dialogues Security

323.285:504.4]:338.49 Scientific article

RISK ASSASSMENT AND ANALYSIS ON SECURITY OF CRITICAL INFRASTRUCTURE – THEORETICAL APPROACH

Oliver Andonov, PhD
Faculty of security, criminology and financial control
MIT University-Skopje
andonov.oliver@yahoo.com

Jordan Popovski, MSc
Security advisor of Prime ministry of government of Republic of Macedonia
jpopovski.moi@gmail.com

Абстракт

Проценатa и анализата на ризиците и заканите врз безбедноста на критичната инфраструктура претставува спој на емпирискиот и теориискиот пристап во научното и прагматичното согледување на безбедносните ризици и закани. Испреплетеноста на теорискиот и прагматичниот пристап се должи на поврзаноста на научната дескрипција на можните ризици и закани врз специфичните објекти или системи поврзани со критичната инфраструктура. Оваа дескрипција влијае и врз проширувањето на проценатa и анализата на ризиците врз истата во насока на дополнителните загрозувања на безбедноста како последица на загрозувањето на виталната критична инфраструктура од различни видови загрозувања.

Овој труд има за цел да направи краток теориски осврт кон проценатa и анализата на некои ризици врз критичната инфраструктура како што се загрозеноста од терористички напади и можни природни катастрофи. Токму превентивното делување чија цел е и самата проценка и анализа ги оправдува искуствените научни и прагматични сознанија. Трудот ќе направи осврт кон некои можни теориски пристапи во проценатa и анализата на ризиците како пристапи и теориски дефинирани поимања на ризикот како појава, притоа нераздвојувајќи го од заканата и предизвиканата штета.

Клучни зборови: ризик, закана, проценка и анализа, критична инфраструктура

Abstract

The assessment and analysis of risks and threats to the security of critical infrastructure is a combination of empirical and theoretical approach to scientific and pragmatic understanding of security risks and threats.

Intertwining of theoretical and pragmatic approach because of the connection of the scientific description of the risks and threats to specific facilities or systems related to critical infrastructure. This description affects the expansion of the assessment and risk analysis on the critical infrastructure towards the additional security threats because of disruption of vital critical infrastructure threats of various kinds.

The study aims to make a brief theoretical review of the assessment and analysis of some risk to critical infrastructure such as threats of possible terrorist attacks and natural disasters. Exactly that preventive action whose aim is the assessment and analysis, justifies the experienced scientific and pragmatic knowingness. The study will take into account some possible theoretical approaches to assessment and risk analysis like theoretical approaches as defined notions of risk occurrence, make it to be inseparable from the threat and caused damage.

Keywords: risk, threat assessment and analysis, critical infrastructure

Introduction

Clarifying toward writing a thesis, which concerns the theoretical and empirical understanding of the risks and threats to security, it is necessary to orient to the importance of safety. Besides setting the basic issues in the security paradigm: "security for whom?" and "security from what?" it is necessary to give an answer about the importance of safety through prism of the importance of safety on the epistemological basis. First, getting answers to questions „for whom"and „from what"is the security about, is based on philosophical understanding of the importance of safety, understanding the security paradigm and modern security concept. All of this would be incomplete if in this context we

do not perceive the risks and threats to security as a major accelerator that affects the answer to submitted questions.

Without a doubt, safety is a much-disputed concept, especially in terms of empirical view towards the sources of danger and object of protection. The correlation of the source of danger and the object of protection is imminent, and the set interaction and mutual influence can be essential for the perception of risks and threats to the security of society or its individual elements or areas.

Relations to the sources of endanger and the risks and threats to security are aimed towards their elimination, reduction or neutralization, with the aim to reduce the damages. To the effectiveness of this approach, influences the power that enhances or decreases the positions of the object in terms of security risks and threats.

Starting from the understanding of security and its need is necessary to determine the reference object of security, because without his determination the whole concept of security is meaningless as well as the analysis in which it is necessary to identify the risks and threats in order to have defined what to protect and from whom.

