technological disasters, chemical, biological, nuclear and radiological contamination, cyber-attacks, the consequences of terrorism, etc.) could cause serious circumstances on the maintenance of key social functions. Therefore in order to protect and save human life (as primary protection) the protection of critical infrastructure needs to be the center of attention.

Due to the above mentioned, the defining and protection of critical infrastructure in Montenegro is a very complex process which demands the engagement of a large number of state bodies at all levels and needs to be continuosly improved and adjusted based on the contemporary challanges and threats.

This article presents some guidelines in the process of the defining and protection of critical infrastructure in Montenegro, based on its own experience, experience of the EU and the USA, as well as based on the experience of the regional coutries. The article provides different definitions of critical infrastucture, which Montenegro can use while making its own definitions. It also analyzes the current state in Montenegro, especially in cyber space, defense systems and the private sector. The significance of mutual dependence of critical infrastructure of different sectors, specific regions or specific coutries is stated as an important segment of critical infrastructure difinition. At the end, analysis of the risk assessment from different threats, the current state of Montenegro, and international and regional experience, pointed to the necessity of defining which steps should be taken in order to define critical infrastructure in Montenegro.

1. The definition of critical infrastructure

Critical infrastructure is a sensitive area because of its role in society and the processes that take place in it. The critical infrastructure is a term that has several definitions depending on the environment in which it is located, but it can be concluded that the current understanding of critical infrastructure includes all facilities and systems, the inactivity or limited use of which causes a social crisis or even a security risk. It includes a wide range of infrastructure, such as transport, energy, oil, gas, health, nuclear, food, water supply, information, and related infrastructure [3].

Defining a framework of critical infrastructure in many countries and organizations may differ. Below are some definitions:

USA: “Critical infrastructure and basic resources (Critical Infrastructure and key resources - CIKR) is a term that refers to a wide range of different resources and assets that are necessary for the daily functioning of the social, economic, political and cultural systems in the United States. Any interruption in the elements of critical infrastructure poses a serious threat to the proper functioning of these systems and can lead to property damage, casualties and significant economic losses” [4].

AUSTRALIA: “Critical infrastructure is/represents those physical facilities, supply chains, information technologies and communication networks, that if you destroy or incapacitate in a long time, could significantly affect the social or economic well-being of the nation, or would affect the state’s ability to maintain national defense and ensure national security” [5].

EUROPEAN UNION: “Critical infrastructure is a property, system or its part, located on the territory of the Member States and which is necessary for the maintenance of key social functions, health, safety, security, economic or social well-being, and whose disruption or destruction would have a significant impact in the member states” [6].

FINLAND: Critical infrastructure includes and represents technology infrastructure, transport, logistics and distribution systems, systems for food supply, energy networks, systems of social and health services, economic systems, and systems related to national defense [7].

NATO: Critical infrastructure consists of those assets, facilities, networks and services, whose malfunction or destruction would seriously affect the health, safety, economic conditions, social protection and the functioning of the state [7].

In order to define critical infrastructure, a system of institutions which will take accountability and authority in this area is required. Of course, strategic commitment in this area is needed, due to the entry in new integration and the new technological developments that have vastly changed the social conditions of business, and all because of the maintenance and strengthening of the existing infrastructure. We must take into account that technological development has changed the way of doing business, management and the implementation of policies and the perceptions of national and public security. Also, technology has become cheaper, more sophisticated and more accessible, which makes it a potentially dangerous instrument that is difficult to control. For this reason it is necessary to create conditions for reducing the risk of negative actions and consequences on critical infrastructure. Disorders in a continuous operation of institutions and critical infrastructure can have extremely detrimental effect on the defense and economic security of the country as a result [8].

Based on the above mentioned, this means that the types of critical infrastructure vary from state to state and it depends on the attitudes of those who decide what critical infrastructure is and on the structural level of authority, but in the protection of critical infrastructure, there is a need for a comprehensive approach. This means that all institutions in Montenegro must recognize and protect their critical infrastructure to avoid system failure, because different critical infrastructures are interconnected and dependent on each other.

2. Good practice of the protection of critical infrastructure in the European Union

Activities related to the protection of critical infrastructure in the European Union started ten years ago. The Council of Europe invited the European Commission to prepare a comprehensive strategy to protect critical infrastructure. In October 2004, the Commission adopted Communication on Critical Infrastructure Protection (CIP).

Also, in addition to the Strategy, the European Program for Critical Infrastructure Protection and Internal Protection Strategy to Protect the European Union was adopted.

An integral part of the program is the European Council Directive on the assessment and designation of the European critical infrastructure and the assessment of the need to improve its protection. The Annex to Directive states is that each Member State must carry out the process to determine critical infrastructure through steps that are clearly defined in the Directive.

When it comes to creating policies for the protection of critical infrastructure, EU member states are facing new and numerous challenges. According to the report of the European Policy Centre, many countries such as the UK, Sweden, Switzerland, the Netherlands, Germany, France and Italy have made significant progress in this respect, while other states are trying to speed up the process of undertaking measures to address the key challenges of critical infrastructure. However, despite the adopted Directive and procedures, problems persist because elements of infrastructure are interconnected, so the failure of one element may cause failure of the entire system.

The incidents that occurred in the previous period such as terrorist attacks on 9/11, the bombing of the Madrid subway, electricity cuts in North America, cyber-attacks in Estonia in 2007, etc., have highlighted the necessity for creating an internationally coordinated policy for the protection of critical infrastructure.

The area of information, communication technology, and information-communication technology has been recognized as one of the important elements of critical national infrastructure. The European Agency for Network and Information Security Agency (ENISA) was established to prevent the endangerment of information security, cyber-crime and cyber terrorism for the Member States of the European Union. ENISA provides guidance to encourage cooperation between the public and private sectors and advises and assists the European Commission and all Member States in the field of information security. The Agency also attempts to solve the security problems, collects and processes statistical data on security incidents in the European Union, encourages development of strategies for the incidents, and raises awareness of the necessity of cooperation between all actors in the field of information security, starting from the ordinary citizen and the local communities to the state and the Union. It is important to point out that Member States of the European Union continue to develop and maintain bases of significant critical infrastructure on a national level and are responsible for the development and business operating continuity in the event of an attack under their national jurisdictions [9].

An analysis of the legal framework of the European Union, which defines critical infrastructure, is of great importance for defining critical infrastructure in Montenegro, given that Montenegro wants to be member of the European Union.

3. Critical Infrastructure in Montenegro

3.1. The current level of protection of critical infrastructure from cyber threats

The system of critical infrastructure protection is a very complex process which is still under development in Montenegro. Adequate protection and prevention of cyber dangers cannot be achieved by using technologies and services. It has to be paired with a quality and applicable framework in order to successfully monitor the dynamic nature of information-communication environment and cyber strategies.

Web portals of state authorities and private organizations in Montenegro have often been targets of cyber-attacks, but fortunately major damage was not caused.

In this regard, it is necessary to define critical infrastructure in Montenegro as soon as possible and to develop procedures for protection in order to ensure its undisturbed operation.

