CRITICAL INFRASTRUCTURE

CONCEPT AND SECURITY CHALLENGES

Marina Mitrevska
Toni Mileski
Robert Mikac

FRIEDRICH EBERT STIFTUNG

MARINA MITREVSKA
TONI MILESKI
ROBERT MIKAC

CRITICAL INFRASTRUCTURE: CONCEPT AND SECURITY CHALLENGES

Skopje, 2019

Content

Preface

Around the end of this year, which marks the 70th anniversary of NATO's foundation, the Alliance member states are expected to complete their national ratifications of the NATO Accession Protocol with the Republic of North Macedonia, making it officially the latest and 30th member state of the Alliance.

Aside from producing a variety of security, as well as economic and social benefits for each member state, being part of NATO also implies a lot of hard work, commitments and obligations for each segment of Macedonian society – the citizens individually, the institutions, organizations, and everyone else. This particularly comes to the fore when it comes to the issue of improving the rule of law and the independence of the judiciary, as well as boosting the development of the education and healthcare system in the country

It is precisely for these reasons that the Friedrich-Ebert-Stiftung decided to provide its input to this process by lending its support to certain endeavours that could prove useful to both the country as a whole and the individual sets of policies it will be pursuing over the next stages of its integration into NATO. The topic of critical infrastructure protection was brought forward in this context by the group of academic authors who co-wrote this publication and, after an inclusive process involving public debates and experts presenting their views on this matter, the final version of the material on critical infrastructure protection eventually saw the light of day.

Using Croatia as an individual example, it was vital to do case studies on newer member states of the Alliance, thus drawing on the experiences and learning of their own process of integration into NATO and how they have been functioning as full-fledged member states of the Alliance. Sharing experiences and good practices in this manner will be vital at this point when the country is going through the final stage of acceding to NATO, as well as in the months and years to come after the official accession when policies will start taking shape and be put into operation.

Having been put together to provide a presentation and elaborate upon all aspects of critical infrastructure protection, as well as to encourage activities to create a national strategy and ultimately adopt a law on critical infrastructure protection in the Republic of North Macedonia, we sincerely hope that this publication will draw the interest of the expert community in the country with regard to this matter and will prove to be of particular use to the relevant institutions when dealing with it going forward.

Nita Starova
Friedrich-Ebert-Stiftung Skopje Office

Introduction

The idea of writing a book like the one in front of you, entitled ***"Critical Infrastructure: Concept and Security Challenges"*** is a bold scholarly and erudite step. We have directed our long-term scientific and research career to several premises. The first basic premise of this book begins with the concept of critical infrastructure as a general set of values and goods that are essential to the economy, the state and the society. Disruption or destruction of such values and goods could have long-term detrimental effects on the core values of the society. Consequently, when creating a modern concept of critical infrastructure protection one recognizes the need to build a coordinated approach.

The second premise that characterizes this book is aimed at showing that the security problems faced by the states today have reached a level of seriousness and urgency. In such situations, it is understandable that quick fixes and ad hoc solutions are not enough and therefore it is necessary to consider actions that will help, or require an effective way of changing the approach to critical infrastructure protection.

The third basic premise of this book is the domain of critical infrastructure protection at national level, that is, individually and for this purpose we have singled out the examples of the United States and Croatia and the polices and processes that the EU and NATO have initiated and are striving to coordinate. These experiences are deemed valuable for future directions in the creation of the critical infrastructure protection system in the Republic of North Macedonia.

In the interest of a comprehensive analysis, we have also included two eminent foreign critical infrastructure experts, namely, Richard Larkin and Matthew Vatter. Their participation in this project, through their analysis of critical infrastructure protection in the United States, adds particular importance to the book in seeking a meaningful solution in the creation of a critical infrastructure protection system in the Republic of North Macedonia.

The content of ***"Critical Infrastructure: Concept and Security Challenges"*** is systematized in six chapters.

Within the **first chapter** entitled ***"Critical Infrastructure: Notion and Concept"***, the emphasis is put on the notional determination of infrastructure as critical. In this context are also elaborated the threats on critical infrastructure and the need for critical infrastructure protection. Furthermore, this part also includes a section referring to the analysis of the Critical Infrastructure Indicative List.

In the **second chapter** entitled ***"Critical Infrastructure Protection in the European Union"***, the focus of the research is dedicated to the development of critical infrastructure protection from the perspective of the European Union, the work of the Union's institutions and the orientation of this domain for cooperation with the private sector. This part also covers the section concerning Directive 2008/114/EC on the identification and determination of European critical infrastructures and the assessment of the need to improve their protection.

In the **third chapter** entitled ***"Critical Infrastructure Protection in NATO"***, the focus of interest is the Alliance's place and role in critical infrastructure protection and through critical analysis of a segment of NATO's involvement and role in critical infrastructure protection an attempt is made to tackle several important issues. One of them is whether NATO is conducting excessive securitization and militarization of the energy sector, which is dominantly perceived as an exceptional economic issue and whether there is an appropriate role and opportunity for engaging NATO in critical infrastructure protection within the framework of strategic concepts, especially after the end of the Cold War.

Within the **fourth chapter** entitled ***"Critical Infrastructure Protection in the United States"***, the emphasis is put on analyzing one of the leading countries in the development of critical infrastructure protection. In this context, the concept and system of critical infrastructure protection with the three basic segments the functional, political and technical mechanisms for critical infrastructure protection are very carefully elaborated.

In the **fifth chapter** entitled ***"Critical Infrastructure Protection in Croatia",*** the achievements in the development of critical infrastructure in Croatia made so far have been analyzed. In this context, Croatia's approach has been elaborated upon adoption of the Law on Critical Infrastructure Protection and bylaws, as well as the organization of the critical infrastructure protection system.

The **sixth chapter** entitled ***"Republic of North Macedonia and Critical Infrastructure Protection",*** provides an overview of the current situation in the Republic of North Macedonia related to building an efficient system for critical infrastructure protection. This section identifies priority sectors of critical infrastructure such as energy, information technologies, water systems and air transport. In each of the sectors mentioned, as a result of the reform efforts of the state, there are certain laws and bylaws that can enable effective regulation of critical infrastructure protection. Based on such situations, appropriate measures and recommendations are being offered that would be most useful in the organization of critical infrastructure protection. As an example, the ways and opportunities for creating an effective strategy for protection of critical energy infrastructure are offered. The strategy, after identifying the existing risks, should provide the right direction to overcome the situation of lack of positive legislation on critical energy infrastructure. However, the authors emphasize that partial solutions have been identified in different sectors of critical infrastructure, which are not faulty but are likely to contribute to "stifling" the entire process of designing and efficient functioning of the optimal system for critical infrastructure protection. As a result of such situations, at the end of the chapter, broader recommendations have been given that should outline practical steps towards building an effective system for critical infrastructure protection.

We express our gratitude to the reviewers Professor Jonas Johansson, Director for Critical Infrastructure Protection Research, Lund University, Sweden and Professor Roberto Setola, Univertsita Capmus Bio-Medico di Roma, Italy, for presenting us with the honour of accepting to peer review this manuscript, and their knowledgeable, academic and sincere support for the publication of this book.

Our deepest appreciation go to the "Friedrich-Ebert-Skopje" Foundation for helping us with this project and for the publication of this book in Macedonian and English.

