LEGAL AND POLITICAL SCIENCE

CONCEPTUAL REVIEW OF THE UNITED STATES CRITICAL INFRASTRUCTURE ARCHITECTURE: POLICY, LAW AND ADMINISTRATION

Vephkhvia Grigalashvili, *PhD, Assistant-professor, International Black Sea University, Tbilisi, Georgia*
Khatuna Abiashvili, *PhD Candidate, Georgian Technical University, Tbilisi, Georgia*

DOI: https://doi.org/10.31435/rsglobal_conf/25042021/7522

Abstract. *The United States` Critical Infrastructure System (CIs) represents an umbrella concept grouping all those resources that are essential for national economic, financial, and social system. These critical infrastructures are vital and without them, or with any damages to them, would cripple the nation, states, and/or local communities and tribes. Based on a systematic review approach (methodology), this paper aims to review the United States' Critical Infrastructure Protection System (USCIPS) at tree aspects. In section one, the policy pillars of USCIPS are outlined based on studding Presidential Policy Directive 21 (PPD-21) and National Infrastructure Protection Plan (NIPP). Section two discusses the interdependent nature of the sixteen critical infrastructure sectors and identified the further designation of life-line sectors. Final sector introduces USCIPS stakeholders, collaboration and partnership across between the private sector and public sector stakeholders.*
Keywords*: US Critical Infrastructure; Critical Infrastructure Architecture; Critical Infrastructure Policy; Critical Infrastructure Protection.*

Introduction. In a modern variable security environment, there are growing concerns and debates regarding CI concept and protection of these CIs, especially, how to effectively protect them given their vital positions in social and economic developments. These concerns have been highlighted with the increased emphasis on improved efficiency, performance and productivity, and this implies that CIs now rarely exist or function in isolation. Rather, they are becoming more tightly coupled into a system of (inter)dependent infrastructures.

In this case the United States is no exception regardless of its economic or military or other strength. The United States` CI provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

Critical Infrastructure Policy.

Since mid-1990s, by issuing the Executive Order (EO) 13010 CI Protection, the US government has begun to formalise efforts to develop a comprehensive national policy for CI. Mentioned order stated 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 [1].

Through 2007 the focus was on the identification and cataloging of the nation's CI assets. From 2007 to 2013 the focus turned to the identification and prioritisation of lifeline sectors and the overall interdependency of the critical infrastructure system as a whole.

Today Presidential Policy Directive 21 (PPD-21), which supersedes Homeland Security Presidential Directive 7 [2], establishes national policy on CI security and resilience. The directive declares that: a) "The Nation's CI is diverse and complex. It includes distributed networks, varied organisational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. CI owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient"; b) CI must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery" [3].

The term "critical infrastructure" has the definition given to that term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)) - the term ‘‘critical infrastructure’’ means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters” [4].

NIPP provides the coordinated approach that is used to establish national priorities, goals, and requirements for protecting and ensuring the continuity of CI and key resources (CIKR) protection so that federal resources are applied in the most effective and efficient manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. It establishes the overarching concepts relevant to all CIKR sectors identified under the authority of Homeland Security Presidential Directive 7, and addresses the physical, cyber, and human considerations required for effective implementation of protective programs and resiliency strategies [5].

The NIPP specifies the key initiatives, milestones, and metrics required to achieve the Nation’s CIKR protection mission. It sets forth a comprehensive risk management framework (Fig.1) and clearly defined roles and responsibilities for the Department of Homeland Security, Federal Sector-Specific Agencies (SSAs), and other Federal, State, local, tribal, territorial, and private sector partners. The cornerstone of the NIPP is its risk management framework establishing the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk [6].