The analysis starts from the determination of whose security is in question. Who should be protected and what is its significance in the macro or microenvironment, and why is it important and what is important for the specified reference objects. Whether is a matter of an analysis of state interests or an object of critical infrastructure, we can determine a tentative model that starts with the determination of the reference object and continues by analyzing the processes of the threat, the degree of the threat and the consequences that could occur not only on the reference object, but also on the broader environment.

There are different types of risks and threats and their sources and we must have in mind that for each specific risk or threat we can use special tools to analyze, evaluate or to construct a model for early warning in accordance with its specificity. Based on this analysis and set prompt detection of risks and threats we can build specific pattern of action, which is based on theoretical knowledge, and empirical impact of previous or similar risks and threats to the reference object or some other similar object.

In this context, we aim at the risks and threats to critical infrastructure and the so far experienced impact of previous threats to specific parts of the critical infrastructure from specific types of threats, as well as assessing the impact that may have on the functioning of society and acceleration of other threats to other reference facilities.

Through this paper, we will try to give a brief overview of the theoretical approach and explanation of the concept of risks and threats within the security concept, and with particular reference to risks and threats to critical infrastructure. We will supplement this approach with the definition of critical infrastructure and empirical observations about the possibility of jeopardizing the critical infrastructure in Republic of Macedonia, and the impact of the theoretical model of analysis and assessment of risks on building a pragmatic approach to critical infrastructure protection in Macedonia.

1.Theoretical determination of the risks and threats

The concept of risks and threats and their scientific treatment requires special elaboration.

When we define the risks, we influence security. Risks and threats are two categories that can be synonymous or not depending on the theoretical model of access.

If you try to give a definition of what represent risks and threats, without intention for deeper elaboration, we can say that the threat primarily refers to unwanted, intentional or unintentional event that can cause damage on a particular subject. According to Lennart Sjoberg, threat concerns the danger to which there is a high probability that they will occur and cause consequences.

In this definition, Sjoberg equates the terms threat and risk reducing them to synonyms, believing that the risk is the expectation of an adverse event such as a social construction[14]. The risk can also be described as an expectation in terms of some external event, actor or a structural condition.

The threats are expressed intent of a facility that will inflict damage upon the subject.

They have a double meaning:

1. It is exactly known who sent the threat (if it is a state, group, organization, criminal group, etc.) and

2. towards whom (to the state, a group, individual, etc.). Sojeberg concluded that threats create a sort of elevated threat perception. He called this process assimilation and he considered that if the threat is very likely (direct) it will emphasize risk.

[14] Л.Георгиева, "Менаџирање на ризици", Филозофски факултет, Скопје, 2006, стр.80-81

Although security concept in modern societies is state responsibility such as basic security entity, in the security paradigm stands human security and building a national security policy. Within the national security policy, protection of critical infrastructure is included as an integral security.

Putting it as part and parcel of national security, including looking at through the prism of protecting the security of citizens, security of critical infrastructure as well as general threat to the security of society, can be defined more precisely or to set up within the analysis through the following points:

- Security for whom (reference object / subject);
- Security of what (values);
- Security from what (procedures), from which threats;
- Security with what (meaning) which means[15].

Experience in protecting critical infrastructure and determining the threats to specific objects of protection, affect the establishment of the analysis and assessment of risks and threats, and the means by which we need to achieve maximum protection as well.

The theoretical definition of risks and threats represents a starting point for determining the reference object of protection, why is he protected, what or which means are protected through his protection, by which means and from which threats it is protected. By establishing the theoretical model and defining the risks and threats as a constant social phenomenon, we are opening the possibility for defining critical infrastructure, right through the prism of its threats and need for protection.

2. Critical infrastructure

Swiss military theorist Henry Antuan-Zhomini that highlights the strategic and operational importance to the leadership of the military actions first introduced the term "infrastructure" in XIX century. Later the term infrastructure begins to be used wider like term that partly assesses the development of a country.