The authors remain thankful for all well-intentioned suggestions, which will be considered in the next edition.

The authors
Skopje, August 2019

CHAPTER 4

CRITICAL INFRASTRUCTURE PROTECTION IN THE UNITED STATES

CHAPTER 4

Critical Infrastructure Protection in the United States

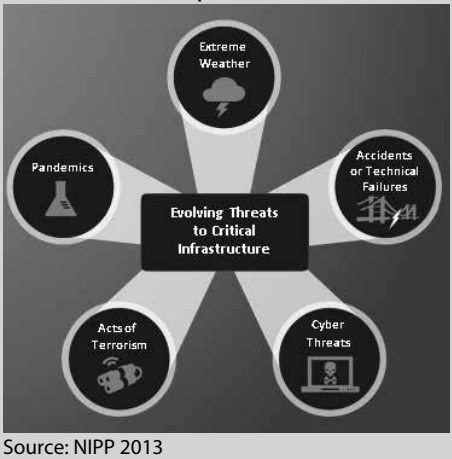
Matthew Vatter, MSS, MSST
US Army Colonel (Retired)
Assistant Commissioner for Enforcement, Minnesota Department of Commerce
Richard J (Rick) Larkin, MA, CEM
Emergency Management Practitioner
Minnesota, USA

4.1. The Organizational Structure of Critical Infrastructure in the United States

In practical terms, critical infrastructure is the power we use in our homes and businesses, the water we drink, the transportation we use to move people and commodities. It is the roads and bridges across the country, the malls in which we shop and the sporting venues we visit. It is our communication systems and our banking and finance systems. All in all it is the structure that enables everyday life as we have come to know it in the United States.

The United States identifies 16 Critical Infrastructure sectors. The systems and assets in these sectors are vital to the general structure and operations of national economy, public health and safety and the overall safety and security of American citizens. Presidential Policy Directive 21 (PPD-21) outlines the policy ensures a strong, resilient and secure system for protecting American critical infrastructure (The White House, 2013). Presidential Policy Directive 7 (PPD-7) established a national policy for federal departments and agencies to identify and prioritize critical infrastructure (Department of Homeland Security, 2003). Having federal level guidelines to direct efforts of federal agencies establishes roles and responsibilities across government and creates the foundation upon which protection activities occur.

Figure 1: List of Critical Infrastructure Sectors in the Republic of Slovenia



Source: NIPP 2013

Separating critical infrastructure into 16 sectors facilitates the assignment of sectoral responsibilities within government and to private industry stakeholders. Sector-Specific Agencies (SSA) are identified to provide a lead resource for the

organization of multi-agency and stakeholder efforts to secure key sector assets. SSAs in coordination with the Secretary of Homeland Security prioritize critical infrastructure based on threat and vulnerability analysis, collaborate with sector specific critical infrastructure owners and operators, carry out incident management, provide technical support and assistance and help mitigate incidents. SSAs are also responsible for regular reporting to the Department of Homeland Security the overall state of preparedness within their assigned sectors and to identify areas of concern. SSA are charged with considering Critical Infrastructure Protection from and "All-Hazards" approach. The Term "all-hazards" means that incidents and threats considered come from natural and human-caused sources and apply to life, property, the environment and public health and safety. All-hazards includes natural disasters, industrial accidents, acts of terror, pandemics, cyber incidents, sabotage, and destructive criminal activities that target critical infrastructure (Department of Homeland Security, 2019).

The table identifies the 16 Critical Infrastructure sectors and the Sector Specific Agencies for each sector as well as a brief description of the areas of responsibility for each sector.

Table 2:
US Critical Infrastructure Sectors and Sector Specific Agencies

Sector and Specific Agent	Description
Chemical: Department of Homeland Security	The chemical sector is responsible for the manufacture, storage, use and transport of potentially dangerous chemicals relied upon by a wide array of other critical infrastructure sectors.
Commercial Facilities: Department of Homeland Security	The commercial facilities sector includes sites that draw large groups of people for lodging, business, entertainment and shopping. These facilities are characterized by having open access to the general public with a vast majority being privately owned.
Communications: Department of Homeland Security	The communications sector provides an enabling function across all sectors of critical infrastructure. It includes terrestrial, satellite and wireless communications.

Critical Manufacturing: Department of Homeland Security	The critical manufacturing sector includes those manufacturing capabilities that underpin many portions of other critical infrastructure sectors. They include primary metals manufacturing, machinery manufacturing, electrical equipment, appliance and component manufacturing and transportation manufacturing.
Dams: Department of Homeland Security	The dams sector provides critical water retention and control which includes hydroelectric power generation, agricultural irrigation, sediment and flood control, river navigation and industrial waste management.
Defense Industrial Base: Department of Defense	The defense industrial base sector is comprised of domestic and foreign companies that provide the materiel and services necessary to build, maintain, mobilize, deploy and sustain US military operations.
Emergency Services: Department of Homeland Security	The emergency services sector provides day to day as well as emergency response and recovery services. It is organized primarily at the federal, state, local tribal and territorial levels of government and includes police, fire, and emergency medical services organizations capable of all-hazard response.
Energy: Department of Energy	The energy sector describes the infrastructure that provides energy resources underpinning all sectors of critical infrastructure. 80 percent of the country's energy infrastructure is privately owned.
Financial Services: Department of Treasury	The financial services sector includes depository institutions, investment institutions, insurance companies and other credit and financing organizations that enable the transfer of financial products and services.

Food and Agriculture: US Department of Agriculture and Department of Health and Human Services	The food and agriculture sector provides for the production, manufacturing, and storage of the nations food and agricultural products supply.
Government Facilities: Department of Homeland Security and General Services Administration	The government facilities sector oversees buildings located in the US and overseas owned or leased by the US government that house embassies, military installations, courthouses, national laboratories, critical equipment and systems.
Healthcare and Public Health: Department of Health and Human Services	The healthcare and public health sector protects all sectors from terrorism, infectious disease and natural disasters. It is responsible for prevention, resiliency response and recovery to public health related issues.
Information Technology: Department of Homeland Security	The information technology sector encompasses the people, hardware and software necessary for the function of government, academia, private sector businesses and the general public. In coordination with the communications sector, is responsible for the internet.
Nuclear Reactors, Materials and Waste: Department of Homeland Security	The nuclear reactors, materials and waste sector includes nuclear power generation, medical isotopes and nuclear and radiological research. It also oversees the movement of radiologic cargo in coordination with the transportation sector.
Transportation Systems: Department of Homeland Security and Department of Transportation	The transportation sector moves people and goods. It includes aviation, highway and motorway, maritime, mass transit and passenger rail, pipeline systems, freight rail and postal and shipping.
Water and Wastewater Systems: Environmental Protection Agency	The water and wastewater systems sector is responsible for the nations clean water supply. It also is critical in the management of sewage and wastewater treatment.

To better prioritize resources and focus, and aid in the rapid recovery from all hazards the National Infrastructure Protection Plan (NIPP) identifies communications, energy, transportation and water management as lifeline functions (Department of Homeland Security, 2013: 17). Identification of these functions within a critical infrastructure sector enables stakeholders to better prepare by prioritizing considerations of these functions and by understanding the interdependencies between sectors. Interdependencies refer to the effect an incident in one sector can have on another. For example, in the event of a large scale power outage, how will the lack of grid power affect transportation, wastewater management and so on. Interdependencies and the requirement for intersectoral cooperation will be discussed in greater detail in another section of this chapter.