The National Security Strategy of Montenegro states that "by increased use of information technology, Montenegro has become endangered in the area of IT security, whose function may be limited or completely paralyzed in the event of cyber-crime" [10]. The Defense Strategy of Montenegro states that "Today's security challenges in the world come from different sources. They are mainly a result of social, cultural, religious, economic, scientific and technological differences. From the spectrum of current security challenges, those that particularly stand out are as follows: international terrorism; proliferation of weapons of mass destruction; unresolved border issues; religious and ethnic disputes; organized crime; natural and man-made disasters; economic and social problems and computer crime." The Strategy also emphasizes that "these threats have a transnational character, no single country has the ability to resist them on its own, but this requires a coordinated global response" [11].

In Montenegro, cyber security is most often associated with cyber-crime. Accordingly, the Criminal Code of Montenegro prescribes that cyber-crime involves damage to computer data and programs, computer sabotage, creation and the insertion of computer viruses, computer fraud, unauthorized access to a protected computer, computer network and electronic data processing, preventing and limiting access to a public computer network, and the unauthorized use of a computer or computer network.

The building of a legislative framework of cyber security requires the adoption of new and the improvement of existing legislation in the field of cyber security. Accordingly, Montenegro has signed the Council of Europe Convention on Cybercrime in Budapest and the Additional Protocol to the Convention. After the ratification, Montenegro harmonized criminal legislation according to the provisions of the Convention, as well as with the Council Framework Decision 2005/222/JHA on attacks against information systems [12].

There is an institutional framework for cyber security within the Ministry for Information Society and Telecommunications which established the National Computer

Incident Response Team (CIRT), which is, among other things, responsible for responding to emergency situations in the case of unauthorized intrusion on a protected database [12]. Also, in the Ministry of Interior Affairs – Police Administration, there is a group for the fight against organized economic crime with a separate division for computer crime.

The strategic framework in this area is defined by the Strategy for the Cyber Security of Montenegro which, among other things, defines key steps in the strengthening of capacity building and training for an effective fight of repressive bodies against computer crime. Manners and terms of implementation of objectives defined by the strategy are clearly defined in the Action Plan. The implementation of key activities, envisaged by the Action Plan for the current year include defining the methodology of identifying critical information infrastructure with a purpose to define critical elements of critical infrastructure, then the establishment of the National council of cyber security, the establishment of local CIRT in public institutions, etc. The development of methodology has already begun and should be implemented as of the second quarter [13].

Regarding the establishment of international cooperation, the umbrella organization (CIRT) in the field of cyber security in Montenegro has carried out activities and established partnerships with key international institutions in the field of cyber security.

The development and implementation of training programs for various target groups and the improvement of education system for cyber security in Montenegro are realized through the TEMPUS project ECESM (enhancement of the cyber educational system of Montenegro). The project, which is in the initial stage of implementation, will help to ensure that the digital Montenegrin nation is able to improve national economic prosperity and security in the 21st century through innovative education on cyber security at different levels, ranging from promotion to specialized training for a Master's degree. The main objective of the project, in accordance with the recommendations of the European Commission expressed during the negotiation process, is to improve, develop and implement standards, guidelines and procedures at the national level of the system in Montenegro, in order to enable development of highly trained personnel capable of responding to the dynamic and rapid development of electronic threats.

On the basis of the above-mentioned, one may conclude that the types of critical infrastructure vary widely from state to state and depend on the attitudes of those who decide what is critical infrastructure of structural authority levels, but in the area of critical infrastructure, there is a necessity for a comprehensive approach. This means that all bodies of the state must recognize and protect their critical infrastructure in order to avoid system failure, because various critical infrastructures are interconnected and dependent on each other.

Furthermore, Montenegro issued the Strategy for prevention of and the fight against terrorism, money laundry, and financing of terrorism for the period of 2010 to 2014 in order to develop more efficient and functional mechanisms of state institutions and to improve protection procedures against terrorism (including cyber terrorism). In order to implement the Strategy, an interagency working group has been formed, and one of its core priorities is the definition of critical infrastructure based on potential terrorist threats (including cyber threats) on the national level. There is no doubt that the development of such a group will contribute to the better overall defining of critical infrastructure on the national level.

3.2. Critical infrastructure and defense system of Montenegro

Present-day challenges to security are so complex that Montenegro cannot base its defense solely on its own resources. The concept of defense strategy is based exclusively on constructing an integrated defense system which can be subjected to future alterations and inclusion in international security and defense integrations. This is the most favorable manner of managing available defense resources [11].

Protection of vulnerable systems, such as infrastructure for a national crisis, represents a major segment in defense. The basis for successfully reacting to future threats in cyber space lies in perceiving its sophisticated nature and substance. It is also very important to establish ground rules in planning national cyber security in accordance with national strategy. The microcomputer revolution vastly changed the world and thus it changed the manner of conducting the conflicts [14].

In the era of the expansion of internet technology, social networks and computer software, the fact that all IT systems can be used against a population, and consequently pose a serious threat to security, cannot be ignored. This broad range of risks demands amendments and the constant adaptations of defense systems, which will enable the development of skills [15].

For the development of a defense system of Montenegro, a realistic and objective assessment of risks and threats is of utmost importance. Nowadays the role of the defense system is significantly different when compared to traditional perception of defense, considering the broad range of security risks and threats, which are by nature difficult to predict, asymmetrical and unconventional.

In present time security threats are less aimed to territories of the state and military facilities, but more at national infrastructure (embassies, airports, energy-producing stations, railways, etc.), civilians (mass meetings, stadiums, etc.) and provoking political and economic crises. The response to these threats requires actions by the whole community and a stronger cooperation of states in the field of critical infrastructure protection.

By taking into account contemporary challenges, risks and threats, the issue of critical infrastructure in Montenegro could be recognized in the area of defense, which represents a new step in its protection. Particularly, the Government of Montenegro has defined the infrastructure of special importance for defense as follows: robust technical systems of special importance for defense, built command posts, electronic communication centers, radio relay nodes, radar and electronic centers, fortification infrastructure, airports, heliports and harbors (bases), experiment areas and laboratories, warehouses for armament, ammunition, assassination means, fuel and military equipment, special rooms for the safe keeping of the Defense Plan of Montenegro, military archives and the server for the military computer network and operation centers, plans for organization, development, equipping, modernization, and deployment of the Armed Forces of Montenegro, crypto devices, and codes [16].

Robust technical systems of special importance for defense are defined as a complex or assembly of mutually arranged parts and procedures which provide technical and technological unity and system independence or its functional connectivity with other technical systems which are important for defense. According to the decision of the Government of Montenegro, the following robust technical systems have been defined in the area of: telecommunication, informatics, traffic, electro energetic, water supply and other areas important for defense [17].

Security of infrastructure of special importance for defense includes the organization and realization of measures for their protection against damage or destruction, or disclosure of confidential information regarding infrastructure or location. Legal documents define the procedures for the application of security measures during protection of the infrastructure of special importance for defense.