According to Moteff *"Infrastructure is the basic physical and organizational structure that is needed for the society, environment, organization or institution to function*

[15] Ibid pp.44

smoothly within itself." He said that *infrastructure is a set of interconnected structural elements that provide related support of overall functioning of the environment*[16]

In the last decades of the XX century, world political scene indicates a need for distinctive conceptual determination of terms infrastructure and critical infrastructure. Thus, the term critical infrastructure was originally perceptual directly connected to energy security, not taking into account the telecommunications, energy systems, gas and oil pipelines, the economy, transport, water supply, emergency services and so on.
Because critical infrastructure includes resources that are necessary for the functioning of society, such as those might be defined the following:

- o Energy facilities and networks;
- o Communication and Information Technology;
- o Finance;
- o Health;
- o Food;
- o Water;
- o Transportation;
- o Production, storage and transportation of dangerous goods, and
- o Government facilities[17].

In accordance with the above division and definition of critical infrastructure listed in the European Programme for Critical Infrastructure Protection (EPCIP) Critical Infrastructure is a system of facilities, services and information systems, which termination defects in the operation or destruction, would have a serious negative impact on the health and safety of the public, the environment, national economy or on the efficient functioning of the state management[18].

The incorporation of critical infrastructure protection in the security policy of each country in order to protect the national, economic and societal security is an inevitable process, whether it is the presence of traditional or asymmetric threats.

---

[16]Moteff J. and Parfomak P., „Critical Infrastructure and Key Assets:Definition and Identification", Congresional Research Service - The Library of Congress, Wasington D.C., 2004, p.p. 5

[17] Commision of the EU Communities, „Critical infrastructure protection in the fight against terrorism", Brusseles, 2004, p.p.4

[18] http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

The process of globalization and the fight against international terrorism poses necessity of protecting critical infrastructure. New challenges such as modern terrorism and natural disasters, initiates a number of factors that threaten the various elements of the infrastructure and their effects influence the status of security. They are threatening factors and they can be divided into the following groups:

- Organized actions with harmful intentions:
- events of natural origin:
- Threats of technological nature (caused by human error or technical involvement):

Besides dealing with military risks and hazards and dangers of internal security character, to complete the security triangle, a holistic approach is necessary to incorporate the protection of critical infrastructure in the architecture of the national security system of the country.

This incorporation into the security system of the Republic of Macedonia involves setting a model for risk assessment and analysis, which will influence the creation of a suitable model for early warning of risks and threats to critical infrastructure. The analysis and assessment of the risks is an introduction to the process of making appropriate security and policy decisions for the organization and operation of critical infrastructure protection and the impact of threats overall society.

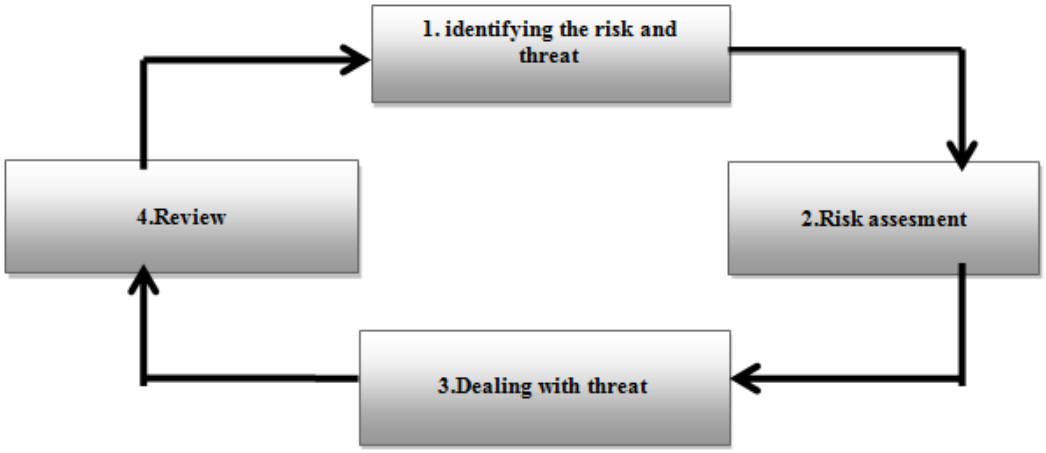
3. Analysis and assessment of risks - theoretical approach

The analysis and assessment of the risks and threats are related activities, which are generally intertwined in no strictly defined order, because with the analysis, the risk assessment is done and through the assessment, it is necessary to analyze the threat. The need to know that the analysis and assessment of the threat is a process that aims to risk management, namely the establishment of at least minimal control over its development and movement, and especially the impact on the reference object of protection (critical infrastructure) and wider implications.