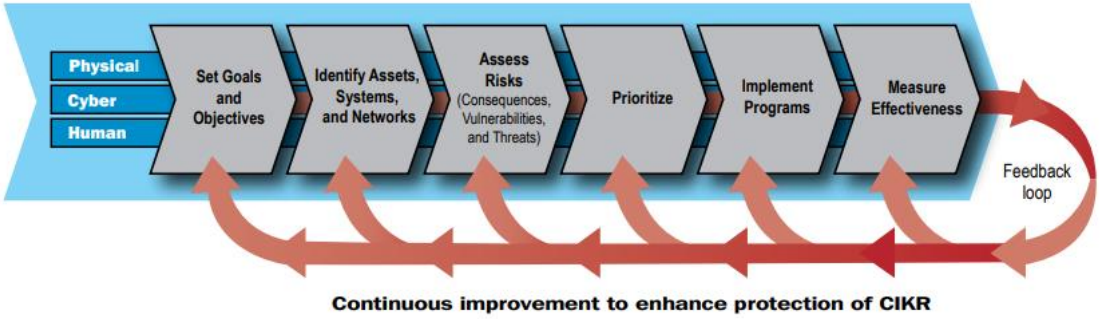

Fig. 1. Risk Management Framework

Critical Infrastructure Sectors

Each Critical Infrastructure Sector (CIS) is crucial to the economic prosperity and continuity of the United States – a direct attack on or disruption of certain elements of CI could disrupt essential functions at the national level and across multiple CIS.

Cybersecurity and Infrastructure Security screens 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof: 1. The Chemical Sector; 2. The Commercial Facilities Sector; 3. The Communications Sector; 4. The Critical Manufacturing Sector; 5. The Dams Sector; 6. The Defense Industrial Base Sector; 7. The Emergency Services Sector; 8. The U.S. energy infrastructure; 9. The Financial Services Sector; 10. The Food and Agriculture Sector; 11. The Government Facilities Sector; 12. The Healthcare and Public Health Sector; 13. The Information Technology Sector; 14. The Nuclear Reactors, Materials, and Waste Sector; 15. The Transportation Systems Sector; 16. The Water and Wastewater Systems Sector [7].

The Chemical Sector is an integral component of the U.S. economy that manufactures, stores, uses, and transports potentially dangerous chemicals upon which a wide range of other critical infrastructure sectors rely. Securing these chemicals against growing and evolving threats requires vigilance from both the private and public sector. Based on the end product produced, the sector can be divided into five main segments, each of which has distinct characteristics, growth dynamics, markets, new developments, and issues: Basic chemicals; Specialty chemicals; Agricultural chemicals; Pharmaceuticals; Consumer products.

The Commercial Facilities Sector includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging. The Commercial Facilities Sector consists of eight subsectors: Entertainment and Media; Gaming; Lodging; Outdoor Events; Public Assembly;

Real Estate; Retail; Sports Leagues. Facilities within the sector operate on the principle of open public access, meaning that the general public can move freely without the deterrent of highly visible security barriers. The majority of these facilities are privately owned and operated, with minimal interaction with the federal government and other regulatory entities.

The Communications Sector as a component of the U.S. economy, underlies the operations of all businesses, public safety organisations, and government. Presidential Policy Directive 21 identifies the Communications Sector as critical because it provides an "enabling function" across all critical infrastructure sectors. This sector is closely linked to other sectors, including The Energy Sector; The Information Technology Sector; The Financial Services Sector; The Emergency Services Sector; The Transportation Systems Sector.

The Critical Manufacturing Sector focuses on the identification, assessment, prioritisation, and protection of nationally significant manufacturing industries within the sector that may be susceptible to manmade and natural disasters. Primary Metals Manufacturing Iron and Steel Mills and Ferro Alloy Manufacturing Alumina and Aluminum Production and Processing Nonferrous Metal Production and Processing Machinery Manufacturing Engine and Turbine Manufacturing Power Transmission Equipment Manufacturing Earth Moving, Mining, Agricultural, and Construction Equipment Manufacturing Electrical Equipment, Appliance, and Component Manufacturing Electric Motor Manufacturing Transformer Manufacturing Generator Manufacturing Transportation Equipment Manufacturing Vehicles and Commercial Ships Manufacturing Aerospace Products and Parts Manufacturing Locomotives, Railroad and Transit Cars, and Rail Track Equipment Manufacturing Products made by these manufacturing industries are essential to many other critical infrastructure sectors.