Considering the current defense state, we might say that Montenegro is determined to use all available resources in a rational way, and to integrate them whenever it is reasonable and possible in order to contribute to the more efficient development and functioning of the defense system.

1.1. Critical infrastructure and private sectors

Since a substantial part of the computer infrastructure is owned by the private sector, it is very important to establish a shared strategic frame which will secure the protection of critical infrastructure and ensure its safety, because the government cannot provide complete safety.

Thus it is essential to enable defense mechanisms to advance alongside one another, so we expect to have better chances to effectively defend and protect a system which is of crucial importance for the functioning and wellbeing of a social structure through reinforced government-private partnership.

It is noted that in Montenegro a great number of systems that can be considered as critical infrastructure is in private property or the property of private companies. This is primarily in the telecommunication and energy sectors. Following the tendencies, it is possible that a portion of transport systems in Montenegro will be deregulated so it is necessary to improve legal frames and cooperation.

The Montenegrin national CIRT is at the moment appointed as administrator for matters of cyber security. In March 2014 the government proposed establishing local CIRT in public offices which may be critical parts of information infrastructure. The signing of a contract of collaboration with the private sector is planned in days to come. This will lead to forming a network of companies which effectively coordinates its activities and resolves possible incidents. In the IT world, timely inflow of information is of utmost importance and this problem should be solved by the previously mentioned network.

On the other hand, a new law on the protection of persons and property is defining that infrastructure of strategic importance for Montenegro or infrastructure which represents significant danger for the lives and health of people must be physically and technically protected. The following infrastructure is considered to have mandatory protection:

- For production, processing, distribution and storage of petroleum, petroleum products and gas;
- For production, processing, distribution and storage of water;
- For food production;
- For production, transportation, and distribution of electricity;
- Facilities for production, usage or storage of radioactive and other dangerous and harmful substances;
- Facilities of importance for all kinds of traffic;
- Facilities with goods pervious to damage or destruction which can cause serious consequences for the health and lives of people;

- Facilities which contain goods of extreme importance for science, culture and arts;
- Financial facilities;
- Post offices and telecommunication facilities [18].

This draft of law defines that protection of infrastructure that requires mandatory protection is conducted based on a protection plan which has to be approved by the competent ministry.

Following the analysis of the mentioned infrastructure it could be concluded that they belong to the group of critical infrastructure which is already defined by most countries, so that adoption of this law, as well as the proposition to form local CIRT in public institutions which may be the part of critical informatics infrastructure, represents a huge step on the road towards the defining and protection of critical infrastructure in Montenegro.

4. Conclusion

Defining of the framework of the national critical infrastructure is a complex task comprised of human resources, facilities and their interconnections. Raising awareness on the necessity to define critical infrastructure in Montenegro and manners of its protection should be part of the national policy.

The concept of critical infrastructure in Montenegro is mentioned only in the Strategy of Cyber Security which only states that it is necessary to define critical infrastructure and develop procedures for its protection. The following documents which should include issues of critical infrastructure are the National Strategy for Emergency Situations and the Law on Protection and Rescue. Nevertheless, these documents still do not include the concept of critical infrastructure.

Although this topic is quite present in recent years, it is evident that, unlike developed European countries, Montenegro has not developed a policy in this area. Given that Montenegro wants to be part of the European Union, protection of critical infrastructure may represent an important element in the process of European integration. Therefore, at the national level, it is necessary to determine the policy of the defining and protection of critical infrastructure, which would define the context, objectives, principles, guidelines and mechanisms. Realization of these activities would be possible through the following steps:

- Creating inter-ministerial working group at the national level, which would be composed of representatives of relevant ministries and institutions, and which would have the task to define critical infrastructure in Montenegro (later on, this working group may perform monitoring of the protection of critical infrastructure, analyze, exchange opinions and attitudes, initiate projects, and may be contact between the public and private sector);
- Development of an adequate legal framework that defines critical infrastructure and its protection at the national level (for example, upgrade of existing National Security Strategy, the adoption of a specific strategy or a law on critical infrastructure);
- Risk assessment, which would help to determine which sectors, or sub-sectors are vital or critical;

- Defining of critical infrastructure with identifying critical sectors, and subsectors (methodology of identifying critical information infrastructure, which is currently in the stage of implementation, may be a starting point for the implementation of this step);
- Identifying relations between different sectors (when defining relations it is necessary to adhere to basic principles of critical infrastructure and the logics of inter-sector connection);
- Identifying national critical infrastructure as part of international critical infrastructure in line with the European Union (given that Montenegro wants to become the part of the European Union).

Finally, the article shows that Montenegro has an infrastructure that can be defined as socially and securely critical. The process of defining critical infrastructure is extremely complex and includes the participation of a large number of state-owned entities. Also, the article stresses the necessity to define and protect the entire critical infrastructure as soon as possible and that a future approach to solving this problem will contribute to new findings in this area.

References

[1] Prezelj Iztok (Ed), *Critical infrastructure in Slovenia,* Ljubljana, 2010.

[2] Jody R. Westby, *International Guide to Combating Cybercrime,* Belgrade, 2004.

[3] Prezelj Iztok, *The conceptual definition of critical infrastructure*, Ljubljana, 2008.

[4] T.G.A.T. Murray, Critical infrastructure protection: The vulnerability conundrum, *Telematics and Informatics 29* (2012).

[5] General's Department-A Division of the Attorney (Emergency Management), *Critical Infrastructure Emergency Risk Management and Assurance,* Australia, 2003.

[6] *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Official Journal of the European Union, 2008.

[7] George Mason University*, The CIP Report - Critical Infrastructure Protection Report* 12 (2008).

[8] Zdenko Kljaić, Sadko Mandžuka, Pero Škorput, *The application of ICT in the management of critical infrastructure in the countries in transition,* Belgrade, 2010.

[9] Bernhard Hammerli, Andrea Renda, *Protecting Critical Infrastructure in the EU*, Centre for European Policy Studies, Brussels, 2010.

[10] *National Security Strategy*, Ministry of Defense, 2008.

[11] *Defense Strategy*, Ministry of Defense, 2008.

[12] Negotiating Position of Montenegro for Chapter 24 - Justice, Freedom and Security, 2013.

[13] Dragan Mladenović, *International aspect of cyber warfare*, Belgrade, 2013.

[14] Dragan Mladenović, *Defining cyber warfare*, Belgrade, 2012.

[15] *Strategic defense review of Montenegro*, Ministry of Defense, 2013.

[16] *Decision on determination of infrastructure and areas of special importance for defense*, Government of Montenegro, 2008.

[17] *Decision on determination of robust technical systems of special importance for defense,* Government of Montenegro, 2008.

[18] *Law on protection of persons and property,* Parliament of Montenegro, 2013.