The beginning of the risk and threat assessment represents a cycle, it begins with identification of risk and changes to the so-called risk management, and it is shown at scheme number 1 in the so-called "traditional cycle" which is a basis for the assessment and risk analysis and threats to the reference object of protection.

Figure 1

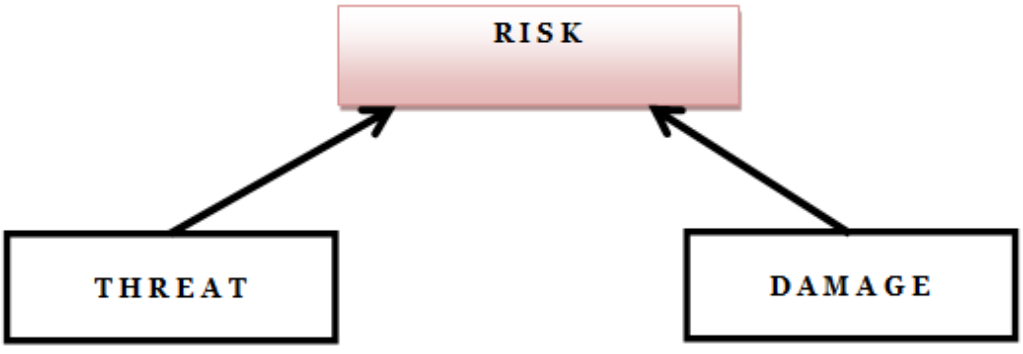
Traditional cycles of assement and managing threats



The simplest model of risk assessment has two dimensions. It is comprised of direct assessment of the likelihood of threats combined with the assessment of consequences incurred or damage that will be caused. This model is made up of the most obvious and essential elements of the risk assessment and we can see that in the Figure number 2.

Figure 2

Simple shame on risk



In every risk, assessment level of threat and possible harm caused is the base for assessment and analysis. The analysis is a complex process and approach that requires more than simplicity in modeling risk assessment.

Assessment and risk analysis is rational and determined approach and comprehensive solution for identifying occurrence that threatens the security and the problems that will probably cause its determination[19].

It is the same method for estimating expected losses from the environment or some adverse events over which we can or we cannot influence.

The key word is **estimating**, because the risk analysis will never be in the context of an exact science even though will use knowledge and information of exact sciences, we still talk about *probability*.

There is no possibility for detailed risk analysis and there are not always issues with a single security exposure caused by a risk, and it would allow determination and detailing the assessment and risk analysis. There are always additional risks despite the risk or threat to the fundamental object of security. The more information we posses, the more accurate analysis and risk assessment we will be able to create, but it is never possible to create 100% analysis and risk assessment that emerges as a threat to security in any aspect of security.

In process of management, it is a logical way for creating the risk analysis, which is a necessity to achieve some basic purposes like:

1. Identifying the resources necessary for the commencement of protection (money, goods, material and technical resources, industrial process, etc.).

2. Identifying the types of risk (hazard-threats) that may influence the occurrence of adverse social or natural phenomena (kidnappings, extortion, robberies, fires or earthquakes).

3. Determining the possible variants of occurrence of risk. This determination is not only a scientific approach but also art in the design of probability (knowledge of probability theory and game theory in security studies, and knowledge of contemporary security paradigm). It is necessary to know that "Nothing is ever 100% safe."

4. Determination of impacts or effects from risk in equivalent to dollars or Euros, if possible, in case of loss or the surrounding material and financial nature.

[19] J. F.Broder , „Risk Analysis and the security survey" , Second Edition, Elsevier science, Burlington, 2000, pp 93

Based on these findings we assess the risk exposure.