The Dams Sector delivers critical water retention and control services in the United States, including hydroelectric power generation, municipal and industrial water supplies, agricultural irrigation, sediment and flood control, river navigation for inland bulk shipping, industrial waste management, and recreation. Its key services support multiple critical infrastructure sectors and industries. Dams Sector assets irrigate at least 10 percent of U.S. cropland, help protect more than 43 percent of the U.S. population from flooding, and generate about 60 percent of electricity in the Pacific Northwest. There are more than 90,000 dams in the United States — approximately 65 percent are privately owned and approximately 80 percent are regulated by state dams safety offices. The Dams Sector has interdependencies with a wide range of other sectors, including: Communications; Energy, Food and Agriculture; Transportation Systems; Water.

The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. The Defense Industrial Base partnership consists of Department of Defense components, more than 100,000 Defense Industrial Base companies and their subcontractors who perform under contract to the Department of Defense, companies providing incidental materials and services to the Department of Defense, and government-owned/contractor-operated and government-owned/government-operated facilities. The sector provides products and services that are essential to mobilize, deploy, and sustain military operations. The Defense Industrial Base Sector does not include the commercial infrastructure of providers of services such as power, communications, transportation, or utilities that the Department of Defense uses to meet military operational requirements. These commercial infrastructure assets are addressed by other Sector-Specific Agencies.

The Emergency Services Sector (ESS) is a community of millions of highly-skilled, trained personnel, along with the physical and cyber resources that provide a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response. The ESS includes geographically distributed facilities and equipment in both paid and volunteer capacities organised primarily at the federal, state, local, tribal, and territorial levels of government, such as city police departments and fire stations, county sheriff's offices, Department of Defense police and fire departments, and town public works departments. The ESS also includes private sector resources, such as industrial fire departments, private security organisations, and private emergency medical services providers. Five distinct disciplines compose the ESS, encompassing a wide range of emergency response functions and roles. The ESS also provides specialised emergency services through individual personnel and teams.

The Energy Sector describes the infrastructure that provides energy resources underpinning all sectors of critical infrastructure. Presidential Policy Directive 21 identifies the Energy Sector as uniquely critical because it provides an "enabling function" across all critical infrastructure sectors. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to growth and production across the nation. The energy infrastructure is divided into three interrelated segments: Electricity; Oil, and Natural gas.

The Financial Services Sector represents a vital component of nation's critical infrastructure. Large-scale power outages, recent natural disasters, and an increase in the number and sophistication of cyber attacks demonstrate the wide range of potential risks facing the sector. The Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organisations, and the providers of the critical financial utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities.

The Food and Agriculture Sector is almost entirely under private ownership and is composed of an estimated 2.1 million farms, 935,000 restaurants, and more than 200,000 registered food manufacturing, processing, and storage facilities. This sector accounts for roughly one-fifth of the nation's economic activity. The Food and Agriculture Sector has critical dependencies with many sectors, but particularly with the following: Water and Wastewater Systems, for clean irrigation and processed water; Transportation Systems, for movement of products and livestock; Energy, to power the equipment needed for agriculture production and food processing; Chemical, for fertilizers and pesticides used in the production of crops.

The Government Facilities Sector includes a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments. In addition to physical structures, the sector includes cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed-circuit television systems) as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge.

The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters. Because the vast majority of the sector's assets are privately owned and operated, collaboration and information sharing between the public and private sectors is essential to increasing resilience of the nation's Healthcare and Public Health critical infrastructure. Operating in all U.S. states, territories, and tribal areas, the sector plays a significant role in response and recovery across all other sectors in the event of a natural or manmade disaster.

The Information Technology Sector is central to the nation's security, economy, and public health and safety as businesses, governments, academia, and private citizens are increasingly dependent upon Information Technology Sector functions. The sector's complex and dynamic environment makes identifying threats and assessing vulnerabilities difficult and requires that these tasks be addressed in a collaborative and creative fashion. Information Technology Sector functions are operated by a combination of entities—often owners and operators and their respective associations—that maintain and reconstitute the network, including the Internet. Although information technology infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges as well as opportunities for coordinating public and private sector preparedness and protection activities.

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.

The Transportation Systems 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.

The Water and Wastewater Systems Sector is responsible for the nation`s clean water supply. It also is critical in the management of sewage and wastewater treatment.

Critical Infrastructure Stakeholders. Presidential Policy Directive 21 (PPD-21) directive refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration.

The Federal Government has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organise itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

The Cybersecurity and Infrastructure Security Agency (CISA), which was established on November 16, 2018 when President Donald Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018, is a standalone United States federal agency, an operational component under Department of Homeland Security oversight [8]. Its activities are a continuation of the National Protection and Programs Directorate (NPPD). CISA leads the nation's effort to understand and manage cyber and physical risk to the USA critical infrastructure - CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

CISA subcomponents include the: Cybersecurity Division; Infrastructure Security Division; Emergency Communications Division; National Risk Management Center; Integrated Operations Division; Stakeholder; ngagement Division; National Emergency Technology Guard (inactive, but can be activated by the director of CISA) [9].

As the nation's risk advisor, CISA mission is to ensure the security and resiliency of CI. However, in today's digitizing world, as organisations are increasingly integrating cyber systems into their operations, they are also facing more diverse, sophisticated threats — cyber, physical, technological, or natural — that may have cross-sector impacts. The evolving risk landscape necessitates an evolved response.

Housed with CISA, the National Risk Management Center (NRMC) helps fulfill the Agency's risk advisor role by leveraging sector and stakeholder expertise to identify the most significant risks to the nation, and to coordinate risk reduction activities to ensure critical infrastructure is secure and resilient both now and into the future. NRMC brings the private sector, government agencies, and other key stakeholders together to identify, analyse, prioritise, and manage the most significant risks to critical infrastructure.

The NRMC's dynamic, cross-sector risk management process transforms private-public engagement into collective action by defragmenting how the government and industry develop response and security plans, risk-reduction activities, and share information. The interconnectedness of the sectors and sophistication of threats and hazards means that the consequences of an attack or imminent threat do not impact only one sector. The NRMC creates an environment where government and industry can collaborate and share expertise to enhance critical infrastructure resiliency within and across sectors.

Separating CI into 16 sectors facilitates the assignment of sectoral responsibilities within government and to private industry stakeholders. 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 recognises the interdependent nature of the critical infrastructure system as a whole. The federal government facilitates regulatory compliance through regular communication, inspection programs, licensing requirements and financial penalties for non-compliance.

SSAs (Tab.1) are identified to provide a lead resource for the organisation of multi-agency and stakeholder efforts to secure key sector assets. SSAs in coordination with the Secretary of Homeland Security prioritise 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 that includes natural disasters, industrial accidents, acts of terror, pandemics, cyber incidents, sabotage, and destructive criminal activities that target critical infrastructure [10].

Table 1. Sector-Specific Agencies

Critical Infrastructure sectors	Sector-Specific Agencies
The Chemical Sector	The Department of Homeland Security
The Commercial Facilities Sector	The Department of Homeland Security
The Communications Sector	The Department of Homeland Security
The Critical Manufacturing Sector	The Department of Homeland Security
The Dams Sector	The Department of Homeland Security
The Defense Industrial Base Sector	The U.S. Department of Defense
The Emergency Services Sector (ESS)	The Department of Homeland Security
The U.S. Energy Infrastructure	The Department of Energy
The Financial Services Sector	The Department of the Treasury
The Food and Agriculture Sector	The Department of Agriculture
The Government Facilities Sector	The Department of Homeland Security and the General Services Administration
The Healthcare and Public Health Sector	The Department of Health and Human Services
The Nuclear Reactors, Materials, and Waste Sector	The Department of Homeland Security
The Information Technology Sector	The Department of Homeland Security
The Transportation Systems Sector	The Department of Homeland Security and the Department of Transportation
The Water and Wastewater Systems Sector	The Environmental Protection Agency

The critical infrastructure protection is a shared responsibility between private sector owners and governmental agencies at the Federal, State, Local, Tribal and territorial levels (Fig. 2). The United States Government Accountability Office estimates that 85 % of the nation's critical infrastructure is owned by the private sector [10].