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.
doi:10.3233/978-1-61499-478-7-277

Risk Management of Terrorist Attacks in the Tunnels as Critical Points of Corridor 5c Infrastructure – Trans-European Road Network Through Bosnia and Herzegovina

Samir AGIĆ [a,1] and Edin GARAPLIJA [b]
[a] *Ministry of Security of Bosnia and Herzegovina*
[b] *INZA Institute of Risk Management and scientific research*

Definition of terms[2]:

a) ''critical infrastructure " means a property, system or a part of them which is located in member states and is necessary for the maintenance of vital social functions, health, safety, the environmental, economic and social welfare of people, whose working malfunction or destruction, as a result of failure to maintain these functions, could have a significant impact in a member state;

b) ''European critical infrastructure" or ''ECI" means critical infrastructure located in member states, and whose malfunction or destruction would have a significant impact on at least two member states. The significance of the impact is assessed considering its cross-sector benchmarks. This includes effects which are a result of cross-sector dependencies on other types of infrastructure;

c) "risk analysis" means a consideration of relevant threat scenarios to assess the weaknesses and the potential impact in the malfunction or destruction of critical infrastructure;

d) "sensitive information about the protection of critical infrastructure" means facts about a critical infrastructure which, if discovered, could be used for planning and action with the aim of causing disruption in the work or the destruction of critical plant infrastructure;

e) "protection" means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to turn away, mitigate or neutralize the threat, risk or weakness;

f) "owners/operators of ECI" means that those entities that are responsible for investments in certain assets, a system or part of them that is based on this Directive are identified as ECI and/or for their daily work.

Keywords. terrorism, terrorist attack, risk management, phase of prevention, phase of preparedness, phase of response and rehabilitation consequence, the recovery phase, strength of the first response, power support, subsidiary response, coordination of the response, Decision CPM 1313/2013EC - mechanism of civil protection, Infrastructure crisis point, TEN trans-European road network, tunnel EU directive 2004/54/EC, construction of the tunnels, the tunnel infrastructures, structural measures, safety equipment, tunnel manager, integrated system, risk analysis, numerical modeling.

[1] Corresponding Author: Dr. Samir Agić, Ministry of Security of Bosnia and Herzegovina; e-mail: Samir. Agic@msb.gov.ba.

[2] Definition (a) – (f) source: 2008/114/EZ EU Council Directive of 8 December 2008. concerning the identification and labeling of European critical infrastructure and the assessment of the need to improve its protection. (Text with EGP relevance), Official Journal of the European Union L 345/75, 23.12.2008.

Introduction

Terrorist organizations or groups, according to the international definition of terrorism, direct their destructive activities on civilian targets for the purpose of inflicting losses, causing fear and uncertainty among the civilian population in order to provide a message to governments about the importance of fulfilling their radical aims of political, religious or similar beliefs.

Terrorism is a criminal act and cannot be justified under any circumstances. During attacks, terrorist usually choose objects of vital importance to the civilian population, as well as places of massive gatherings. Government, therefore, must devote special attention to capacity building and the establishment of standard operating procedures for the complete protection of the civilian population from terrorist attacks as well as the rehabilitation of the consequences of terrorist attacks.

Bosnia and Herzegovina's Strategy for the prevention and fight against terrorism and Plan for civil - military cooperation in case of the response to terrorist attacks and remediation their consequences, are documents that determine the political-institutional relationships and responses in the realization of civil - military cooperation in case of response to terrorist attacks and dealing with the consequences of terrorist attacks. They also include the organization and the priority actions of the competent civil institutions and authorities of Bosnia and Herzegovina, the Entities and Brčko District administrative bodies, Bosnia and Herzegovina in the protection and rescue of people and property from the effects of terrorist attacks, as well as the support of the Armed Forces of Bosnia and Herzegovina to civilian structures in response to acts of terrorism and dealing with the consequences of terrorist attacks.

Taking into account the strategic position of Bosnia and Herzegovina as a country located in Southeastern Europe in general, it can be said that the relevant institutions of Bosnia and Herzegovina are aware of the potential dangers that terrorism carries and which are connected to the growing importance of preventing and combating all forms of terrorism [1].

Civilian response and military support imply the constitution of a lead agency for the implementation of certain measures of response and its role, responsibilities and capacities.

The plan establishes the role, responsibility and capacities of the Armed Forces of Bosnia and Herzegovina, and precisely which measures, when and to what extent the Armed Forces of Bosnia and Herzegovina are included in actions of response to repair the consequences of terrorist attacks [2].

1. Normative legal basis in the fight against terrorism in Bosnia and Herzegovina

International regulations:

- United Nations Global Strategy for Fight Against Terrorism (Resolution GS UN No. 1137 of 2001.) and Action Plan of the United Nations for the fight against terrorism (8th September 2006);
- European Union strategy against terrorism;
- The United Nations Convention on the fight against terrorism[3];

[3] BiH Strategy for Fight Against Terrorism (2006-2009) based on UN Convention

- 2008/114/EZ EU Council Directive of 8 December 2008 concerning the identification and labeling of European critical infrastructure and the assessment of the need to improve its protection.

Regulations in Bosnia and Herzegovina:

- Criminal Code and criminal procedure code of Bosnia and Herzegovina, the entities and Brčko District of Bosnia and Herzegovina[4];
- Law on implementation of the Convention on the prohibition of the development, production, the stockpiling and use of chemical weapons and on their destruction[5];
- Strategy of Bosnia and Herzegovina for fight against terrorism in the period 2006 -2009. , was adopted in May 2006[6];
- BiH Law on Defense[7];
- Law on Intelligence - Security Agency[8];
- Law on the State Investigation and Protection Agency[9];
- Law of the Border Police of Bosnia and Herzegovina[10];
- Framework law on the protection and rescue of people and property from natural and other disasters in Bosnia and Herzegovina[11];
- Law on the protection and rescue of people and property from natural and other disasters in the Federation of Bosnia and Herzegovina[12];
- Law on civil protection of the Republic of Srpska[13].

2. The general concept of terrorism and defense against terrorist threats and attacks

The complexity of defining the causes, levels and effects of terrorism as one of the most latent threats to modern society has defined a number of different forms depending on the understanding of the socio-political, economic or religious motives. One of the distinguished contemporary definitions is that Terrorism constitutes an illegal use of force against people and property in order to frighten or force the government, the civilian population or other segments of the government into achieving political and social goals. The threat of a terrorist attack itself represents, in all countries, with the rule of law, the crime of terrorism. There are four key phases of which the consistent application is the most appropriate way to confront today's terrorist threats in modern society:

[4] Ibid

[5] Ibid

[6] Criminal Code BiH "Official Gazette BiH" no.3/03, 32/03, 37/03, Criminal procedure code BiH " Official Gazette of BiH" no.3/03, 32/03, 36/03, Code of criminal procedure BDBiH " Official Gazette of BD BiH" no.10/03, Criminal code BD BiH "Official Gazette BD BiH" no.10/03, Criminal Code FbiH "Official Gazette of FBiH" no.36/,03, Code of criminal procedure FBiH "Official Gazette of FBiH" no.35/03 and 56/03, Criminal Code RS "Official Gazette of RS" no.49/03, Code of criminal procedure RS "Official Gazette RS" no.50/03;

[7] Official Gazette of BiH, no.15/06

[8] Ibid, no.88/05

[9] Ibid, no.12/04, 20/04

[10] Ibid, no.27/04

[11] Ibid, no.50/04

[12] Ibid, no.39/03, 22/06

[13] Official Gazette of RS, 50/03

- prevention phase,
- preparation phase,
- response phase,
- rehabilitation phase.