Identification of lifeline functions is critical in the development of state, local tribal and territorial (SLTT) response and recovery plans. Threat analysis and vulnerability assessments must consider the effect on each of the functions within a sector to identify the prioritization of response and recovery assets. A comprehensive analysis of the loss of energy during a pandemic crisis would emphasize the need for backup power generation at key medical facilities, for example. It would also help planners to understand the effect on communications and water delivery resulting in plans to mitigate the negative effects of losing capability in this lifeline function. Focus on lifeline functions helps to create a foundation for Critical Infrastructure Protection and helps to delineate the responsibilities for all stakeholders.

Threats to the nation's critical infrastructure fall into five categories: direct enemy attack, cyber threats, accidental or technical failures, extreme weather and pandemics (Department of Homeland Security, 2013: 8). A particularly important lifeline sector is energy. The importance of electrical energy in daily life is obvious and often taken for granted. Events or actions in any single threat category could result in significant disruption to the electric energy distribution system. Combined attacks in multiple threat categories could result in catastrophic, long-term loss of electric power. Enemies of the US could look for or facilitate widespread grid outages and exploit degradation in communications, commitment of security resources to domestic recovery, disruptions in food, water and health service delivery and attack when the US is weakened.

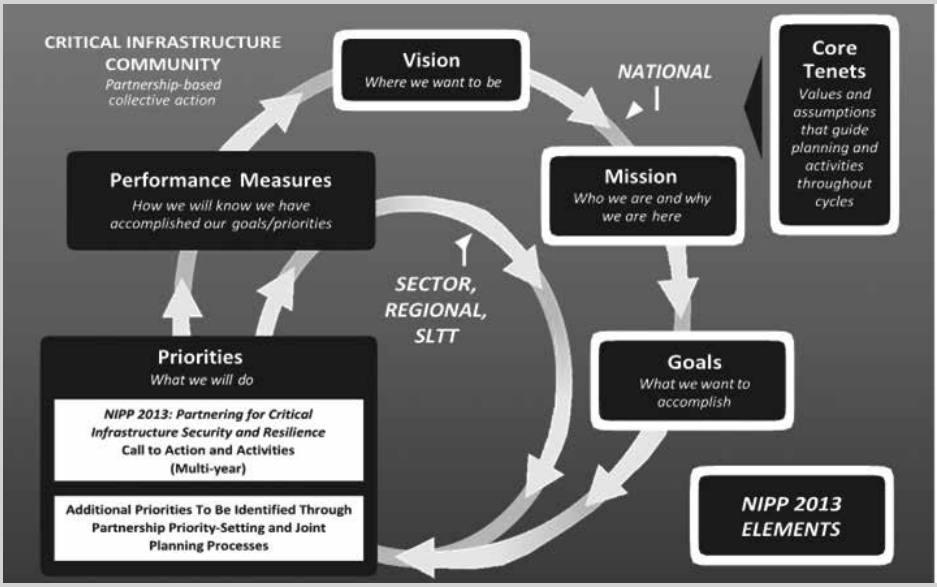
Exacerbating the vulnerability of America's critical infrastructure is the fact that no single organization has authority over it (Association of Old Crows and others, 2014: 5). No matter how diligent critical infrastructure owners are, the achievement of a cohesive, synchronized effort to protect the vast number of interdependent portions will likely not be fully achieved. Enabling individual citizens willing to take greater control where they realistically can will help to strengthen the overall effort. It is estimated that approximately 85 % of critical infrastructure is privately owned (United States Government Accountability Office, 2009). Protecting the nation's infrastructure to include the electric grid requires cooperation and communication among all the stakeholders, governments, private industry and local communities. Although governments regulate many aspects of power production and distribution, private industry, public commissions and cooperatives along with the average citizen must collaborate to establish vital elements of resiliency and

security. In the next section we will discuss the relationship between government at the federal, state, local, tribal and territorial levels and the private sector owners of critical infrastructure.

4.2. Public-Private Partnerships: The Roles and Responsibilities of Critical Stakeholders

The critical infrastructure protection in the United States is a shared responsibility between private sector owners in each sector and governmental agencies at the Federal, State, Local, Tribal and territorial levels. The United States Government Accountability Office (GAO) estimates that 85 % of the nation's critical infrastructure is owned by the private sector (United States Government Accountability Office, 2009). The U.S. government, in coordination and collaboration with key stakeholders has developed a number of standardization documents that provide structure to protection programs across the breadth of the 16 sectors.

Figure 2:
The United State's Plan's Approach to Building and Sustaining Unity of Effort



Source: NIPP, 2013

The 2013 USA National Infrastructure Protection Plan, maintains the task from previous versions of the National Plan for The Department of Homeland Security to maintain sectoral plans for all critical infrastructure sectors that represent a cross-section of sectoral policies, measures and activities of all involved sectoral factors. The first such sectoral plans were adopted in 2010 and revised in 2015. Each of them is additionally linked to specific strategic security policy documents. Sector specific policy can only be executed through voluntary collaboration with private sector owners and operators and their government counterparts. The Government and private sector each have unique responsibilities and the perspectives of each

are equally important. Sectoral Specific plans are maintained through the use of Sector Coordinating Councils, Government Coordinating Councils and Regional Consortia. These collaborative bodies are further broken down to focus on specific areas within a sector. For example, in the Financial Services sector, the Financial Services – Information Sharing and Analysis Center (FS-ISAC) acts as the financial industry "go to" resource for cyber and physical threat intelligence analysis and sharing. This is a membership based organization comprised of private sector, government, non-profit and select partner stakeholder organizations. ISACs are established in other sectors as well. The National Council of ISACs is a coordinating body that facilitates the collaboration of sector-based ISACs. A complete list of all operating sector based ISACs can be found at the NCI website: https://www.nationalisacs.org. ISAC members contribute sector specific information and intelligence in an effort to benefit from sector-wide knowledge and experience. This voluntary collaboration among sector stakeholders is a key element in the overall National Critical Infrastructure Protection Plan and is vital to successful Critical Infrastructure Protection efforts.

The overarching guidance for protection of the Energy Sector is the United States National Infrastructure Protection Plan. 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. In 2015 sector specific updates addressed the nexus between cyber and physical security, interdependence of sectors, risks associated with aging infrastructure, outdated technology and climate change and the changes in the workforce needed to continue to support the National Plan.

Lifeline Sector Plan Overviews

Energy

In 2013, PPD-21 identified the Energy Sector as uniquely critical because it provides an essential function across virtually all critical infrastructure sectors. The most recent Sector-Specific Plan for the Energy Sector is the 2015 edition (Department of Homeland Security, 2015a). The lead agency for the Energy Sector plan is the US Department of Energy (DOE). The Energy sector update was a collaborative effort between the DOE, the Energy Sector Coordinating Councils and government partners. The interrelated sub-components for the Energy Sector are Electricity, Oil and Natural Gas. This includes the production, refining, storage and distribution of electricity, gas and oil. It does not include the production of hydroelectric or nuclear power. These specific sources fall under separate sub-sectors. The Energy Sector supports the transportation industry, supplies electricity to businesses and neighborhoods and provides power to industrial and agricultural production across the United States. It is in turn dependent on information technology, communications, water and finance as well as other aspects of the Critical Infrastructure sectors.