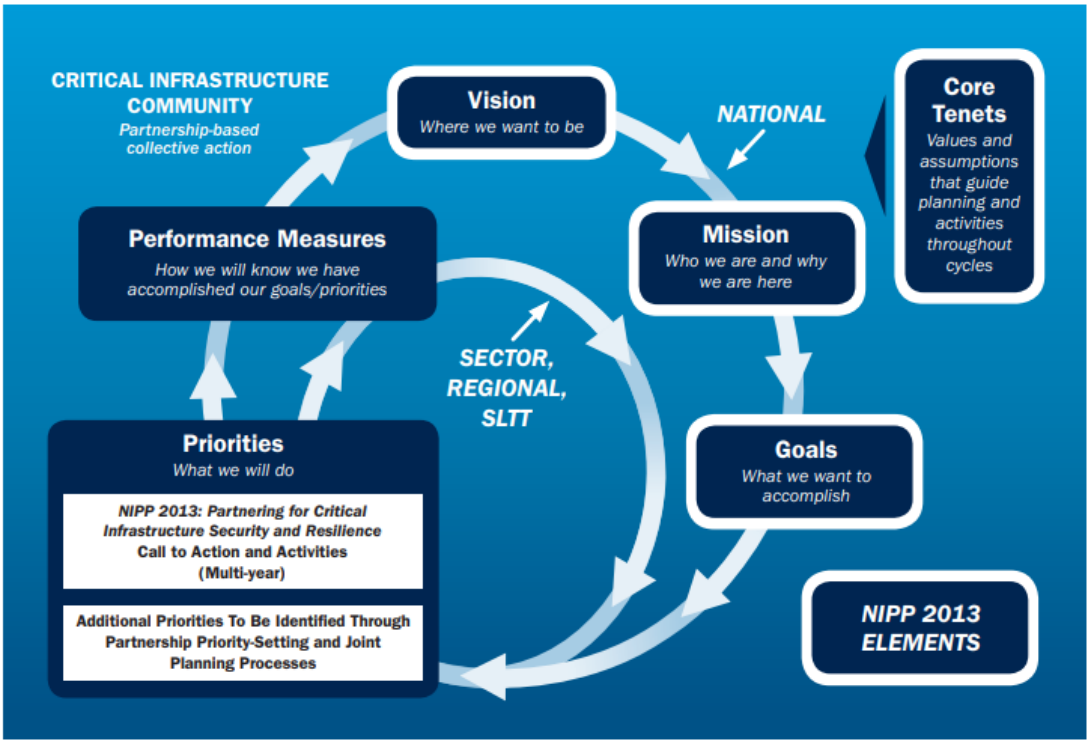

Fig. 2. The United States' Plan's Approach to Building and Sustaining Unity of Effort [11]

Conclusions. As study shows CIPP continues to be a high priority and yet a persistent challenge to the United States. CIPP 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 to ensure a resilient and reliable CI architecture.

REFERENCES

1. EO 13010: Critical Infrastructure Protection. Homeland Security Digital Library. https://www.hsdl.org/?abstract&did=1613 (Accessed in 10.04.2021)
2. HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 7: CRITICAL INFRASTRUCTURE IDENTIFICATION, PRIORITISATION, AND PROTECTION https://www.cisa.gov/homeland-security-presidential-directive-7 (Accessed in 14.04.2021)
3. Presidential Policy Directive - Critical Infrastructure Security and Resilience https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (Accessed in 14.04.2021)
4. 42 U.S. Code § 5195c - Critical infrastructures protection https://www.law.cornell.edu/uscode/text/42/5195c (Accessed in 10.04.2021)
5. National Infrastructure Protection Plan https://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf (Accessed in 11.04.2021)
6. National Infrastructure Protection Plan https://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf (Accessed in 11.04.2021)
7. Cybersecurity and Infrastructure Security Agency on its official website https://www.cisa.gov/ (acceded in 11.04.2021)
8. Cimpanu, Catalin (November 16, 2018). "Trump signs bill that creates the Cybersecurity and Infrastructure Security Agency". ZDNet. Archived from the original on February 19, 2019. Retrieved December 16, 2018
9. Cybersecurity and Infrastructure Security Agency Organisational Chart. Department of Homeland Security. February 27, 2019. Archived from the original on April 17, 2019. Retrieved May 4, 2019
10. MItrevska M., MIletski T., Mikac R., CRITICAL INFRASTRUCTURE: CONCEPT AND SECURITY CHALLENGES, 2019.
11. NIPP 2013 Partnering for Critical Infrastructure Security and Resilience. Homeland Security. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (Accessed 12.04.2021)