The prevention phase represents measures and actions of preventing the occurrence of a terrorist attack or to prevent the spread of the consequences resulting from a terrorist incident.

The preparation phase is an activity of planning measures to ensure the most effective and efficient response to the emergency situation caused by terrorist strike, and it's the basis of the response operation to a terrorist attack. It activates before the detection of lethal means (whether it is classic or special explosive of great destructive power or a RCB agent). The practical goal of this stage is to check whether all operational elements and compositions are ready for timely, controlled, coordinated and effective use, both at the scene of an incident/accident whether it is on local, middle or highest, national or international levels.

The response phase and the rehabilitation of consequences is the phase that occurs immediately with the creation of an emergency caused by a terrorist attack, or by the resulting threats to use NHBR funds (WMD). The response phase involves the immediate actions of law enforcement agencies towards potential terrorists and detecting, deactivating and removing detected suspicious objects and real explosive devices (with or without contained RCB agents). Dealing with the consequences is a result of the action of removing an executed terrorist attack or the action of removing the rubble, rescue and protection of lives, protection of material goods and basic needs of people (secure supply of food, water, etc.). Measures of monitoring/surveillance and detection NHBR agents and the warning/informing of citizens on any enduring effects RCB contamination are implemented simultaneously.

The recovery phase and phase of rehabilitation follow the activities that come after the response and rehabilitation of consequences, and they focus on the restoration and reconstruction of communities of the effects resulting from the accident.

3. The significance of the Civil Protection Mechanism of the European Union (CMP - Civil Protection Mechanism)

On December 17th 2013 Decision No. 1313/2013/EU of the European Parliament and of the Council of the EU of the EU Mechanism for Civil Protection was adopted [3], which represents the continuity of the previous Decisions of the Community Mechanism for Civil Protection, established by Council Decision 2001/792/EC, Euratom, modified by Council 2007/779/EZ, Euratom. The funding of this mechanism is provided by Council Decision 2007/162/EC, Euratom, which established the financial instrument for civil protection.

This Decision predicts the financial assistance of the EU which has to be provided as a contribution to improving the functionality of the response to an emergency situation on a larger scale and to strengthen the prevention and preparedness for all types of emergency situations, including the continued application of the measures previously adopted within the framework of the Council Decision 1999/847/EZ.

The protection that should be provided within the framework of the EU Mechanism for Civil Protection should particularly include the population, but also the environment and property, including cultural heritage, from all kinds of natural disasters and man-made disasters, including environmental disasters, pollution of the sea and emergency medical situations occurring within or outside the Union.

In the framework of the Mechanism of the Union it is possible to request civil protection and other assistance in emergency situations in the event of any such disaster to supplement the capacity to response in the affected country. In relation to the disaster caused by terrorist acts, nuclear or radiological accidents, the Mechanism Union should cover only the actions of preparedness and response in the field of civil protection. The candidate countries and potential candidate countries including Bosnia and Herzegovina have shared obligation to harmonize its laws and subordinate legislation with the EU Civil Protection Mechanism.

4. The place and role of Armed Forces of Bosnia and Herzegovina

The Armed Forces of Bosnia and Herzegovina realize their role in accordance with the Law on Defense of Bosnia and Herzegovina (“Official Gazette of B&H”, No. 88/05) [4]. One of the unavoidable functions of the Armed Forces of Bosnia and Herzegovina is to provide assistance to civilian structures in case of natural or other disasters.

Help of the Armed Forces of Bosnia and Herzegovina to civilian structures is given by the request to the Ministry of Defense, through the Ministry of Security of Bosnia and Herzegovina (Coordinating body of Bosnia and Herzegovina for the protection and rescue), which is approved by the Presidency of Bosnia and Herzegovina. Along with this daily report, a daily situational report is delivered no later than 5 pm on the same day. Before or after this time, after the occurrence of a new emergency, an additional situational report can be submitted. The recommendation is to not introduce too many reports because it suffocates the communications system and creates more confusion. Finally, at the end of the operation, a report of the completion of actions is made. According to current practice, the Armed Forces of Bosnia and Herzegovina, during action on the field, act solely according to the laws provided for coordination mechanisms in which the civilian power structures play a leading role.

Forms of Standard Operating Procedures for seeking and providing the assistance of the military Forces of Bosnia and Herzegovina were made on the basis of the forms used in the NATO Communications Agency. Notification of the accident, based on the approval of the competent national coordination body, is delivered to neighboring countries and operational centers of international organizations (NATO, EU, UN, Interpol) over the relevant operational center of Bosnia and Herzegovina. Once delivered, a notice to the international community requires a periodic reporting on the situation in the affected area by delivering daily situational reports (one in 12 or 24 hours), and if it is necessary, in special reports, if other party of communication demands it.

The same patterns are used in the preparation phase before the event, and for the realization of exercises, with the proviso that in the header of each form it must be emphasized that these are exercises.

5. CASE STUDY: The terrorist threat and attack to tunnel L = 600 m on a section of the Lepenica - Tarčin highway on Corridor 5C

Terrorist attacks on critical points of infrastructure, especially in tunnels, from a security aspect the most sensitive facilities TEN Trans-European road network, represent a latent threat to the functioning of not only the country that is attacked, but also the wider region, because of the long-term secondary and tertiary consequences such as traffic jam and the normal functioning of the economy.

In analyzing terrorist threats on a global scale, we come to the conclusion that they are most commonly performed by explosive attacks in the form of hand luggage and car bombs of various sizes from personal cars to trucks positioned at critical points of infrastructure and public facilities, and to a lesser extent on military targets, because the same are defended at much higher levels and their access to direct terrorist attack is very difficult.

(Example of attacks by hijacked civilian planes on the World Trade Center towers in New York, when the enormous temperatures from the explosion and fire caused by kerosene from hijacked planes, yielded to payload structure and the WTC towers came to their total collapse.)

6. Scenario of explosion - car bomb

Out of the known explosive materials most commonly in use is TNT or trotyl or Trinitrotoluene ($C7H5N3O6$), a nitro compound of toluene, and the most applied military explosive. It is a pale-yellow crystalline solid. In the sunlight it turns into dark orange. It can be stored for a long time, and does not change its properties. It's slightly sensitive to attack, so it is easy to handle. It belongs to middle-strong high explosives. Alight outdoors it burns a steady red-yellow flame. It is used poured and pressed, pure or mixed with other explosives, such as penthrite, hexogen, tetryl (tetratol) and ammonium nitrate.

For blasting and demolition trotyl is pressed or treated in various forms called "trotile bullet" in the shape of a cylinder of 75g and 100g, 100g and 200g in a rectangular shape, 500g and 25kg in a wooden box.