Risk analysis and threat is a combination of theoretical, scientific and pragmatic model that must be adjustable in terms of the types and levels of threats and risks have on the security or specific infrastructure that implies wider implications and security threats.

Determining the security risk is dependent on the identification of threats and vulnerabilities that depend on the probability of threats, vulnerability together, and their influence will determine the means of protection[20].

Risk brings uncertainty to the security and reveals the vulnerability of society or institution-critical infrastructure and the possible consequences and the main purpose of the analysis is to reduce the uncertainty (in particular introduction to the threat and risk) and by taking appropriate measures and actions to reduce vulnerability.

There are some conditioners threats and developments affecting the increase or reduction of vulnerability:

- Lack of professionals,
- Possession of knowledge and technical resources
- Changing the security codes to protect the system and infrastructure.

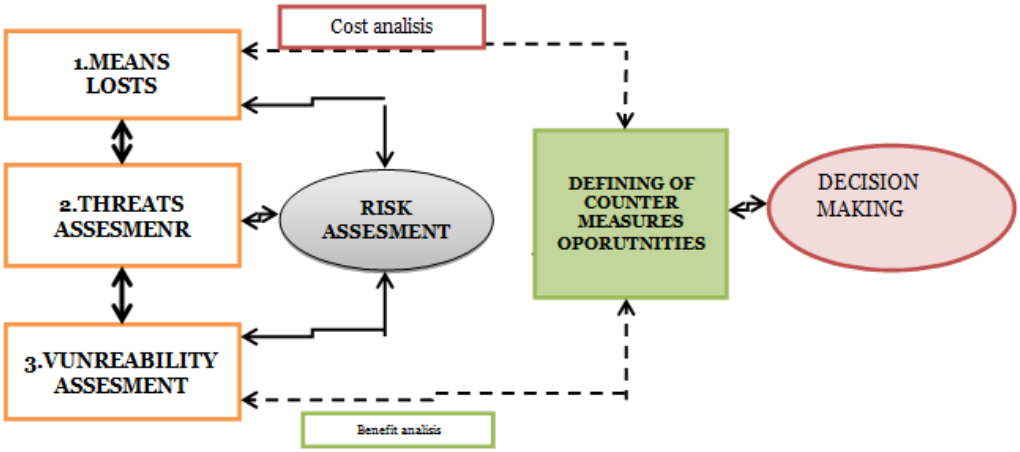
Risk assessment and analysis is a process. This process is determined and modeled, but it can undergo essential changes depending on the urgency of the analysis, the level of threat of overwhelming threat and the degree of risk and potential harm that would be suffered.

The Figure number 3 shows the basic process of risk assessment.

[20] D. Landoll, "The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments", CRC Press, New York, 2011, pp 365

Figure 3

Basic process of risk assessment



The process of risk assessment applied a few steps, procedures, but it is especially important to identify the risks and threats, determine vulnerabilities, determine opportunities to protect and identify facilities that are available and identified priorities for action. All this depends on proper analysis and availability of information on the risks and threats that affect the total adoption of appropriate decisions to deal with the threat and risk reduction or avoidance of damage, primarily human losses.

3.1. Assesment and analysis of specific risks to critical infrastructure in the Republic of Macedonia

The core values of a nation, health, economy and security are dependent on the production and distribution of certain goods and services, which in turn have interdependence with the string physical assets, functions, and systems of critical infrastructure (transport of goods and people, communications, banking and finance, supply and distribution of electricity and water, etc.).

Risk assessment on critical infrastructure includes analysis of threats, vulnerabilities and consequences. Dealing with defined risk management involves deciding which safeguards will be taken based on advance procedures and strategies to reduce risk. Models or methodologies for risk management have been developed based on what threats, vulnerabilities and risks are present to then execute the allocation of resources to reduce

those risks. The methodology for risk management on critical infrastructure would include identifying critical infrastructure elements and assess which ones are most critical, characterizing and assessing specific threats to them, identifying the expected effects of these threats and determining ways to prevent or reduce, and defining the measures to reduce the risk based on the applied methodology or strategy.

There are many kinds and types of factors threatening the critical infrastructure that could be divided into the following categories:

Natural disasters:

Meteorological:
- Windstorm, tropical cyclone, Hurricane, tornado
- Thunderstorm
- Snow, ice, hail, sleet storm
- Flood
- Storm surge
- Extreme weather
- Heat wave
- Cold wave
- Drought

Glacier, iceberg

Geophysical:
- Earthquakes
- Tsunami
- Volcanic eruptions
- Landslide, mudslide, subsidence
- Geomagnetic storm

Fire:
- Forest, wild land
- Urban
- Fire following earthquake

Biological:

- Diseases that affect humans
- Diseases that affect animals
- Diseases that affect plants
- Animal or insect infestation or damage

Attacks:

- Chemical attack
- Biological attack
- Radiological attack
- Nuclear attack
- Explosive attack
- Cyber attack
- Conventional arms attack
- Enemy attack / war
- Electromagnetic pulse
- Sabotage
- Espionage (industrial and otherwise)
- Crimes (e.g., theft, kidnapping, arson, extortion)
- Social unrest (riot, lawful /unlawful protest, disruption)
- Strike or labor disruption

Other intentional actions that can affect critical infrastructure (Non-malicious):

o Border closure
o Regulation change

Accidents or technical hazards:

Accident:
- Transportation accident

- Hazardous material spill or release (explosive, flammable liquid, flammable gas, flammable solid, oxidizer, and poison, biological, radiological)
- Fire
  - o urban fire
  - o Industrial fire
  - o Chemical fire
- Accidental explosion

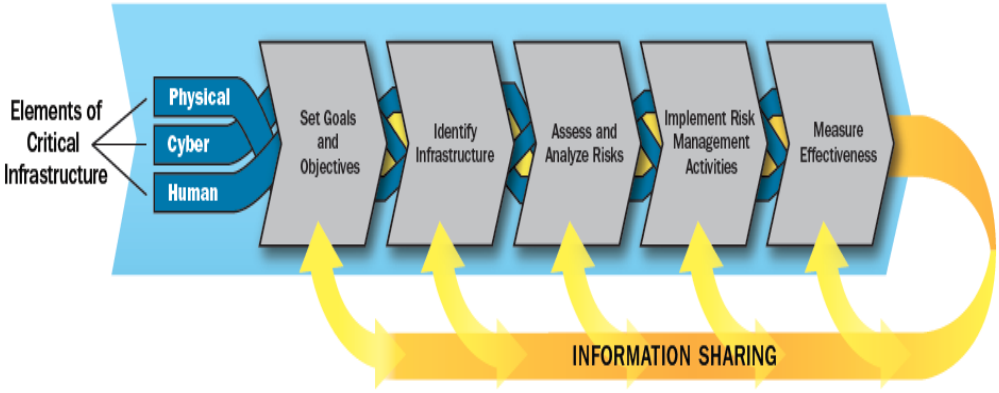
Failure / Technical

- Technical failure
- Mechanical failure
- Software failure
- Operator error
- Process / procedure failure
- Structural failure (e.g., Bridge collapse, Mine collapse, Dam collapse / failure, Water main failure)
- Dependent CI disruption /failure (i.e. failure in provision of critical services or products in the information & communication technology, finance, energy, food, safety, government, health, manufacturing, transportation or water sectors) [21]. The above list of types of threatening factors is certainly not permanent and complete. It is always possible to accuse unexpected situations (and the combination of the above) that cause threats to critical infrastructure, and therefore more effectively address risks and threats to critical infrastructure requires the division of critical infrastructure elements into categories or sectors as lepers image No.1. [22]

[21] Risk Management Guide for Critical Infrastructure Sectors, Public Safety Canada, а согласно ISO 31000 International Standard: "Risk Management – Principles and guidelines on implementation"

[22] Risk Management Guide for Critical Infrastructure Sectors, Public Safety Canada, p.36, http://www.publicsafety.gc.ca/srv/msg404.aspx?aspxerrorpath=/prg/em/ci/index.aspx

Image 1



One of the more important documents of the United States in terms of protection of critical infrastructure, which integrates a number of activities designed to enhance the security of critical infrastructure, is the NIPP - National Infrastructure Protection Plan. According to this plan, critical infrastructure is divided into 16 critical infrastructure sectors:

- Chemical sector, which can be divided into five sub-sectors, depending on the final manufactured product:
  - Basic chemicals
  - Specialty chemicals
  - Agricultural chemicals
  - Pharmaceuticals
  - Consumer products
- Communication sector, which is a critical since it provides "enabling functions" on all other sectors, and in particular to:
- The energy sector which allows operation of relay stations, central servers and other important communication devices;
- Sector of Information Technology that provides critical control systems and services as well as Internet infrastructure;
- The financial services sector that relies on communication for transmission of transactions and functioning of financial markets,
- Emergency services.

- Sector for dams, which consists of funds that include projects for dams, hydropower facilities, dikes, dams, barriers to hurricanes, tailings and other industrial waste, and other similar facilities for retention and control of water;
- Emergency Sector, which is a system of prevention, preparedness, response and recovery components, and is the first national line to prevent and mitigate the risk of terrorist attacks, accidents caused by human factors and natural disasters;
- The financial services sector, a vital component of critical infrastructure;
- Government buildings and facilities sector,
- Information Technology sector, which is of paramount importance to the nation's security, economy, and public health and safety,
- Transportation systems sector, which is divided into seven sub-sectors: aviation, highway infrastructure, maritime transport system, mass transit and rail, gas systems, rail freight and postal shipments
- Commercial Building Sector;
- Critical manufacturing sector;
- Defense industrial base sector;
- Energy sector;
- Food and Agriculture sector;
- Healthcare and Public Health Sector
- Nuclear reactors, materials, and waste sector
- Water and wastewater systems sector[23]

The subject of interest and analysis, although last in the list of specified sectors, will be water supply and wastewater. The plan to protect the water supply is specially prepared annex of the Plan for the Protection of National Infrastructure. The three attributes that are crucial for the water users are, getting the required amount of water at any time, water safe to use and the required pressure.

Water supply systems are not independent systems but interdependent with other infrastructure. For example, in order to submit water to the end users we will need electricity, information technology, communications etc. This interdependence gives sufficient degree of critical necessity for taking appropriate preventive measures. There are

[23] National Infrastructure Protection Plan, преземено на 20.07.2015 од http://www.dhs.gov/critical-infrastructure-sectors

several cases where the water supply system was the target. For example, closing the valves of the Lipkovo Lake in 2001 left the city of Kumanovo longer periods without water. In 2014, Ukraine shut valves to North Crimean canal through which the river Dnieper supplies water to the Crimean peninsula. On July 12 this year in Pristina, police closed water supply system because of suspected bioterrorist attack on the lake Badovci (this reservoir provides 40% of drinking water in Pristina). Skopje is supplied with water through Rasche and well system Nerezi-lepenec. Rasche by its location (17 km west of Skopje) and a capacity of four cubic meters per second attracts attention. Therefore, it is first necessary functional theoretical model for the analysis and assessment of risks and the vulnerability of the water supply infrastructure critical element of specific threats.

The first step in analyzing and assessing risks is identifying risks. This step in the assessment of risks should it identify all the threats and dangers that can harm this critical infrastructure element. Initially, we should take into account all the analysis of operational documents, threats from organizational nature, vulnerability and criticality assessment. Based on an analysis it is necessary to draw up a list or register of risks that are possible to occur. From the list of risks provided, it is necessary to identify those with the highest priority on which we will develop further evaluation. This evaluation would include a description of the risks, the source of risk, threat or danger that may cause the risk, area where the water supply would be affected by a particular risk, the causes of risks and their priorities, existing measures and means to deal with specific risks. Besides the above basic procedures, additional analysis can be applied to analysis of existing threat assessments, historical records of natural disasters, accidents or attacks, scientific models or theories, experience and consultations with experts in a specific field, and so on. The evaluation of risks to the water supply system should result in a decision for tolerable and acceptable level of risk (unlikely with minor threats) or prioritization of risk by determining the specific measures to prevent or prepare adequate protocols or standard operating procedures for dealing with threats and ex ante crises occurred.

Conclusion

Theoretical approach to the analysis and assessment of the risks inevitably leads to the establishment of certain more or less successful practical models. The experience of countries, especially those that are more exposed to specific threats against critical

infrastructure are different and strongly influence the dynamics of the creation of the model and its success. In general, we can conclude that the theoretical approach underlying guidelines for successful analysis and risk assessment in relation to all types' threats and reference objects of security aimed at avoiding damage with less resources used. This as a determinant of attitudes toward the practical approach is more or less difficult task. Above all, the intensity of the threats is very different as well as their probability and vulnerability of the object of protection. Especially specific is the threat to critical infrastructure, which could pose a high-level risk with long term and devastating consequences for the whole society.

In this context, pragmatic approach to critical infrastructure protection requires as possible assessment that is more detailed, analysis, and evaluation of the anticipated standard operating procedures and their success. When it comes to practical application of the assessment and analysis of risks and threats to specific critical infrastructure in the Republic of Macedonia or taken example for the water supply system of the City of Skopje, we must conclude that it is not present. As much as we try not to be too harsh in this conclusion, practical knowledge and investment in modern technology and systems for the protection of this important reference object of security is low. This implies that neither based on theoretical knowledge, nor based on practical experiences of other countries does not exist a special model and specifically structured operational procedures for the protection of critical infrastructure of this kind in the Republic of Macedonia.

The recommendations necessary to apply in order to establish an appropriate practical model for the protection of critical infrastructure in the country, and model which will allow an adequate response to institution at least to several specific threats may be related to several aspects:

1. Physical protection of facilities for water supply
2. Predicting the inclusion of alternative sources of water supply that will provide the minimum required drinking water
3. Use of SCADA systems for managing water (despite continued economic benefit in preventing water loss will allow prevention of mechanical closure of supply and control the entire electronic system)
4. Prediction of operational measures and procedures for rapid response in the event of a threat to the system, i.e. the conservation of the water supply system (this involves the system to function at minimum necessity without the presence of personnel who will control and will also be protected by outside impacts).

All these recommendations actually require extensive and detailed analysis of risks and threats to critical infrastructure, in this case water supply system and powerful predictive analysis of risks and vulnerability of infrastructure under permanent monitoring of threats. The consequences of the threat to critical infrastructure, each type of infrastructure, especially not having any assessment of the risks and threats or provided operating procedures for operation of the institutions and at the slightest threat can end up causing great harm. Thus, it is necessary to bear in mind that the threat of specific infrastructure facility or institution will necessarily have a negative effect on others, which of course in the complex social system are interconnected. This connection only increases the vulnerability of society and citizens, which in base of contemporary security paradigm is a key reference object of protection, and in this context, it is necessary to assess the vulnerability of a particular risk and threat.

Bibliography

1. B. Bognar, „The process of critical infrastructure protection", AARMS, Budapest, 2009
2. James F.Broder , „Risk Analysis and the security survey" , Second Edition, Elsevier science, Burlington, 2000
3. Douglas Landoll, "The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments", CRC Press, New York, 2011
4. Moteff J. and Parfomak P., „Critical Infrastructure and Key Assets: Definition and Identification", Congressional Research Service - The Library of Congress, Washington D.C., 2004
5. Лидија Георгиева, "Менаџирање на ризици", Филозофски факултет, Скопје, 2006
6. Carl, A.Roper, "Risk Management for Security Professionals", Butterworth Heinemann, Burlington, 1999
7. Risk Management Guide for Critical Infrastructure Sectors, Public Safety Canada, a согласно ISO 31000 International Standard: "Risk Management – Principles and guidelines on implementation"

8. Commission of the EU Communities, "Critical infrastructure protection in the fight against terrorism", Brussels, 2004
http://www.dhs.gov/critical-infrastructure-sectors
9. http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.p