ISSN 1857-7172

SECURITY DIALOGUES

Vol. 10, Number 1-2, 2019

ФИЛОЗОФСКИ ФАКУЛТЕТ - СКОПЈЕ
ИНСТИТУТ ЗА БЕЗБЕДНОСТ, ОДБРАНА И МИР

Година 10, Број 1-2, 2019.

БЕЗБЕДНОСНИ ДИЈАЛОЗИ

СПИСАНИЕ ОД ОБЛАСТА НА БЕЗБЕДНОСТА, ОДБРАНАТА И МИРОВНИТЕ НАУКИ

www.fzf.ukim.edu.mk
www.sd.fzf.ukim.edu.mk

БЕЗБЕДНОСНИ ДИЈАЛОЗИ / SECURITY DIALOGUES

ISSN 1857-7172
eISSN 1857-8055
Година 10, Број 1-2, 2019/Vol. 10, No. 1-2, 2019

dialogues
Security
International peer reviewed journa

ISSN 1857-7172
eISSN 1857-8055
OPEN ACCESS
http:// sd.fzf.ukim.edu.mk

Издавач/Publisher

Филозофски факултет – Скопје/Faculty of Philosophy – Skopje
Институт за безбедност, одбрана и мир/Institute of security, defence and peace
Уредувачки одбор/Editorial board: тел. (+389) 2 3066 232, email sd@fzf.ukim.edu.mk

Компјутерска обработка: МАР-САЖ

Печати: МАР-САЖ   Тираж: 150

Ss. Cyril & Methodius University in Skopje, Faculty of Philosophy - Institute of Security, defence and peace has entered into an electronic licensing relationship with EBSCO Publishing, the world's most prolific aggregator of full text journals, magazines and other sources. The full text of Security Dialogues can be found on the following EBSCO Publishing's databases collections: International Security & Counter-Terrorism Reference Center.

CONTENTS

005.334:355.45 - 005.52:005.334(1-4)(083.92) Review

NATIONAL PLAN FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE - A CONDITION FOR PROVIDING A COORDINATED APPROACH IN ESTABLISHING NATIONAL GOALS AND PRIORITIES FOR PROTECTING KEY RESOURCES

Grozdanka Naumovska,
Head of section for prevention and planning of technological and complex disasters**,** Sector for prevention, planning and development, Protection and Rescue Directorate - Skopje,
E-mail: grozdanka.naumovska@gmail.com

Aleksandar GLAVINOV, PhD
Ministry of defense, University "Goce Delchev "– Shtip,
Military Academy "General Mihailo Apostolski" – Skopje,
E-mail: aleksandar.glavinov@ugd.edu.mk

Abstract: The National Plan for the Protection of Critical Infrastructure, created on the basis of specific sector support plans, will provide continuously secure basic services to the nation and the community.

Consequently, proactive and coordinated efforts through various means, networks and systems to strengthen the safe functioning, maintain and strengthen their resistance are vital to public confidence and the security, prosperity and well-being of the nation.

Critical infrastructure is diverse and complex, from organizational structures, models, distribution networks and interdependent functions of systems, both in physical space and in cyberspace, which includes respect for a variety of regulations on all fields.

Critical infrastructure must be safe and able to withstand the various effects of all hazards on national security, economic stability, public health or a combination of these and rapid recovery. In order to achieve this, it is necessary to integrate the national system for prevention, protection, mitigation, response and recovery in order to reduce vulnerability, minimize the consequences, identify and anticipate threats.

The aim of this paper is to determine the legal position or the gap with experience and good practice in the developed countries to offer a model of protection of the critical infrastructure in the Republic of North Macedonia.

Keywords: Critical infrastructure, National Plan for Critical Infrastructure Protection, Specific Sector Support Plans, Key Resources

Introduction

Modern trends at new techniques and technologies provide a much easier flow of information, goods, people, which increases the vulnerability to national security of the community. On the other hand, climate change, the destructive effect of man in nature, cause reduces resistance to natural and technical-technological disasters. New threats such as migration crises, cyber-crime, extreme terrorism and hybrid threats are demanding new mechanisms and models to strengthen the critical infrastructure security in order to preserve the integrity, security and social and economic stability of the community.

By analyzing the models for protecting critical infrastructure and experiences in developed countries, we will consider the benefits that can be applied in creating policies and strategies for protecting critical infrastructure in the Republic of North Macedonia.