According to the quantity of explosive material with which the bomb attack is performed we divide it based on:

- Bomb in hand luggage <50 pounds (cca.20 kg) of TNT
- Bomb size passenger vehicles with power <500 pounds (cca.200 kg) of TNT
- Van vehicle Bomb size with power <5000 pounds (cca.1000 kg) of TNT
- Bomb truck size strength> 10,000 pounds (cca.2000 kg) of TNT

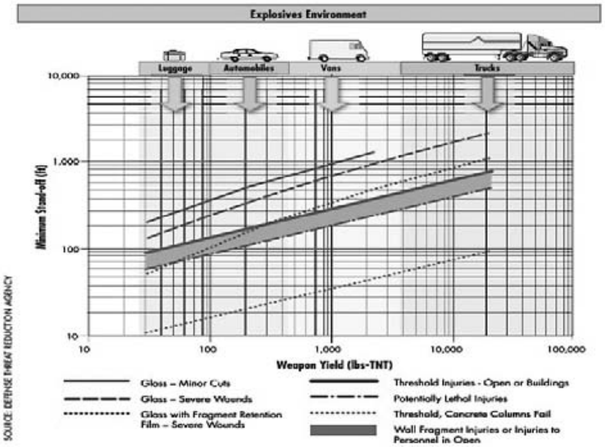


Figure 1. Space Explosion - Key risks are injuries by the pieces of glass and the collapse of the supporting structure [5]

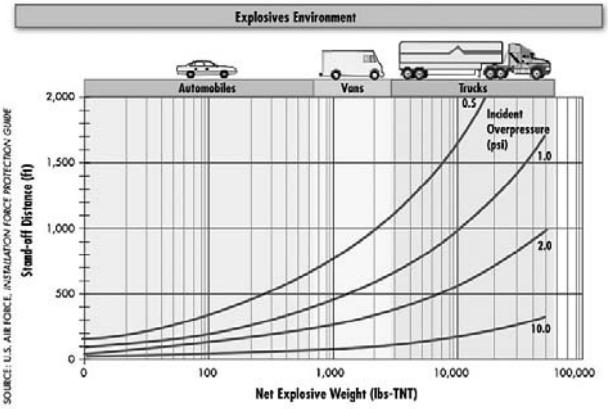


Figure 2. Overpressure measured as function of stand-off distance and ex. Weight [6]

Conclusion: the calculation of blast effects (strike effect) during the detonation of a bomb in the tunnel shows that the activation of less explosive device dimensions of hand luggage with max. 20 kg of TNT would impose significant property damage but not disturb the construction of the tunnel. However, in the case of activation of car bombs, most probably it would lead to collapse of the construction of tunnels and its collapse.

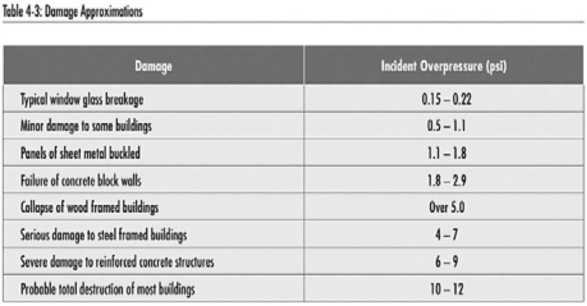


Table 4-3: Damage Approximations

Damage	Incident Overpressure (psi)
Typical window glass breakage	0.15 – 0.22
Minor damage to some buildings	0.5 – 1.1
Panels of sheet metal buckled	1.1 – 1.8
Failure of concrete block walls	1.8 – 2.9
Collapse of wood framed buildings	Over 5.0
Serious damage to steel framed buildings	4 – 7
Severe damage to reinforced concrete structures	6 – 9
Probable total destruction of most buildings	10 – 12

Figure 3. Explosive shocks in air [7]; Facility Damage and personnel injury from explosive blast [8];

Numerical risk assessment based on internationally recognized models represents a significant part of the strategy of defense against terrorist attacks on the tunnels as a critical point of infrastructure, including the planning of preventive security measures and infrastructure construction of tunnels recommended by the Tunnel Directive 2004/54/EC.

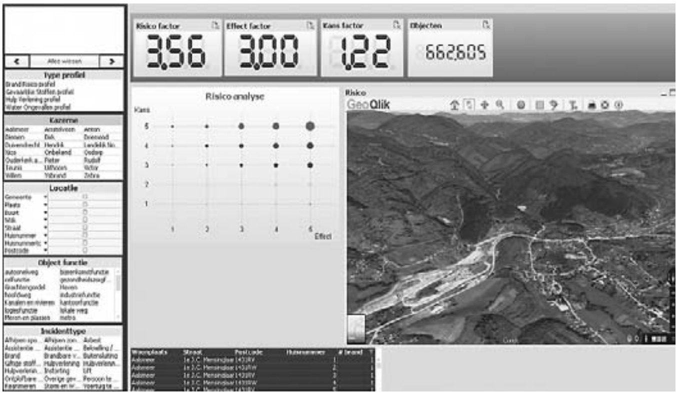


Figure 4. RISICO fire safety software [9]

Tarčin, Trans European 5C corridor that passes through Bosnia and Herzegovina, software package Pyros version 2014.1.0110, FDS version 6.0.1 and Smoke view as used. CFD[14] simulations have become an integral part of the analysis in disciplines such as aerodynamics, fluid dynamics, fire engineering and others. Computer simulations, at the same time, provide great opportunities in simulations of fire spreading and fire parameters. Fire is a very complicated and complex process which consists of combustion, turbulence, fluid dynamics and other physical and chemical processes. FDS[15] simulation of fire and tracking of fire parameters in the tunnel in the last decade has become an effective tool to prepare scenarios for saving the environment affected by fire, and fire suppression. Computer simulations allow the visualization of the spread of fire and its parameters, such as temperature, air velocity, liberated heat transfer, smoke, etc., and in some cases allows the testing strategy and the effectiveness of fire suppression that may be useful for prevention. Computer simulations of fire are the safest, most economical and fastest possible methods for research and analysis of the process of fire in a particular environment. Through them it is possible to develop different scenarios and models of actions in case of fire. It has become evident that it is not enough to just design engineering reliance on the traditional empirical approach to the design of fire protection and safety systems in the tunnels, but the modeling and simulation of various scenarios of risk has become an obligation of the appropriate preventive approach.

[14] Computer Fluid Dynamics - platform for computer simulation of fluid

[15] Fire Dynamics Simulator - platform for computer simulation of the parameters of fire

7. Scenario of fire in the tunnel

The modeled tunnel has dimensions of 9.5 mx 600 mx 6.5 m (width x length x height). In the tunnel there are six fans. Two fans at the ends are located at 50 m from the entrance or exit and the distance between the fans in the tunnel is 100 m. The modeled tunnel is already imported from AutoCAD and modeled in the Cartesian coordinate system, with coordinates x [1210.05, 1810.05], y [3298.94, 3309.69], z [-4.11713; 3.21151].