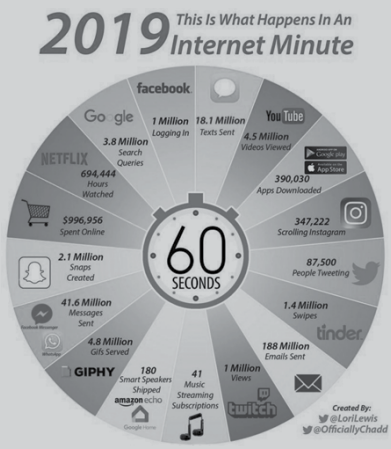
A key component of the sector specific plan is the assessment of threats and risk. The Energy sector plan identifies risk and threat in each of the sub sectors. For the Electricity sub-sector the 2015 plan highlights cyber and physical security threats; natural disasters and extreme weather conditions; workforce capability and human error; equipment failure and aging equipment; evolving environmental, economic and reliability regulatory requirements and changes in the technical and operational environment as the primary threats and risks. Similarly in the Oil and Gas sub-sectors, natural disasters and extreme weather; regulatory and legislative changes – including environmental health; volatile oil and gas demand; operational hazards; political and civil unrest and terrorist activity; transportation infrastructure constraints; inadequate and unavailable insurance coverage; aging infrastructure and workforce and cybersecurity risks and insider threat as primary areas of threat and risk.

Communications

The nature of communications has changed significantly in the past 25 years moving from a primarily voice services oriented environment to an interconnected industry using terrestrial, wireless and satellite communications systems. The Communications Sector Coordinating Council and the Communications Sector Government Coordinating Council worked collaboratively to update the 2010 Communications Sector Specific plan. The plan recognizes the importance of private sector participation in that most communications infrastructure in the US is privately owned and operated. In the 2015 plan the sector identifies 3 goals:

1. Protect and enhance the overall physical and logical health of communications.
2. Rapidly reconstitute critical services in the event of disruption and mitigate cascading effects.
3. Improve the sector's national security and emergency preparedness posture with Federal, State, local, tribal, international and private sector entities to reduce risk (Department of Homeland Security, 2015b: iv).

Figure 3: Internet data every minute



Source: Cyber Security Hub via Linkedin

The sector specific plan update provides targets for public and private partner collaboration among government agencies and private industry. The Communications sector provides products and services that are necessary to the function of other critical infrastructure sectors. They involve both physical infrastructure such as switches, towers and antennas as well as cyber infrastructure such as switching software, applications and operational support architecture. Virtually every aspect of modern life depends upon the cyber infrastructure. Banking, goods and services, emergency communications

and day to day personal interaction are now dependent on a resilient and reliable cyber network. This dependence makes it critical for public-private partnership that addresses all-hazard threats across all aspects of the sector and at all levels of responsibility, to include that of the individual.

The amount of data that is transmitted via the internet every minute emphasizes the reliance modern societies have on the communications infrastructure of not only the US but globally. According to Ericsson (2019), mobile data usage in North America has increased by 40% since 2015. It is projected that this exponential growth will continue with increased capacity of smart devices as well as flexibility of service plans.

With the continued growth of the number and types of devices and the supporting architecture to support them is the necessity for new and emerging policy that protects the infrastructure and more rapidly identifies threats and vulnerabilities. Sector partners must continue to collaborate and evolve to meet this increasing need.

Risk assessment is a key part of the sector specific plan. The Communications Sector plan update for 2015 identifies the following areas within its risk profile:

- Natural disasters and extreme weather – hurricanes and wildfires are among the events that have increased in frequency in recent years. Geomagnetic storms are also on the list of natural events that could cause widespread collapse of power grids and cause long-term outages to national communications.
- Supply chain vulnerabilities – the sector is reliant on hardware and software and the suppliers that provide them to the industry.
- Global political and social implications – geopolitical unrest, economic conditions both foreign and domestic can negatively impact the sector.
- Cyber vulnerabilities – the proliferation of malicious activity to disrupt or deny internet access, data access and data integrity is an on-going concern.

The Communications sector is one of the few sectors that can affect all other sectors. The stability and reliability of the sector facilitates the stability and reliability of the system as a whole.

Transportation

The 2015 update represents the maturation of the sector's partnerships and describes an approach to manage security and resilience in the nation's transportation systems. It balances the freedom of movement of goods and people with the potential loss of civil liberties that could result from over regulation and restrictions. Transportation systems provide lifeline services for the movement of commodities and the ability to respond and recover from disasters. The Transportation Sector, Sector Specific Plan (TS SSP) identifies 4 goals:

1. Manage the security risks to physical, human and cyber elements of critical transportation infrastructure.
2. Employ the sector's response, recovery and coordination capabilities to support whole community resilience.

3. Implement processes for effective collaboration to share mission-essential information across sectors, jurisdictions and disciplines as well as between public and private stakeholders.
4. Enhance the all-hazards preparedness and resilience of the global transportation system to safeguard US national interests (Department of Homeland Security, 2015c: iv).

The TS SSP recognizes advances in efforts to upgrade cyber security to align with growing concerns regarding cyber threats and their effects. It considers an all-hazards approach to resiliency and preparedness across aviation, maritime, freight rail, highway and motor carrier, pipeline, postal and shipping and mass transit transportation systems domestically and internationally. Similar to other sectors, transportation is primarily facilitated by private sector companies. Its owners and operators assess risk and develop plans to mitigate risk and respond to disaster. These plans are developed collaboratively via the numerous coordinating councils and partnership councils facilitated by both government sector and private sector agencies. The US Department of Homeland Security is the primary responsible agency for sector plan development and coordination and within it's span of control shares responsibility with the US Department of transportation, Transportation Security Administration (TSA) and the US Coast Guard (USCG). Government coordinates with industry through regional councils, professional and academic organizations and informal information sharing conferences and knowledge events. Information sharing is the foundation to collaboration among stakeholders. The Transportation Security Information Sharing Environment plan listed multi-directional sharing; effective and efficient processes; trusted partnerships; security education, training and awareness and protection of private liberties as the key goals of the plan. To address growing concerns regarding cybersecurity in the transportation sector, the Transportation System Cybersecurity Working Group was established. It is comprised of Federal, SLTT and private industry representatives. This group raises general industry awareness, promotes community actions and fosters collaborative approaches to heightening overall cybersecurity across the entirety of the transportation sector.

Risks to transportation critical infrastructure include manmade and natural events. Man-made threats include terrorism, both physical and cyber. Aging infrastructure results in higher probability of catastrophic destruction to physical infrastructure due to severe weather, vandalism, sabotage and technological failure. Natural disasters, climate change and extreme weather events can destroy and or degrade transportation systems. Floods, wildfires blizzards hurricanes, tornadoes and droughts all affect transportation services. In the spring of 2019, droughts in Central America resulted in lower water levels in the Panama Canal. Lowered water levels restrict the size of ships that can navigate through the canal. This results in loss of revenue for the canal operators, reduction in quantity that can move through the canal and in extreme events, restrictions in the types of vessels that can navigate the canal (Zamorano and Franco, 2019).