1. Terminology, definition and infrastructure division

The term "infrastructure" was first introduced in the 19th century by Swiss military theorist Antoine-Henry Jomini, who potentiates the strategic and operational significance of the leadership of the military actions. By the middle of the 20th century, the term "infrastructure" is a military term that denotes the territorial organization of the system for maintaining and functioning of the army. Later "infrastructure" begins to be used in economic theory and in management theory. Currently, it is widely applied in the computer science, economic geography and security researc

There are many definitions of the term infrastructure. Among them are:

Infrastructure is a basic physical and organizational structure that needs of a society, environment, organization or institution to function smoothly within its frameworks.

Infrastructure is a set of interconnected structural elements that provide a framework for support for the overall functioning of one community.

In **civilian terms**, **infrastructure** is defined as a term for which is made partial assessment of the development of a country.

From **a functional point of view**, **infrastructure** facilitates the production and distribution of goods and services to consumers (roads, plumbing, electricity, etc.), as well as enabling the use of basic social services (schools, ambulances, etc.).

The infrastructure can be divided into:

Rigid (heavy, physical) infrastructure - refers to large physical networks that are need for the functioning of a country, institution, organization, etc.

The rigid infrastructure is divided into:

- transport (streets, roads, bridges, tunnels, airports, ports, canals, etc.),
- energy (electricity network, gas pipelines, oil pipelines, lines for transportation of ore, etc.),
- water supply network (sewage network, sewerage, sewage drainage, etc.) and
- communication (Internet, telephony, television, etc.).

Soft (service) infrastructure - refers to all institutions that are needed to maintain economic, health and cultural and social standards of a state. Soft infrastructure includes physical assets such as highly specialized facilities and equipment, rules and regulations that regulate various systems, the financing of these systems, and so on.

The soft infrastructure can be divided into:

- state (state institutions, judiciary, police, fire protection, etc.),
- economic (economic zones, financial and banking systems, etc.),
- social (health care, school system, social networks, etc.),
- cultural, sports and recreational (parks, museums, libraries, tourist facilities, etc.) and
- military infrastructure.

The term **military infrastructure** is used for all built and permanent installations necessary for the smooth operation and support of the military forces whether they are in the barracks, whether they are deployed in another country or perform certain operations.

The term Key Resources - refers on publicly or privately controlled resources essential for minimal business operations of the economy and the government.

2. Appearance and models for assessing the protection of critical infrastructure

At the end of the 20th century, the term critical infrastructure protection (CCI) emerged, which constitutes an essential component of the security policy of many countries, especially in the NATO and EU member states.

The protection of critical infrastructure is connected, on the one hand, with the processes of globalization, and on the other, with the fight against international terrorism. There is a direct link between the threat of terrorism and the protection of critical infrastructure.

The immediate cause of activating the critical infrastructure protection policy is the terrorist attacks in the United States since September 11, 2001, as well as the terrorist attacks in Madrid in 2004 and London in 2005.

The second main reason is the development and control of major infrastructure projects for the transfer of oil, gas and other strategic raw materials.

2.1. Models for assessing and protecting critical infrastructure in the US, UK and Canada

After the terrorist attacks of September 11, 2001 in the United States, critical infrastructure protection is becoming a top priority. Initially, this activity is being implemented by the FBI National Infrastructure Protection Center. In 2002, the critical infrastructure protection is carried out by the **Department of Homeland Security (DHS)** and is regulated by the Homeland Security Act. Most of the obligations are implemented by the Directorate for “Information Analysis and Protection of Infrastructure” within the Ministry of Homeland Security.

The Department of Homeland Security in collaboration with other owners and operators of critical infrastructure should develop a unique methodology for identifying objects, systems and functions with criticality from the national level in order to establish the protection priorities and build a complete database of these critical objects, systems and functions. After drawing up the list, a process of assessment of each element is carried out by teams of experts which carry out field research on individual elements. Annually in the United States estimates are made at about 300 sites of critical infrastructure.

In the UK, critical infrastructure protection activities are carried out by two organizations: **The Governmental Coordination Center for National Infrastructure Security** and **The Advisory Council on Information Security** (it is a public-private organization). United Kingdom, unlike the United States, has no full conception of the assessment and protection of critical infrastructure. This activity is implemented by the existing Ministries in their own departments with coordinated activity of the mentioned authorities.

In Canada within the Ministry of Defense in 2000 was established an expert group for the protection of critical infrastructure, carrying out a comprehensive overview of the national critical infrastructure. At the same time, Canada has a private organization, **CANCERT (Canadian Computer Emergency Response Team)**, which focuses its activities on protecting critical infrastructure information.

3. Analyzing EU normative documents and EU policy on the protection of critical infrastructure

EU policy of the protection of critical infrastructure is developing very dynamically after 2004 in the context of the fight against international terrorism. From an institutional point of view, the EU's policy of protecting critical infrastructure is coordinated by the European Commission's Directorate-General for Justice, Freedom and Security.

In November 2005. The European Commission accepts so-called "The Green Paper for the European Program for the Protection of Critical Infrastructure" and for the first time at Community level defines the term "critical infrastructure" as a system of facilities, services and information systems, whose braking, defect functioning or destruction would be severely negative impact on the health and safety of the population, the environment, the national economy or the efficient functioning of the state administration. Apart from the term "national critical infrastructure", the authors of the Green Paper promote the term "European critical infrastructure".

Based on the Green Paper in 2006, the EU launched the European Program for Critical Infrastructure Protection (EPCIP), and in the process of developing the Critical Infrastructure Warning Information System (CIWIN).

The other key EU policy paper on critical infrastructure protection is the proposal for a Council Directive from December 2006 on the recognition and establishment of European critical infrastructure and the assessment of the need to improve its protection.

The Directive establishes a new list and recommends a list of sectors of critical infrastructure. The following sectors are listed: Energy Sector; Sector black industry; Sector for Information and Communication Technologies; Water Supply Sector; Food Insurance Sector; Health Sector; Sector Finance; Transport Sector; Sector for the chemical industry; Space Capacity and

Scientific Capacity. This list of sectors is not final and subject to specification. EU regulations includes significant number of directives and provisions for activities in 5 of the critical infrastructure sectors - information technology, health, transport, chemical and nuclear sectors. These regulations provide measures for protection of the relevant sector, but there are no criteria for assessing the criticality of infrastructure facilities in the sectors. EU sectoral laws have a bearing on the development of disaster protection plans faster.

4. National Security Policy and Building Resilience to Critical Infrastructure

National Security Policy and Building Resilience to Critical Infrastructure is the first step of the community to counter the physical and cyber threats. This policy clearly defines and establishes responsibility among national, regional and local entities and "owners" of public and private critical infrastructure and operators. The policy points to a clear link between the structures mentioned above, their function, roles and responsibilities in order to enhance the security and resilience of national essential functions.

Through policy, it is necessary to analyze all threats that can affect national critical infrastructure, economic stability, public health and safety, and their combination. A great effort is being made to reduce vulnerability, minimize the consequences, identify new risks, enhance response, and recovery.

Three important strategic priorities are imperative in the policy:

- clear functional realities and links between government departments and a mutually united effort in the security and resilience of critical infrastructure;
- enabling efficient exchange of information by identifying the base data and requests for the Government; and
- conducting an integrated and analytical function in informing for planning decisions and undertaking activities related to critical infrastructure.

In order to implement this policy, it has to implement of international regulation in national legal solutions.

In principle, it is useful one agency or line ministry to play the role of a national coordinator, which includes:

- Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences, in coordination with Agency and other national departments and agencies;
- Maintain national critical infrastructure centers that shall provide a situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure;
- In coordination with Agency and other national departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure;

- Conduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the Agency and in collaboration with regional and local entities and critical infrastructure owners and operators;
- Coordinate National Government responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities;
- Support the Attorney General and law enforcement agencies with their responsibilities to investigate and prosecute threats to and attacks against critical infrastructure;
- Coordinate with and utilize the expertise of Agency and other appropriate National departments and agencies to map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies; and
- Report annually on the status of national critical infrastructure efforts as required by statute.

4.1. Sector-Specific Agencies

Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that benefit from an identified Sector-Specific Agency that has institutional knowledge and specialized expertise about the sector. Recognizing existing statutory or regulatory authorities of specific National departments and agencies, and leveraging existing sector familiarity and relationships, Sector-Specific Agency shall carry out the following roles and responsibilities for their respective sectors:

1. As part of the broader national effort to strengthen the security and resilience of critical infrastructure, coordinate with the National Agency/ Ministry and other relevant national departments and agencies and collaborate with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with regional and local entities;
2. Serve as a day-to-day national interface for the dynamic prioritization and coordination of sector-specific activities;
3. Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations;
4. Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate; and
5. Support the Head / or other person from Agency/ Ministry statutorily required reporting requirements by providing on an annual basis sector-specific critical infrastructure information.

The term "Sector-Specific Agency" (SSA) means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

5. National Plan for Critical Infrastructure Protection - Model of the US Department of Homeland Security

The National Plan takes into account the varying risk management perspectives of the public and private sectors, where government and private industry have aligned, but not identical, interests in securing critical infrastructure and making it more resilient. It leverages comparative advantages of both the private and public sectors to the mutual benefit of all. The National Plan is organized in the following manner:

1. Vision, Mission, and Goals – Outlines the vision, mission, and goals for the critical infrastructure community.
2. Critical Infrastructure Environment – Describes the policy, risk, and operating environments, as well as the partnership structure within which the community undertakes efforts to achieve goals aimed at strengthening security and resilience.
3. Core Tenets – Describes the principles and assumptions that underpin this National Plan.
4. Collaborating to Manage Risk – Describes a common framework for risk management activities conducted by the critical infrastructure community in the context of national preparedness.
5. Call to Action – Calls upon the critical infrastructure community (respective of authorities, responsibilities, and business environments) to take cross-cutting, proactive, and coordinated actions that support collective efforts to strengthen critical infrastructure security and resilience in the coming years.

5.1. Vision, Mission, and Goals

- Vision - A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.
- Mission - Strengthen the security and resilience of the Nation’s critical infrastructure, by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community.
- Goals
- Access and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;

- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services;
- Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk informed decision making; and
- Promote learning and adaptation during and after exercises and incidents.

5.2. Critical Infrastructure Environment

5.2.1. Key Concepts

The key concepts described below provide context for this critical infrastructure environment. An understanding of these key concepts influences the state of critical infrastructure and shapes the community's approach to ensuring security and resilience.

- Critical infrastructure represents "systems and assets, whether physical or virtual, so vital to the community 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."2 The National Plan acknowledges that the Nation's critical infrastructure is largely owned and operated by the private sector; however, national and regional and local governments also own and operate critical infrastructure, as do foreign entities and companies.
- Security as "reducing the risk to critical infrastructure by physical means or defens[ive] cyber measures to intrusions, attacks, or the effects of natural or manmade disasters." There are several elements of securing critical infrastructure systems, including addressing threats and vulnerabilities and sharing accurate information and analysis on current and future risks. Prevention and protection activities contribute to strengthening critical infrastructure security.
- Resilience, is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions...[it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." Having accurate information and analysis about risk is essential to achieving resilience. Resilient infrastructure assets, systems, and networks must also be robust, agile, and adaptable. Mitigation, response, and recovery activities contribute to strengthening critical infrastructure resilience.
- Security and resilience are strengthened through risk management. Risk refers to the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood [a function of threats and vulnerabilities] and the associated consequences;" risk management is the "process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost."3
- Partnerships enable more effective and efficient risk management. Within the context of this National Plan, a partnership is defined as close cooperation between parties having common interests in achieving a shared vision. For the critical infrastructure community,

leadership involvement, open communication, and trusted relationships are essential elements to partnership.

2 USA Patriot Act of 2001 § 1016(e). 3 U.S. Department of Homeland Security, DHS Risk Lexicon – 2010 Edition, September 2010, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

5.2.2. Risk Environment

The risk environment affecting critical infrastructure is complex and uncertain; threats, vulnerabilities, and consequences have all evolved over the last 10 years. For example, critical infrastructure that has long been subject to risks associated with physical threats and natural disasters is now increasingly exposed to cyber risks, which stems from growing integration of information and communications technologies with critical infrastructure operations and an adversary focus on exploiting potential cyber vulnerabilities.

The Strategic National Risk Assessment4 (SNRA) defines numerous threats and hazards to homeland security in the broad categories of adversarial/human-caused, natural, and technological/ accidental threats. Critical assets, systems, and networks face many of the threats categorized by the SNRA, including terrorists and other actors seeking to cause harm and disrupt essential services through physical and cyber attacks, severe weather events, pandemic influenza or other health crises, and the potential for accidents and failures due to infrastructure operating beyond its intended lifespan. The potential for interconnected events with unknown consequences adds uncertainty in addition to the known risks analyzed as part of the SNRA.
It also identifies 16 critical infrastructure sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

5.2.3. Policy Environment

The National Plan is aligned with the goal of National Preparedness, of "a secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk." These five mission areas are central to a comprehensive approach for enhancing national preparedness and critical infrastructure risk management activities across all five mission areas contribute to achieving the National Preparedness Goal. In addition, the National Plan is consistent with the National Planning Frameworks and Interagency Operational Plans developed pursuant to National Preparedness. The scope of the National Plan is not meant to and does not alter the implementation and execution of prevention activities, as described in the Prevention Federal Interagency Operational Plan. The National Plan scope comprises activities that often support and abut prevention activities designed to avoid, prevent, or stop an imminent threat or actual attacks.

5.2.4. Operating Environment

The Nation's critical infrastructure has become much more interdependent, continuing to move from an operating environment characterized by disparate assets, systems, and networks to one in which cloud computing, mobile devices, and wireless connectivity have dramatically changed the way infrastructure is operated. Interdependencies may be operational (e.g., power required to operate a water pumping station) or physical (e.g., collocated infrastructure, such as water and electric lines running under a bridge span). Interdependencies may be limited to small urban or rural areas or span vast regions, crossing jurisdictional and national boundaries, including infrastructure that require accurate and precise positioning, navigation, and timing (PNT) data. PNT services are critical to the operations of multiple critical infrastructure sectors and are vital to incident response.

5.2.5. Partnership Structure

Voluntary collaboration between private sector owners and operators (including their partner associations, vendors, and others) and their government counterparts has been and will remain the primary mechanism for advancing collective action toward national critical infrastructure security and resilience. The Federal Government must make economic calculations of risk while also considering many non-economic values, such as privacy concerns, when addressing its role in national and homeland security. As a result, government may have a lower tolerance for security risk than a commercial entity. Both perspectives are legitimate, but in a world in which reliance on critical infrastructure is shared by industry and government and where industry may be on the front lines of national defense, such as in a cyber attack, a sustainable partnership must be developed to address both perspectives.

The National Plan organizes critical infrastructure into 16 sectors and designates a Federal department or agency as the lead coordinator—Sector-Specific Agency (SSA)—for each sector (refer to Appendix B for the roles and responsibilities of SSAs). The sector and cross-sector partnership council structures described in previous NIPPs remain the foundation for this National Plan.

5.3. Core Tenets

The National Plan establishes seven core tenets, representing the values and assumptions the critical infrastructure community should consider (at the national, regional, local, and owner and operator levels) when planning for critical infrastructure security and resilience.

1. Risk should be identified and managed in a coordinated and comprehensive way across the critical infrastructure community to enable the effective allocation of security and resilience resources.
2. Understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing critical infrastructure security and resilience.
3. Gaining knowledge of infrastructure risk and interdependencies requires information sharing across the critical infrastructure community
4. The partnership approach to critical infrastructure security and resilience recognizes the unique perspectives and comparative advantages of the diverse critical infrastructure community.
5. Regional and local partnerships are crucial to developing shared perspectives on gaps and actions to improve critical infrastructure security and resilience.
6. Infrastructure critical to the United States transcends national boundaries, requiring cross-border collaboration, mutual assistance, and other cooperative agreements.
7. Security and resilience should be considered during the design of assets, systems, and networks.

5.4. Collaborating To Manage Risk

The national effort to strengthen critical infrastructure security and resilience depends on the ability of public and private sector critical infrastructure owners and operators to make risk-informed decisions on the most effective solutions available when allocating limited resources in both steady-state and crisis operations. Therefore, risk management is the cornerstone of the National Plan and is relevant at the national, regional, State, and local levels. National, regional, and local resilience depend upon creating and maintaining sustainable, trusted partnerships between the public and private sector. While individual entities are responsible for managing risk to their organization, partnerships improve understanding of threats, vulnerabilities, and consequences and how to manage them through the sharing of indicators and practices and the coordination of policies, response, and recovery activities. Critical infrastructure partners manage risks based on diverse commitments to community, focus on customer welfare, and corporate governance structures. Risk tolerances will vary from organization to organization, as well as sector to sector, depending on business plans, resources, operating structure, and regulatory environments. They also differ between the private sector and the government based on underlying constraints. Different entities are likely to have different priorities with respect to security investment as well as potentially differing judgments as to what the appropriate point of risk tolerance may be. Private sector organizations generally can increase investments to meet their risk tolerances and provide for their community of stakeholders, but investments in security and resilience have legitimate limits. The government must provide for national security and public safety and operates with a different set of limits in doing so. Finding the appropriate value proposition among the partners requires understanding these differing perspectives and how they may affect efforts to set joint priorities. Within these parameters, critical infrastructure security and resilience depend on applying risk management practices of both industry and government, coupled with available resources and incentives, to guide and sustain efforts.

Specifically, the three elements of critical infrastructure (physical, cyber, and human) are explicitly identified and should be integrated throughout the steps of the framework, as appropriate. In addition, the updated framework consolidates the number of steps or "chevrons" by including prioritization with the implementation of risk management activities. Prioritization of risk mitigation options is an integral part of the decision-making process to select the risk management activities to be implemented. Finally, a reference to the feedback loop is removed and instead, the framework now depicts the importance of information sharing throughout the entire risk management process. Information is shared through each step of the framework, to include the "measure effectiveness" step, facilitating feedback and enabling continuous improvement of critical infrastructure security and resilience efforts.

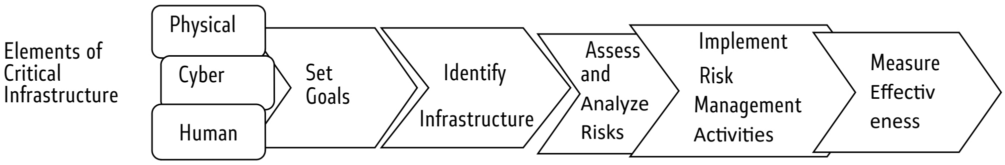

Figure 1 – Critical Infrastructure Risk Management Framework.

The critical infrastructure risk management framework is designed to provide flexibility for use in all sectors, across different geographic regions, and by various partners. It can be tailored to dissimilar operating environments and applies to all threats and hazards. The risk management framework is intended to complement and support completion of the Threat and Hazard Identification and Risk Assessment (THIRA) process as conducted by regional, SLTT, and urban area jurisdictions to establish capability priorities.[85]

The critical infrastructure community shares information throughout the steps of the risk management framework to document and build upon best practices and lessons learned and help identify and fill gaps in security and resilience efforts. It is essential for the community to share risk information, also known as risk communication, which is defined as the exchange of information with the goal of improving risk understanding, affecting risk perception, and/or equipping people or groups to act appropriately in response to an identified risk.

Critical infrastructure risks can be assessed in terms of the following:

- Threat – natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

[85] Comprehensive Preparedness Guide 201: Threat and Hazard Identification and Risk Assessment, Second Edition cites infrastructure owners and operators as sources of threat and hazard information and as valuable partners when completing the THIRA process.

- Vulnerability – physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
- Consequence – effect of an event, incident, or occurrence.

Decision makers prioritize activities to manage critical infrastructure risk based on the criticality of the affected infrastructure, the costs of such activities, and the potential for risk reduction. Some risk management activities address multiple aspects of risk, while others are more targeted to address specific threats, vulnerabilities, or potential consequences. These activities can be divided into the following approaches:

- Identify, Deter, Detect, Disrupt, and Prepare for Threats and Hazards
- Reduce Vulnerabilities
- Mitigate Consequences

5.5.Call to Action: Steps to Advance The National Effort

This Call to Action guides efforts to achieve national goals aimed at enhancing national critical infrastructure security and resilience. These activities will be performed collaboratively by the critical infrastructure community. Federal departments and agencies, engaging with SLTT, regional, and private sector partners—taking into consideration the unique risk management perspectives, priorities, and resource constraints of each sector—will work together to promote continuous improvement of security and resilience efforts to accomplish the tasks below. The actions listed in this section are not intended to be exhaustive nor is it anticipated that every sector will take every action. Instead, this section is intended as a roadmap to guide national progress while allowing for differing priorities in different sectors. As such, the actions listed below provide strategic direction for national efforts in the coming years. Call-out boxes throughout this section identify linkages between the Call to Action activities and the national goals presented in section 2.

It include:

- Build upon Partnership Efforts:
- Innovate in Managing Risk:
- Focus on Outcomes:

6. Special Sector Plans

Each sector agency has developed a specific plan detailing the application of the NIPP framework to the unique characteristics and risk of their sector.

Special Sector Plans (SSPs) provide the way NIPP is implemented in all key infrastructure and key resources (CICRs) sectors as well as the national framework for each sector to respond to its unique characteristics and risk. This coordinated approach applies federal resources and resources in the most effective way to manage risk.

Sector - Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environment Protection Agency	Drinking Water and Water Treatment Systems
Department of Homeland Security Office of infrastructure Protection	Chemical Commercial Facilities Dams Emergency Services Nuclear Reactors, Materials and Waste
Department of Homeland Security Office of Cyber Security and Telecommunications	Information Technology Communications
Department of Homeland Security Transportation Security Administration	Postal and Shipping
Department of Homeland Security Transportation Security Administration United States Coast Guard	Transportation Systems
Department of Homeland Security Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

Table 1. Sector- Specific Agency - Critical Infrastructure/Key resources Sector

As part of the National Infrastructure Protection Plan, the public and private sector partners in each of the 16 critical infrastructure sectors and the state, local, tribal, and territorial government community have developed a Sector-Specific Plan that focuses on the unique operating conditions and risk landscape within that sector. Developed in close collaboration with federal agencies and private sector partners, the Sector-Specific Plans are updated every four years to ensure that each sector is adjusting to the ever-evolving risk landscape.

SSPs are tailored to address the unique characteristics and risk landscapes of each sector while also providing consistency for protective programs, public and private protection investments, and resources:

- Define sector security partners, authorities, regulatory bases, roles and responsibilities, and interdependencies;
- Establish or institutionalize already existing procedures for sector interaction, information sharing, coordination, and partnership;

- Establish the goals and objectives, developed collaboratively with security partners, required to achieve the desired protective posture for the sector;
- Identify international considerations; and
- Identify the sector-specific approach or methodology that Sector-Specific Agencies (SSAs), in coordination with the Department of Homeland Security (DHS) and other security partners, will use to implement risk management framework activities consistent with the NIPP.

7. Conclusion

Republic of North Macedonia has not yet established a critical infrastructure regulation, for many reasons:

- which institution to be competent,
- does that institution have staff and facilities to brings and solves all issues,
- existing methodologies of risk assessment is not an appropriate (one from CMC, one from PRD)
- existing Plan for protection and rescue from natural and other disasters are not national in the right sense, it is more institutional,
- overlapping in regulation from different entities

We can conclude that is good opportunity to make clarify and finally to make more effort in prepare policy of critical infrastructure, new regulation, use the best practices for planning process, with clear rules and responsibilities, with unique approach on national, regional and local level with good cooperation and collaboration with private business sector and operators. It is good opportunity to separate prevention and preparedness in existing documents with amending or prepare a new. Plan for protection and rescue will be good to divide in two separate national plans, one for protection of critical infrastructure and another for preparedness, emergency response plan. In this case will be more easy to coordinate and collaborate in two deferent scopes, prevention and preparedness. This is necessary, to integrate the national system for prevention, protection, mitigation, response and recovery in order to reduce vulnerability, minimize the consequences, identify and anticipate threats.

Bibliography

1. Center for Security Studies “Crisis and Risk Network Critical Infrastructure Protection”, Centre for Security Studies (CSS). 2009.ETH Zürich.
2. Government of Canada Threats to Canada`s Critical Infrastructure available at http://www.publicsafety.gc.ca/prg/em/ccirc/_fl/03-001-eng.pdf
3. Idzorek, T. Infrastructure and Strategic Asset Allocation: Is Infrastructure an Asset Class? Ibbotson a Morningstar Company. 2009
4. Jenkins, B. The Potential of Nuclear Terrorism. Santa Monica, CA Rand.1977

5. Homeland Security Presidential Directive-7 "Critical Infrastructure Identification, Prioritization and Protection available at http://www.dhs.gov/xabout/laws/ gc_ 1214597989952,shtm.
6. Moteff, J and Parfomak, P. Critical Infrastructure and Key Assets: Definition and Identification. Conyresncil on Public signal Research Service-The Library of Congress. 2004.
7. National Council on Public Works Improvement. Fragire Foundations. A report on America`s Public Works, Final Report to the President and Congress. Washington DC. 1988.
8. Protective Critical Infrastructure in the EU available at http://www.ceps.eu/ceps/download/4061
9. Smith, A. Stirling, A. and Berkhout, F. The governance of sustainable socio-technical transitions. Research Policy. 2005
10. Spain Threatens Iraq Troop Pull-out, 2004. Story from BBC News: http://news.bbc.co.uk/go/pr/fr/-z/hi/europe/3512144.stm.
11. United Nations. "International Strategy for Disaster Reduction". Available at http://www.unbrussels.org/agencies/unisdr.html.
12. Vaughan, R. and Pollard, R. Rebuilding America, Vol. I, Planning and Managing Public Work in the 1980. Council of State Planning Agencies. Washington, DC. 1984.
13. National Infrastructure Protection Plan, partnering for Critical infrastructure Security and Resilience www.dhs.gov/nipp

IN THIS NUMBER:

SIMONE BORILE
FRANK REININGHAUS
ZORAN KEKOVIĆ, DAVORKA GALIĆ
PAVEL BUČKA, RASTISLAV KAZANSKÝ
JOVAN PEJKOVSKI, MIRJANA KAEVA PEJKOVSKA
TONI MILESKI, GORDANA KAPLAN
MARIJA STOJANOVIĆ-ANĐELIĆ, DEJAN NOVAKOVIĆ
IVAN DIMITRIJEVIĆ, ANA PARAUŠIĆ
JURIS LUKASS, RAIMONDS RUBLOVSKIS
AGIM NUHIU
ELIZABETA TOMEVSKA-ILIEVSKA, TATJANA STOJANOSKA IVANOVA
NATASHA ANGELOSKA GALEVSKA, LJUPKA TRAJCEVSKA
MAJA TIMOVSKA
BORIS KRŠEV, ZDRAVKO SKAKAVAC
NIKOLA TUPANCESKI, ALEKSANDRA DEANOSKA TRENDAFILOVA
TOMISLAV TUNTEV, GJORGI ALCESKI
MIRSAD BUZAR
SANDE SMILJANOV
MILICA ĆURČIĆ, SANJA PETRONIĆ
SARA SPASOVA
ANA PARAUŠIĆ
IVAN TRAJKOV, VLADIMIR ILIEVSKI
VASKO SHUTAROV
DENKO SKALOVSKI
ŽELIMIR KEŠETOVIĆ, VELIBOR LALIĆ
SVETLANA NIKOLOSKA, MARIJA GJOSHEVA
NENAD TANESKI, DEJAN BOGATINOV
IGOR GJORESKI, TONI PETRESKI
MARJAN NIKOLOVSKI, MARJAN GJUROVSKI
ZLATAN BAJRAMOVIĆ
SASHO MITEVSKI, BLAGOJCHO SPASOV
GORAN KOVAČEVIĆ
ALEKSANDAR PAVLESKI, NIKOLCO SPASOV
ZORAN DRAGIŠIĆ, MILICA ĆURČIĆ
GROZDANKA NAUMOVSKA, ALEKSANDAR GLAVINOV

IN THIS NUMBER:

SIMONE BORILE
FRANK REININGHAUS
ZORAN KEKOVIĆ, DAVORKA GALIĆ
PAVEL BUČKA, RASTISLAV KAZANSKÝ
JOVAN PEJKOVSKI, MIRJANA KAEVA PEJKOVSKA
TONI MILESKI, GORDANA KAPLAN
MARIJA STOJANOVIĆ-ANĐELIĆ, DEJAN NOVAKOVIĆ
IVAN DIMITRIJEVIĆ, ANA PARAUŠIĆ
JURIS LUKASS, RAIMONDS RUBLOVSKIS
AGIM NUHIU
ELIZABETA TOMEVSKA-ILIEVSKA, TATJANA STOJANOSKA IVANOVA
NATASHA ANGELOSKA GALEVSKA, LJUPKA TRAJCEVSKA
MAJA TIMOVSKA
BORIS KRŠEV, ZDRAVKO SKAKAVAC
NIKOLA TUPANCESKI, ALEKSANDRA DEANOSKA TRENDAFILOVA
TOMISLAV TUNTEV, GJORGI ALCESKI
MIRSAD BUZAR
SANDE SMILJANOV
MILICA ĆURČIĆ, SANJA PETRONIĆ
SARA SPASOVA
ANA PARAUŠIĆ
IVAN TRAJKOV, VLADIMIR ILIEVSKI
VASKO SHUTAROV
DENKO SKALOVSKI
ŽELIMIR KEŠETOVIĆ, VELIBOR LALIĆ
SVETLANA NIKOLOSKA, MARIJA GJOSHEVA
NENAD TANESKI, DEJAN BOGATINOV
IGOR GJORESKI, TONI PETRESKI
MARJAN NIKOLOVSKI, MARJAN GJUROVSKI
ZLATAN BAJRAMOVIĆ
SASHO MITEVSKI, BLAGOJCHO SPASOV
GORAN KOVAČEVIĆ
ALEKSANDAR PAVLESKI, NIKOLCO SPASOV
ZORAN DRAGIŠIĆ, MILICA ĆURČIĆ
GROZDANKA NAUMOVSKA, ALEKSANDAR GLAVINOV

ФИЛОЗОФСКИ ФАКУЛТЕТ
СКОПЈЕ