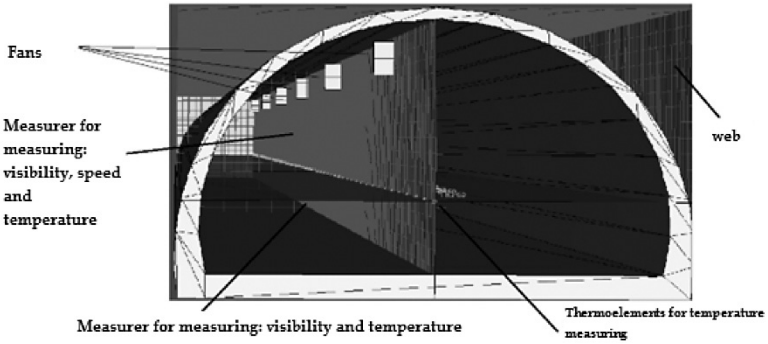

Fans
Measurer for measuring: visibility, speed and temperature
web
Measurer for measuring: visibility and temperature
Thermoelements for temperature measuring

Figure 5 – Fire dinamic software, INZA Institute of Risk Management [9]

The source of fire is represented as a pool measuring 10m x 5m. Distance from the source of fire to the exits and entrance of the tunnel is approx. at 300 m, which means that a fire is in the middle of the tunnel. Maximum heat released per unit area (HRR TIMES) is 6000 kW / m, and the total heat liberated after seven minutes of simulation of fire HRR is ≈ 150 MW. As to „PIARC Committee on Road Tunnels[16]“ title “Fire and smoke control in road tunnels” approximately equals to the total heat liberated by liberate one tank (tank Combustible) with $5m^3$ of fuel. The longitudinal ventilation speed is 5 m/s up to 7 minutes when the source of the fire extinguishers (fire stops) and then increases the fan speed to a speed of 50 m / s in order to eject the smoke out of the tunnel. The total simulation time is 15 minutes (900 seconds). Initial temperature throughout the tunnel is 20°C. The dynamics of the source of fire and ventilation will once again repeat as follows. Beginning of fire t = 0 and beginning with the ventilation air speed of 5 m/s in the positive x direction. At time t = 420 s (7 minutes) stops the source of fire and at that point is the largest liberated heat while at the same time the fans go at a speed of 50 m / s to simulate smoke extractor tunnel after a fire, also in the positive x-direction as is fixed to the end of the simulation (900 seconds).

The movement of smoke is simulated through a tunnel tube during a fire with normal ventilation and movement of smoke after a fire when it’s concerning smoke extractor tunnel tubes. The temperature values at fixed points are measured at every 10 meters at a height of 1.85 m (z-axis), which roughly corresponds to the height of the head of a man who is trapped in the fire.

Also at that height of 1.85 m (z-axis) a slice is set up on which we will monitor the temperature and visibility throughout the tunnel. Through the middle of the tunnel (on the y-axis) we will monitor visibility, speed and temperature throughout the tunnel. The simulation of fire in the tunnel was performed on an Intel (R) Core (TM) i3-3240 @ 3.4 GHz processor, with 12.0 GB of installed memory and 64-bit operating system. The

[16] PIARC - World As sociation for paths and roads, formed in 1909, 120 government-members worldwide

network, which is located in the tunnel model consists of four sub networks whose cell size in the x-axis of 1.0 m, the y-axis of 0.45 m and the z-axis of 0.41 m total number of cells in the model is 259 632 of which depends on the total simulation time. The total time to simulate the FDS-in is 31 hours 35 minutes and 12 seconds.

Visibility is an important factor during the evacuation and extinguishing actions.

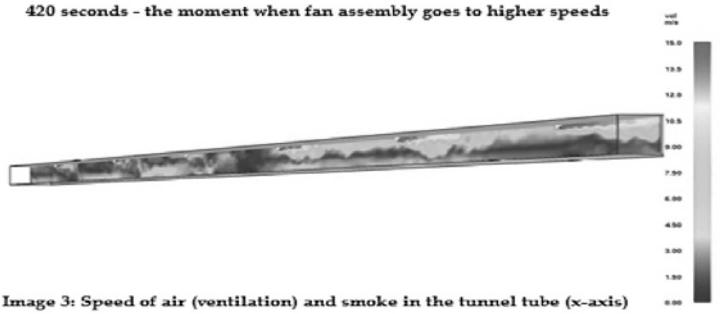
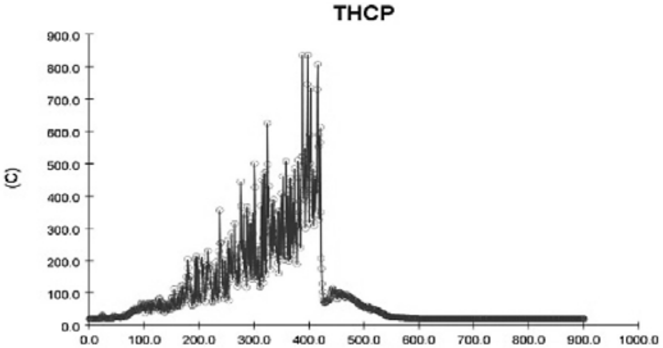

420 seconds – the moment when fan assembly goes to higher speeds

Image 3: Speed of air (ventilation) and smoke in the tunnel tube (x-axis)

Simulation on 360 seconds from the start of fire shows that the temperature reaches over 500°C, and 400 seconds on 850°C.

470
425
380
335
290
245
200
155
110
65.0
20.0
1210.1
1260.1
1310.1
1360.1
1410.1
1460.1
1510.1
1560.1
1610.1
1660.1
1710.1
1760.1



Figures 6, 7 and 8. Speed of air (ventilation), smoke and temperature in the tunnel tube (x-axis) Fire dynamic software [9]

Conclusion: The action of fire extinguishing, since its beginning, should begin in 420 seconds (7 minutes) if it wants to achieve an adequate response and prevent more serious consequences. If you are late with the intervention of extinguishing longer than 600 seconds (10 minutes) of fire, the temperature reaches over 1000°C, and soon it comes to an explosive cracking the concrete construction of the tunnel (eng. spalling), disrupting its integration and capacity and 900 seconds (15 minutes) after the start of fire may lead to the total collapse of tunnel construction.

8. Risk management of terrorist threats of attacks on tunnels

The preventive approach involves the application of preventive measures during the design and construction of the tunnel as the most sensitive critical infrastructure points.

In the engineering and architectural sense, it is necessary to respect the guidelines of the European Tunnel Directive 2004/54/EC and European regulations for construction products CPR 305/2011, which requires the use of construction products whose properties must ensure that the designed resistance of fire, preventing its spread and preserve the integrity of structures in order to provide sufficient period of time for an adequate response of firefighting forces or safe evacuation of threatened. Designing according to Eurocodes[17] means respecting all the preventive measures and the selection of construction materials resistant to fire, whose resistance is proved in independent accredited laboratories according to EN 17025 standards. The tunnel directive suggests a risk analysis of tunnels, and directions for the technical prevention measures during the design and construction of a tunnel. For long tunnels of 500 m, the integration of security systems for the early detection of fire, video surveillance and evacuation, with active systems for fire, smoke, drainage, and signalization is recommended.