The continued cooperation among all stakeholders and the continuation of extensive information and intelligence sharing through councils and work groups within the sector and in cross-sector events is critical to meeting the ever-changing threat environment.

Water and wastewater

The purpose of the Water and Wastewater Sector Specific Plan (Water SSP) is to secure and strengthen the resilience of the sector's infrastructure (Department of Homeland Security, 2015d). Simply put, the Water and wastewater sector pertains to the maintenance of safe and reliable drinking water systems necessary to maintaining public health and preventing disease. The infrastructure that delivers fresh drinking water and safely transports and treats wastewater is overseen by Federal, state, local, territorial and tribal government entities as well as private sector stakeholders. The Water SSP uses the partnership model outlined in the NIPP to bring private and public sector leaders into the planning and implementation of sector protection efforts. The US Environmental Protection Agency (EPA) is the government agency with primary responsibility for the sector.

The safety and reliability of the nations drinking water system is paramount to health, economic, psychological and environmental concerns nationwide. Events such as the contamination of drinking water systems such as the Flint Michigan water supply contamination event highlight the drastic human health issues caused by negligence in addressing possible contamination (NRDC, 2018). In an effort to save money, city officials decided to discontinue using fresh water piped in from Detroit and instead would use water sourced from the Flint River until a new pipeline from Lake Huron could be built. The city failed to properly decontaminate and purify this supply which resulted in significant increases in blood lead levels in children, skin rashes and numerous other ailments. An effort to save money resulted in significant extra costs to not only clean up the water supply and delivery systems but to compensate Flint residents for their medical and health related expenses.

The Water SPP is a guiding document to help eliminate events such as that experienced in Flint, Michigan. In addition to the human element, the plan considers numerous elements in the drinking water category. Water source, conveyance, raw water storage, treatment, finished water storage distribution systems and monitoring systems comprise the physical components addressed in planning. Supervisory Control and Data Acquisition (SCADA) systems and Process systems and operational controls are areas of emphasis under cyber elements. The control and management of distribution and production are increasingly controlled by digital systems. Compromise of these systems is an identified threat.

Wastewater is addressed separately in the Water SPP. The physical element of the wastewater portion of the plan consists of collection, raw influent storage, preliminary treatment, treatment, disinfection, effluent/discharge, residual and biosolids and monitoring systems. The cyber element involves the same areas as identified in the water sections, SCADA and process systems and operational controls. Of course the human element has to be considered. Not only are the public officials but also laboratory technicians, microbiologists, chemists, public works employees and environmental specialists to mention a few of the professionals necessary to administer this complex system.

Sector risk is categorized as Most Significant, High, and Medium risks. Most significant threats require prioritized attention and mitigation. They pose the

greatest potential for high impact. High risk requires serious attention whereas medium risk events could escalate without thoughtful attention. Examples of Most significant risk are natural disasters such as floods, earthquakes and other natural events that negatively impact water quality for large geographic areas, aging infrastructure and associated economic implications and the possibility of escalating consequences resulting from the inability to manage a crisis across a large area. High risks can be deliberate malicious acts, inaction from stakeholders or utilities and inadequate preparation, response and recovery. Medium risks are insufficient or improper management of assets and resources and a lack of planning in emergency response and mutual aid. These examples of how risk is categorized help to create prioritization based on recognized need across the sector. Risk analysis is situationally dependent and the context of risk analysis outlined in the SSP helps to contextualize the process required to evaluate unique situations.

Sector specific plans exist for all of the 16 sectors. An outline of the Sector Specific Plans provides a general understanding of the detail that each sector specific agency must facilitate in order to address the complexity of each sector. As demonstrated throughout this section, the necessity for collaboration among all stakeholders in each sector cannot be over emphasized. Regular interaction whether formally or informally is required to address the dynamic nature of technology, threat and vulnerability. Plans must be flexible and agile and contain policy that enables adaptation with oversight.

4.3. National standards and the Role of the Government in Policy and Enforcement

The US government began to formalize efforts to develop a comprehensive national policy for Critical Infrastructure in the mid-1990s. *Executive Order (EO) 13010 Critical Infrastructure Protection,* 1996 states that "certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." Threats to Critical Infrastructures are primarily determined as physical and cyber (The White House, 1996). The EO further establishes bodies and accompanying mechanisms with the aim of developing a normative framework for critical infrastructure protection in the United States. Among others, it established the President's Commission on Critical Infrastructure Protection (PCCIP) composed of both public and private sector representatives, and charged them to assess the threats and vulnerabilities to the Nation's infrastructure and to recommend national policy and a strategy for protection. In July 1996, President Clinton established the Commission on Critical Infrastructure Protection (PCCIP), with a charter to designate critical infrastructures, to assess their vulnerabilities, to recommend a comprehensive national policy and implementation strategy for protecting those infrastructures from physical and cyber threats, and to propose statutory or regulatory actions to affect the recommended remedies. The PCCIP submitted its report, *Critical Foundations: Protecting America's Infrastructures,* in October 1997. The PCCIP report was the basis for Presidential Decision Directive 63 (22 May 1998), *Critical Infrastructure Protection,* which establishes national policy and an organizational structure for effecting a

public-private partnership and for accomplishing the special protection functions that are inherently the responsibility of government (Department of Defense, 1998). Critical Infrastructure was defined in 1998 *Presidential Decision Directive / NSC-63 Critical Infrastructure Protection* as "physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." Further, it is emphasized how "[m]any of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber-attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security" (The White House, 1998).

Presidential Policy Directive 21 (PPD 21) articulates the primary responsibilities of the US Federal Government's role in strengthening the security and resilience of US Critical Infrastructure against physical and cyber threats. PPD 21 emphasizes the need for partnership with private sector and international stakeholders and recognizes the interdependent nature of the critical infrastructure system as a whole (The White House, 2013). The federal government facilitates regulatory compliance through regular communication, inspection programs, licensing requirements and financial penalties for non-compliance.

To assist state and local governments with implementing the National Infrastructure Protection Program (NIPP), the Department of Homeland Security (DHS) has implemented a program which uses "Protective Security Advisors". According to the United States Government Accountability Offices (GAO-18-62 Critical Infrastructure Protection), DHS PSA program was established in 2004 to assist with ongoing state and local CI security efforts by establishing and maintaining relationships with state Homeland Security Advisors, State Critical Infrastructure Protection stakeholders, and other state, local, tribal, territorial, and private-sector organizations. PSAs are to support the development of the national risk picture by conducting vulnerability and security assessments to identify security gaps and potential vulnerabilities in the nation's most critical infrastructures (United States Government Accountability Office, 2017).

While useful and a large improvement over earlier, disconnected or inconsistent efforts to implement a national level program , through obtaining local level information, the PSA role is still to focus on the National Level, while assisting with and supporting the state, local, tribal and territorial efforts. PSAs are a tremendous help in making the connection between the local level governments and the CI owners/operators. They serve as subject matter experts on the NIPP and are most often, the representative of DHS CIPP efforts that is most well-known by state and local officials.

Following the release of PPD-21 and Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity*, the Interagency Security Committee (ISC)

established a working group to review The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard and evaluate its effectiveness pertinent to strengthening the security and resilience of Federal critical infrastructure. EO 13636 further directed the National Institute of Standards and Technology (NIST) to lead the development of a framework to reduce cybersecurity risks to critical infrastructure. In February of 2014, National Institute of Standards and Technology (NIST) published the *Framework for Improving Critical Infrastructure Cybersecurity.* The framework was further revised and in 2018 Version 1.1 of the document was released. The primary purpose of this document is to provide business and government a common framework using common language that identifies cybersecurity risk and facilitates the implementation of practices and policies to identify vulnerabilities and reduce the risks those vulnerabilities pose. It also outlines methodologies for categorizing risk and risk tolerance. The commonality of the framework and use of globally recognized standards allows for the Framework to stand as a model for international cooperation across all sectors (National Institute of Standards and Technology, 2018).

In 2017, the White House issued an Executive Order focused on continuing to strengthen efforts in CIP – particularly for Cybersecurity of Federal Networks and support to CI owners/operators. The Executive Order directed all Federal Departments to "use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk" (White House, 2017).

The directive further orders key departments and agencies to *"identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities"* (White House, 2017). Clearly, the US continues to view Critical Infrastructure Protection as a key element of National Security.

Throughout this discussion, it has been emphasized the importance of the private sector involvement in CIP policy and action. US Governmental oversight relies upon the involvement and input from industry. Through the many coordinating councils and sector specific information sharing organizations, sector stakeholders develop standards and operational best practices to which they generally hold themselves accountable. This is not to say that the Federal, State, local, territorial and tribal governments do not implement laws, rules and regulations governing the conduct of activity related to Critical Infrastructure. At all levels of government in the US, agencies implement legislation that guides and directs the operations of owner-operators across all 16 sectors. To provide a comprehensive list of all the governing documents is not realistic for this text but a highlight of the nature of a few can be used to illustrate how regulation shapes activity relating to CIP.

The National Infrastructure Protection Plan 2013 is the overarching document that outlines the vision, mission, goals and core concepts for both government and public-private owner-operators of critical infrastructure. It creates the structure in which partnerships measure against established goals and associated metrics. Sector-specific plans, as previously identified, further refine goals and objectives and

refine information relevant and current to specific sectors. Standards organizations such as NIST develop even greater detail in the way of specific operating practices. Although NIST is a non-regulatory agency, standards developed by NIST create benchmarks by which organizations are measured to determine their ability to securely provide goods and services. The US Federal government uses these standards in the awarding of government service contracts. Private sector organizations that do not demonstrate NIST compliance in areas of concern, such as cyber security, do not meet the basic requirements for consideration in the contracting process. This concept exists for numerous other organizational and industry standards. A detailed list of organizations and the industries they serve can be found by visiting the American National Standards Institute (ANSI) website.[4] The following is a short list of a few of the larger organizations that cross many Critical Infrastructure sectors:

1. NSF International. NSF is a non-governmental, not-for-profit organization that is internationally recognized in the public health and safety field. This organization provides training and certification in a wide variety of disciplines related to public health and safety.[5]
2. ASME (American Society of Mechanical Engineers). ASME is a not-for-profit professional association that promotes the practice of mechanical and multidisciplinary engineering practices throughout the world. Over 500 ASME technical standards are recognized globally for nuclear power components, piping systems, valves cranes and pressure containers among other areas.[6]
3. ISO (International Standards Organization). ISO is a nonprofit organization that develops and publishes standards of virtually every nature. It is headquartered in Geneva, Switzerland represented by 162 members each representing their home country. ISO is the largest developer and producer of standards in the world.[7]
4. FINRA (Financial Industry Regulatory Authority). FINRA is a not-for-profit organization authorized by the US Congress to protect investors by ensuring the broker-dealer financial market operates fairly and honestly. FINRA is a collaborative organization that writes rules governing investment dealings, conducts examinations of firms to ensure compliance and provides investor education. FINRA licensed dealer-brokers must adhere to rigorous standards to protect US financial investment markets.[8]
5. US Department of Transportation (DOT) standards. The US DOT oversees the nation's highways and waterways. This agency provides a comprehensive program involving regulation, production standards, operating standards

4 ANSI provides information on Standards Developing Organizations that work to conform best practices across numerous industries that work within the 16 sectors of Critical infrastructure. Although not tied directly to the National Plan, many standards and organizations play a critical role in ensuring the highest standards of quality and safety are maintained in both the public and private sectors. See more at https://www.standardsportal.org/usa_en/resources/sdo.aspx

5 Detailed information regarding NSF International standards and programs can be found at http://www.nsf.org/

6 Detailed information regarding ASME and ASME standards can be found at http://www.asme.org/

7 Details regarding ISO and their programs can be found at https://www.iso.org

8 FINRA provides a wide variety of tools and services within the financial sector. A comprehensive understanding of their regulatory activity and licenses are available at https://www.finra.org

and general rule making in the greater scope of the transportation sector. DOT collaborates with non-governmental standardization organizations in numerous areas to ensure the nation's transportation system is safe and efficient. DOT areas of focus include automobiles, aviation, bicycles and pedestrians, public transit, pipelines and hazardous material, trucking and motorcoaches, maritime and waterways and roadways and bridges.[9]

6. HIPAA (Health Insurance Portability and Accountability Act). The HIPAA Act of 1996 established standards for the protection of individuals medical records and other personal health information. HIPAA requirements apply across sectors that involve public health and the transmission of personal health information.[10]
7. North American Electric Reliability Corporation (NERC). NERC standards apply to bulk energy producers in North America. The standards focus on performance, risk management and entity capabilities.[11] NERC standards define the reliability requirements for operating bulk power systems. NERC develops standards through the use of a standards committee comprised of representatives from all aspects of the energy production and distribution system, both the private sector and public sector. NERC facilities compliance and enforcement of standards and regulates the North American power grid and the owner-operators that comprise the power generation and distribution system.

These are a few of the high profile organizations that establish and enforce standards that span all aspects of the national Critical Infrastructure system. It is a collaborative that involves government agencies, not-for-profit organizations, industry professionals and academic institutions. Only through participation from all parties can the broad and dynamic nature of the nation's Critical Infrastructure be addressed, maintained and secured.

4.4. Critical Infrastructure Sector Interdependency

The 16 Critical Infrastructure sectors cannot be considered independently. Each sector has a linked dependency to other sectors. Understanding the relationships between sectors and the sub-components of sectors and how they mutually support other sectors enables a comprehensive approach to identifying risk and mitigating responsibilities.

There is reasonable concern that national and international energy and information infrastructures have reached a level of complexity and interconnection that makes them particularly vulnerable to cascading outages, initiated by material failure, natural calamities, intentional attack, or human error. The potential ramifications of network failures have never been greater, as the transportation, telecommunications, oil and gas, banking and finance, and other infrastructures depend on the continental power grid to energize and control their operations.

9 A complete list of responsibilities, activities and processes are available at the Department of Transportation website. https://transportation.gov.

10 HIPAA privacy rules and how they apply to various industries can be found at the US Department of Health and Human Services website. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

11 Standards, NERC.com 2019. https://www.nerc.com/pa/Stand/Pages/default.aspx

Each of the previously mentioned sectors can be seen as a certain "level above" typical Critical Infrastructure in terms of the importance of the service/function provided. The degree to which our modern society relies on these particular sectors supports their designation as "lifeline sectors" for critical infrastructure.

A growing portion of the world's business and industry, art and science, entertainment, and even crime are conducted through the World Wide Web and the Internet. But the use of these electronic information systems depends, as do the more mundane activities of daily life, on many other complex infrastructures, such as cable and wireless telecommunications; banking and finance; land, water, and air transportation; gas, water, and oil pipelines; and the electric power grid.

Taken individually, or in the aggregate, all these systems are intimately linked with the economic well-being, security, and social fabric of the communities they serve. Thinking about critical infrastructure through the subset of lifelines helps clarify features that are common to essential support systems and provides insights into the engineering challenges to improving the performance of large networks.

Lifeline systems are interdependent, primarily by virtue of physical proximity and operational interaction. Lifeline systems all influence each other. Electric power networks, for example, provide energy for pumping stations, storage facilities, and equipment control for transmission and distribution systems for oil and natural gas. Oil provides fuel and lubricants for generators, and natural gas provides energy for generating stations, compressors, and storage, all of which are necessary for the operation of electric power networks. This reciprocity can be found among all lifeline systems (O'Rourke, 2007).

The most important directive for current Critical Infrastructure Protection in US policy, is Presidential Policy Directive (PPD) 21. Following the recommendations adopted in PPD-21, the 2013 NIPP affirms that "effective risk management requires an understanding of the criticality of assets, systems, and networks, as well as the associated dependencies and interdependencies of critical infrastructure" (Department of Homeland Security, 2013).

Assessment of critical infrastructure dependencies and interdependencies is one of the seven core tenets defined in the 2013 NIPP. According to the plan, "understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing critical infrastructure security and resilience" (Department of Homeland Security, 2013). These strategic directives reveal the importance of analyzing infrastructure dependencies, interdependencies, and associated cascading effects from critical infrastructure disruptions to improve national security and resilience.

The directive also highlights the importance of lifeline critical infrastructure dependencies, noting the need to consider "sector dependencies on energy and communications systems, and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems" (The White House, 2013).

Evolving theories regarding infrastructure protection includes viewing infrastructure systems as complex interactive networks (Amin, 2000). Increasing interactions take place between this infrastructure and the electric power grid;

size and complexity continues to increase at a rapid rate. The occurrence of several cascading failures in the past has helped focus attention on the need to understand the complex phenomena associated with these interconnected systems.

Many of our nation's critical infrastructures are complex interdependent networked systems; prime examples are the highly interconnected and interactive industries, which make up a national or international infrastructure, including telecommunications, transportation, gas, water and oil pipelines, the electric power grid, and the collection of satellites in earth orbit. Interactions between networks such as these increase the complexity of operations and control. Secure and reliable operation of these systems is fundamental to our economy, security and quality of life. These large scale networks are characterized by many points of interaction among a variety of participants-owners, operators, sellers, and buyers. The networks' interconnected nature makes them vulnerable to cascading failures with widespread consequences.

Energy, telecommunications, transportation, and financial infrastructures are becoming increasingly interconnected, thus posing new challenges for their secure, reliable, and efficient operation (Amin, 2002). Virtually every crucial economic and social function depends on the secure, reliable operation of infrastructures.

As these infrastructures have grown more complex to handle a variety of demands, they have become more interdependent. The Internet, computer networks, and our digital economy have increased the demand for reliable and disturbance-free electricity; banking and finance systems depend on the robustness of electric power, cable, and wireless telecommunications. Transportation systems, including military and commercial aircraft and land and sea vessels, depend on communication and energy networks. Links between the power grid and telecommunications and between electrical power and oil, water, and gas pipelines continue to be a lynchpin of energy supply networks. This strong interdependence means that an action in a part of one infrastructure network can rapidly create global effects by cascading throughout the same network and even into other networks.

Cross-Sector Measures and Collaboration

The evolution of the cross-sector collaboration and cooperation in CIP in the US includes the development of the Critical Infrastructure Cross-Sector Council. The CI Cross-Sector Council is the private sector organized and managed representative critical infrastructure cross-sector council. Developed in 2015, the CI Cross-Sector Council facilitates consultations, information sharing, and coordinated effort across the critical infrastructure sectors and sub-sectors and with the Federal government, as well as with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), the Regional Consortium Coordinating Council (RC3), and the National Council of Information Sharing and Analysis Centers (NCISAC) (Department of Homeland Security, 2015e).

The CI Cross-Sector Council was formed to assure the opportunity to engage with Federal government officials for the purpose of achieving consensus on joint priorities and actions to advance critical infrastructure security, protection and

resilience, joint meetings between the CI Cross-Sector Council and representatives of Federal departments and agencies (Department of Homeland Security, 2015e: 2). The CI Cross-Sector Council is organized and managed by, and responsible to, the leaders and designated representatives of the Sector Coordinating Councils (SCCs) that comprise its membership. The CI Cross-Sector Council provides the representative forum for consultations, coordination, and cooperative efforts on matters pertaining to critical infrastructure security, protection and resilience for its members.

Additionally, the National Infrastructure Advisory Council (NIAC), which serves in an advisory capacity to the President of the United States, recommended in August of 2017 that further studies be undertaken in the area of increased collaboration and cross-sector measures.

The NIAC recommended to the President of the United States that the Council could assist with informing risk reduction activities by further study of the following seven areas:

1. Incorporating resilience into Federal capital planning and recovery investments
2. Using insurance to recognize and reward investment in resilience
3. Public-private, cross-sector, and regional information sharing
4. Cross-sector interdependency risks during long-duration energy disruptions
5. Port infrastructure security and resilience
6. Workforce trends affecting critical infrastructure security and resilience
7. Security and resilience of oil and natural gas transit by pipeline and rail (Department of Homeland Security, 2017a).

As our world becomes more and more connected and our modern marketplace develops faster and more intelligent systems to provide control and management of critical infrastructure, it is a growing challenge that we will be forced to identify and mitigate risk caused by these increasing interdependent and connected systems.

4.5. Future Landscape of Critical Infrastructure in the United States

The Nation's critical Infrastructure and the focus to identify and protect is ever-evolving. From the end of World War II to Pre-9/11 (the attacks on the World Trade Center in New York, USA) the focus has been on the defense industrial base and physical threats posed by actors external to the United States, primarily from nation states. After the World Trade Center attacks, a defining moment much like the attack on Pearl Harbor, the national attention shifted and the vulnerability to terrorist attacks on the nation's infrastructure became more apparent. Through 2007 the focus was on the identification and cataloging of the nation's critical infrastructure assets. From 2007 to 2013 the focus turned to the identification and prioritization of lifeline sectors and the overall interdependency of the critical infrastructure system as a whole. The proliferation of digital information exchange and connected enterprise lead to our current focus, building resiliency and cybersecurity.

The proliferation of connected devices will exponentially increase the complexity of protecting critical infrastructure. Automation and autonomous systems present new potential attack surfaces in all sectors. The increasingly interconnected and interdependent nature of CI systems will make cross-sector collaboration a dire necessity.

Critical Infrastructure Protection across the nation at all levels of government and community stakeholders remains a priority and a challenge. The US National Preparedness Report (NPR) findings from 2017 indicate that "public and private-sector partners continue to focus on improving infrastructure systems to address vulnerabilities posed by deteriorating critical infrastructure" (Department of Homeland Security, 2017b: 89).

CIPP continues to be a high priority and yet a persistent challenge to US states and local governments. In the 2017 National Preparedness report, summarizing the status of preparedness and security in the United States, the section on Infrastructure Systems provides a concerning assessment on the state of affairs.

The focus of Infrastructure Systems is on stabilizing critical infrastructure functions, minimizing health and safety threats, and efficiently restoring and revitalizing systems and services to support a viable, resilient community. While Federal departments and agencies took steps to address challenges to this core capability, as detailed on page 89, limited evidence exists demonstrating that the Nation has made significant progress in this area. Aging infrastructure in many sectors presents growing risks, as well as decreases resilience …States and territories identified this core capability as exhibiting below-average levels of proficiency in 2016 (Department of Homeland Security, 2017b: 14).

Regardless of the approach, there needs to be a basic understanding of the elements that make up the system. A challenge for future researchers, whether academic, private sector, or government institutions, is to develop a "maturity model" to evaluate local CIP efforts and a guide towards a more fully robust and mature risk reduction and resilience model. Critical Infrastructure Protection must continue to evolve to meet the dynamic nature of maturing societies, the changing needs of its people and the development of new and yet to be seen technologies. An agile, adaptive and integrated methodology that uses all system stakeholders is the only way to ensure a resilient and reliable Critical Infrastructure Architecture.

Chapter conclusion

This chapter looked at five aspects of Critical Infrastructure Protection. In section one, the general structure of US Critical Infrastructure Protection was outlined. This section discussed the sixteen Critical Infrastructure Sectors and identified the governmental agencies with primary responsibility for policy, oversight, strategic planning, security collaboration and enforcement. Section two discusses the public-private nature of critical infrastructure ownership and oversight and identified some of the formal collaborative group established to bring stakeholders together to work through the evolving challenges the nation faces to secure its critical infrastructure. Section three discusses the structure of National Standards that create the frameworks used to establish consistency across sectors and to create a

common language for all stakeholders in all sectors. Section four builds on section three by discussing the interdependent nature of the sixteen critical infrastructure sectors and identified the further designation of life-line sectors. Since the sectors cannot be considered independently, the structure of National Standards and National Frameworks like the NIST Cybersecurity Framework ensures cross-sector standardization and helps to model the nature of potential cascading effects of events originating in one or more sectors. Finally, the chapter looked at the future landscape for Critical Infrastructure Protection with a brief discussion of the impact of cyber events, the proliferation of connected devices and the ease of disruption by non-state actors in a changing and evolving geopolitical landscape.

The way forward for Critical Infrastructure Protection and practitioners in the field is complex and ever-changing. The need for collaboration and partnership across sectors and between the private sector and public sector stakeholders will become more imperative. As everyday life becomes more connected and average people depend more of autonomous services and interconnected devices, the role of the individual in Critical Infrastructure Protection will also become more important. Any system is only as secure as its weakest point. A strong Critical Infrastructure Protection plan encompasses all possible vulnerabilities and weaknesses, to include the human being.

About authors

Marina Mitrevska is a Full Professor at the Institute for Security, Defence and Peace at the Faculty of Philosophy, University of Ss. Cyril and Methodious in Skopje, Republic of North Macedonia. She is Head of the third cycle doctoral studies in security, defence and peace. She is a member of the Accreditation and Evluation Board of Higher Education in the Republic of North Macedonia. She is Editor-in-Chief of the international scientific journal Contemporary Macedonian Defence. Her field of scientific research is security, diplomacy, peacekeeping operations and crisis management. She is actively engaged in researching and publishing scientific papers and books in the field of security. She is the author of eleven books and more than a hundred scientific papers.

E-mail: marinamitrevska@yahoo.com

Toni Mileski is a Macedonian full professor and researcher in the field of political geography and geopolitics, environmental security, energy security and migration and conflicts. He is an employee of the Ss. Cyril and Methodius University, Faculty of Philosophy – Department of security, defence and peace. Professor Mileski has taken participation in several scientific and research project. In October 2012 he participated in the International Visitor Leadership Program organized by US Embassy. Program held in Washington, New York and Boston, USA. Recently, he is second year consequently programme coordinator of the two projects developed together with Brandenburg University of Technology in Cottbus – Germany and DAAD Foundation. He is the author of six books, several books chapters and more than an eighty scientific papers.

E-mail: toni@fzf.ukim.edu.mk

Robert Mikac is Assistant Professor at the Faculty of Political Science of the University of Zagreb in the area of Social Sciences, Field of Political Science, Subfield International Relations and National Security. Areas of his interest and expertise are: International Relations; International and National Security; Security Management; Crisis and Disaster Management; Civil Protection; Afghanistan; Privatization of Security, Critical Infrastructure Protection and Resilience; Migrations and Security. Unitl now he published three books (the first on Afghanistan, the second on Privatization of Security, the third on Critical Infrastructure Protection) and about forty scientific and expert papers. At the previous workplace in National Protection and Rescue Directorate was in charge of affairs related to critical infrastructure, and from 2012 till 2015 the national point of contact for critical infrastructure.

E-mail: robert.mikac@yahoo.com

Richard Larkin is the former Director of Emergency Management for the City of Saint Paul, Minnesota, USA. He has over 30 years' experience in Public Safety as an Emergency Medical Technician/Paramedic, Firefighter, and Emergency Management practitioner in the 16th largest metropolitan area in the United States. He has been involved in Emergency Management (Civil Protection/Crisis Management) program review and support activities in Hong Kong, PRC; Peru, Republic of Croatia and 3 of the British Overseas Territories in the Caribbean. His areas of his interest and expertise are: Emergency Management and Homeland Security Program Administration, Crisis and Disaster Management; Civil Protection; Critical Infrastructure Protection and Resilience; National Standards and Accreditation of Emergency Management and Business Continuity programs, Emergency Planning and Preparedness, Incident Management and Emergency Response. He is a member of the international Institute for Security Policy and a past Chairperson for an International Emergency Management Standard Development Organization (EMAP). He is also a contributing author to 3 peer-reviewed textbooks on Critical Infrastructure Protection and Resilience.

E-mail: rjlarkin103@gmail.com

Matthew Vatter is a retired Senior Army officer from Minnesota National Guard. During his assignment to the Minnesota National Guard, he held numerous leadership positions culminating as the Director of Strategic Plans and Policy. In this capacity he led the MN National Guard Contingency Operations program which focused on Military Support to Civil Authority during National emergencies and national disasters. His team wrote and exercised the plans that provide military resources to civilian authorities and established command authority and relationship development among local, state and tribal emergency response agencies. He oversaw the state partnership program with the country of Croatia assisting Croatia with the development of various National security programs and policies to include crisis response, critical infrastructure protection and cyber defense training along with traditional military inter-operability. He is a graduate of the United States Army War College and the Universities of Minnesota and Wisconsin. He holds an undergraduate degree in earth science education and masters of science degrees in strategy and security technologies. He has contributed to academic texts on critical infrastructure protection and written academic papers on energy resiliency. He currently serves the state of Minnesota as an Assistant Commissioner for the Department of Commerce where he leads a team 58 consumer service agents and professional investigators. He frequently lectures on cyber security for small business and the shared responsibility of government and private sector on security and resiliency.

E-mail: mattvatter@gmail.com