The tunnel directive recommends the establishment of the institution of tunnel Manager for tunnels longer than 3000 m, and the establishment of checkpoints for central monitoring and control. A very important element in adequate response to the potential risks is the establishment of a rapid intervention unit for fire-extinguishing and rescue in the immediate vicinity of critical points, and the strengthening of local government units and their subordination in the action-fighting. Ongoing training and the doing of exercises where all actors are involved in fire-fighting and rescue system is recommended. Phase planning preparedness measures and response in accordance with the plan of cooperation in the case of the response to terrorist attacks and remediation of their consequences is an extremely important part in the overall system of prevention and response to risks in critical types of infrastructure.

9. The levels of activation/response

The principle of subsidiary, early warning and alerting and operational response are carried out from the lowest to the highest level - from local government to the state level. The decision on the need for a higher level of activation on the basis of assessments is brought by the authorized administrative authority or professional body of senior levels of government at the request of the competent authority of lower levels of government (Headquarters of Civil Protection as a professional operative government body / entity / District). Entities and Brčko District of Bosnia and Herzegovina are obliged to align their plans with this plan in order for a timely response to prevent, rescue and protect from the consequences of a terrorist attack.

9.1. Level 1 - Activity before response

The regular monitoring and communicating for the purposes of the constant exchange of information on security - interesting phenomena. Operating Centers of police

[17] Eurocode - Eurocodes, design technical guidelines

administrations and Civil Protection in the entities and Brčko District of Bosnia and Herzegovina, work continuously 24/7, while municipal civil protection operational centers in entities operating in regular activities by the system 8/7, regular regime of work and the composition of the staff.

9.2. Level 2 - Operative response to an imminent threat of terrorist attack

Increased monitoring and communicating with the relevant departments and higher authorities for effective and timely assessment. Operative centers go to the regime of continuous operation (24/7) with reinforcement of regular staff composition. At this level it is possible to find suspicious items/objects whose removal requires fast reaction forces for law enforcement.

9.3. Level 3 - Operative response to the consequences of a terrorist attack

The terrorist attack has been performed and a state of natural or other disasters declared. Operative centers of law enforcement agencies in the field of security, civil protection and other emergency professional services work continuously 24/7 in increased operating mode and extended composition of operational staff on the principle of subsidiary reporting and response to the consequences. Per activation of competent staffs and coordinating body for the management and coordination of operations and response forces, a mechanism of regular notification through reports on the situation is established. It all starts with information about the incident / accident and the same is delivered to the higher competent authority immediately after the occurrence of the incident.

Once past efforts by first response to further assess the impossibility of dealing with the consequences of an incident/accident following the ascending line of subsidiarity, a request for assistance is submitted to higher level.

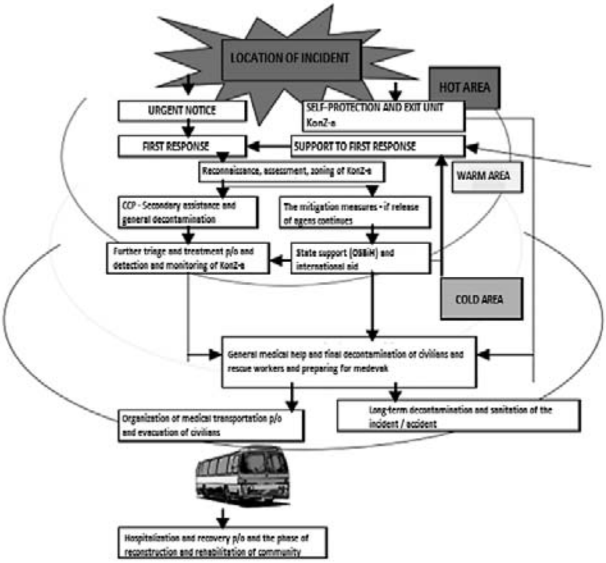

LOCATION OF INCIDENT
HOT AREA
URGENT NOTICE
SELF-PROTECTION AND EXIT UNIT KonZ-a
FIRST RESPONSE
SUPPORT TO FIRST RESPONSE
Reconnaissance, assessment, zoning of KonZ-a
WARM AREA
CCP - Secondary assistance and general decontamination
The mitigation measures - if release of agens continues
Further triage and treatment p/o and detection and monitoring of KonZ-a
State support (OSBiH) and international aid
COLD AREA
General medical help and final decontamination of civilians and rescue workers and preparing for medevak
Organization of medical transportation p/o and evacuation of civilians
Long-term decontamination and sanitation of the incident / accident
Hospitalization and recovery p/o and the phase of reconstruction and rehabilitation of community

Figure 9. Scheme of a danger zone from terrorist attacks with the phases of response, extract from the cooperation plan in the case of the response to terrorist attacks [10].

10. General conclusions

Terrorism as a global risk has resulted in a growing number of human casualties and the enormous material damage is a latent threat to civil society. Potential terrorist targets are critical points of infrastructure because with their communication position they connect certain geostrategic points and spaces of economic interest. Means for the terrorist attacks can be complex (sophisticated explosive devices) but can be as simple as the kidnapped fuel tanks that may provoke a considerable damage in tunnels as critical points of infrastructure. The preventive approach to designing and construction significantly reduces the risk and consequences of natural and other disasters caused by man's influence. Adequate response and coordination at all levels of government and civilian structures, including military force in order to prevent and eliminate the consequences of terrorist attacks is a common obligation and duty. Only well prepared, well trained and equipped units power responses are a guarantee of risk reduction and defense against potential terrorist attacks.

References

[1] Strategy of B&H for prevention and fight against terrorism; Ministry of Security of Bosnia and Herzegovina, 2010.

[2] Plan of civil - military cooperation in case of response to the terrorist attacks and their aftermath remediation, Ministry of Security of Bosnia and Herzegovina 2014.

[3] Decision No. 1313/2013/EU of the European Parliament and of the Council of the EU of the EU echanism for Civil Protection

[4] Law on Defense of Bosnia and Herzegovina (»Official Gazette of B&H«, No. 88/05)

[5] Space Explosion - Key risks are injuries by the pieces of glass and the collapse of the Supporting structure, DEFENSETHREAT REDUCTION AGENCY

[6] Overpressure measured as function of stand-of distance and ex Weigt, U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE

[7] Explosive shocks in air, KINNEY&GRAHAM, 1985.

[8] Facility Damage and personnel injury from explosive blast, MONTGOMERY&WARD, 1993.

[9] INZA Institute of Risk Management

[10] Risk Assessment of Bosnia and Herzegovina from natural or other disasters, Ministry of Security of Bosnia and Herzegovina, 2011.

This page intentionally left blank

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015
© 2015 The authors and IOS Press. All rights reserved.

Subject Index

Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection
Denis Čaleta and Vesela Radović (Eds.)
IOS Press, 2015

© 2015 The authors and IOS Press. All rights reserved.

Author Index

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank