IX INTERNATIONAL SCIENTIFIC PROFESSIONAL CONFERENCE
SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTICE (SeCMan)
- IX INTERNATIONAL FORUM „SAFETY FOR THE FUTURE 2023" -
29th and 30th September 2023, Belgrade, Republic of Serbia

CHALLENGES OF CRITICAL INFRASTRUCTURE PROTECTION IN CONTEMPORARY SECURITY ENVIRONMENT

Dragisa Jurisic[1a]
[1] Security Research Center, Street Sinise Mijatovica 9, Banja Luka, Republic of Srpska, Bosnia and Herzegovina, bicbl@yahoo.com

Received: 28th August 2023
Accepted: 4th September 2023

Original scientific paper

Abstract: *Infrastructures are all around and the life of people in contemporary times depends on them. People are using that infrastructure to make their lives easier and more acceptable. In order to have a nice life people are trying to protect some of that infrastructure. The same situation is with the states. Protection of critical entities or infrastructure is one of the state's tasks when it comes to the basic needs of the population, but these infrastructures usually, in the contemporary world, cross the border, and then there are more subjects responsible for protection. Moreover, some infrastructures are so important and they are in focus for the all world. That kind of infrastructure should be also in some way protected because it has benefits for most of the population in the world. However, the big geopolitical players are calculating depending on their interests whether they would protect that infrastructure or not. This paper shows that world critical infrastructure depends on the interest of big geopolitical players and individual states are not able to do anything to prevent destruction or failure on purpose of that infrastructure.*

Keywords: *infrastructure, geopolitics, protection, security*

(introductory lecture of the forum - work by invitation)

1. INTRODUCTION

Challenges, risks, and threats in the contemporary world are taking on more and more subtle substantive forms, which in a short period of time can threaten vital international subjects or their parts and thus have significant impacts on the development of our civilization.

Natural disasters, the threat of nuclear weapons, terrorism, and hybrid wars remain permanent a threat, and their consequences could have different manifestations. In the coming period, more sophisticated threats such as man-made epidemics/pandemics, attacks with biological and chemical weapons, attacks from virtual space, and hybrid influence will be focused more and more on the vital infrastructures of society and the state, too. Adding to that the indirect and direct endangerment of the natural environment, which causes natural disasters to occur

[a] ORCID: 0000-0002-7225-0493

in more frequent periods, creates a picture of an unsafe way of living in the coming period with the impossibility of predicting the ultimate implications.

Critical infrastructure protection is viewed from different positions: technical, defense, economic, national security, etc. The urgency of critical infrastructure protection stems from the fact that these systems are connected and highly vulnerable, and the number of malicious activities directed against processes and activities in society and the state is growing. Criticality assessment is approached from economic, political, and functional aspects. The Economic element indicates the importance of some infrastructure and the entire Economic system. The political aspects take into account the ownership of critical infrastructure, the stability of political conditions or systems in the environments or countries where critical infrastructure is located, and the functional aspect looks at the extent to which the absence of service of a network or infrastructure affects the functioning of the economy, service activities, healthcare, education, and communal services to the preservation of public order and peace and the usual way of life (Maksimovic, 2013).

This paper aims to discuss the topic of critical infrastructure relations on a global scale. It will cover the relationships between major geopolitical players such as Russia, USA, China, India, Great Britain, France, Japan, as well as companies like Facebook, Twitter, Shell, Huawei, and more. The paper will begin by presenting the current security environment, followed by the basics of critical infrastructure protection. It will then provide brief comments on the methodology and focus on specific infrastructures that can have a significant impact on the world if they fail or are destroyed. The paper will also discuss how this impact is manifested or can be manifested globally.

2. CONTEMPORARY SECURITY ENVIRONMENT

Various reports, including EMDAT (2023), highlight the increasing prevalence of natural, technogenic, and anthropogenic hazards in our daily lives. While these threats have existed for centuries, their impact was less significant. There are more than 8th billion people on the planet, billions of factories, cars, trains, planes, buildings, and they depend on electricity, chips, computers, GPS, oil, gas and etc. Most of those entities are very important in order to sustain everyday life. So, they are supposed to be protected in order to sustain our daily routines.

Natural hazards have always existed, and they are not a new phenomenon for humans. However, the way these hazards have impacted people over the last century has completely changed the relationship between humans and nature. Humans have been exploiting natural resources without considering the possibility of replenishing them for future generations. As a result, nature is fighting back and destroying important infrastructure that is vital for human survival and well-being. This is not a conspiracy theory, but rather a consequence of the destructive actions taken by humans towards the environment.

Moreover, there are many technological complexes that support human life on earth or they make it better. Some of those complexes are very dangerous such as nuclear power plants. Any technical failure caused by technological processes, human intervention, or natural hazards can produce huge damage to the population and nature for many years. A similar situation is with the chemical industry which is very dangerous for the population around those facilities. Those factories were built near to the towns but in the last fifty years towns have gotten closer to them and those factories are now in the suburbs of the towns.

However, man, even though it is not the biggest, it is the most significant producer of real dangers. Man can cause, sometimes directly and sometimes indirectly, some natural or technogenic disasters, but a large part of the dangers can still be attributed to man's activities.

His activities and influence on nature, other people, infrastructure, space, etc., can cause huge changes in those areas and in overall human life on Earth. Wars, exploitation of minerals, and deforestation are the most dangerous activities of humans that can cause its destruction.

All those three different types of hazards in the last hundred years are in expansion. Also, there is no possibility to protect everything that is important at all times, and there is no 100% security. Taking it under consideration it is important to decide what kind of "entity" should be protected and which is not so important. In that way, the "critical entities" or "critical infrastructure" are selected.

3. CRITICAL INFRASTRUCTURE PROTECTION

Many scientific papers in the world and neighboring countries discuss the topic of critical infrastructure. Over the past decade, this issue has become a crucial part of security discussions. It has become apparent that safeguarding everything all the time is not feasible and thus must decide which infrastructure holds the highest priority and the reason behind it. Critical infrastructure protection (CIP) is a complex topic that involves politics, business, technology, and risk. Although everyone recognizes the importance of critical infrastructure, there is still no universally accepted definition or list of what constitutes critical infrastructure. This lack of agreement leads to different approaches to defining critical infrastructure and determining how best to protect it.

Despite all this diversity, the common denominator is the importance of that infrastructure. The first broad definition of CI was: "Critical infrastructure consists of those facilities, networks, services and physical and information technology assets that, if interrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning government in member states. Critical infrastructure spans many sectors of the economy, including banking and finance, transportation and distribution, energy, utilities, healthcare, food supply and communications, as well as key government services" (COM (2004) 702).

In particular, the new definition of critical infrastructure given in Directive 2022/5557/EC should be highlighted. According to that document, "critical infrastructure" means an asset, facility, equipment, network, or system or part of an asset, facility, equipment, network, or systems needed to provide the key services. It should be noted that the key term in this document is "critical entity" and the entire document is oriented towards that term, which means that "critical entity" is a public or private entity that the member state has determined belongs to one of the categories given in the document and those categories are divided in there are 11 sectors, ten subsectors, with 52 categories of subjects. This new document on the resilience of critical entities in the EU was prepared based on a study conducted by the European Commission in 2019, study related to the implementation of the previous directive on the identification and marking of European critical infrastructure and the assessment of the need to improve its protection (Directive 2008/114/EC). Directive 2022/5557/EC does not mention European critical infrastructure but critical entities of particular European importance (providing the key services to six or more EU member states).

With these divisions, certain differences were made between key infrastructure, which the EC now calls critical entities, and critical infrastructure, which represents specific elements, thus making a clear distinction and resolving confusion between these two terms, thus clarifying the difference and defining more clearly what is protected. The characteristics of critical infrastructure facilities are:

- Long-term construction - from design to start of work;

- The specificity of the assessment of the endangerment of the object of critical infrastructure;

- Most often, in terms of infrastructure, they are complex constructions (chemical laboratories with auxiliary facilities, school buildings with playgrounds, energy infrastructure facilities - with piers, auxiliary buildings, helipads, etc.);

- Provision of the same is specific;

- Use of specific equipment when performing work and protection activities;

- The destruction or even partial damage of just one object can cause incalculable losses in human and material resources, but also cause the collapse of energy systems, pollute the human environment, or destabilize the banking or financial sector of a country for a long period of time.

For the provision of individual objects of critical infrastructure, an immediate (special) assessment is also carried out, which in principle should contain:

- The state of international relations in the global and regional field (decisions of the main geopolitical actors, decisions and implementation of the activities of organizations and associations in the field of security and defense, etc.);

- Challenges, risks, and threats with indirect and direct impact on the object (situation on the territory, possible types of natural and technical-technological threats, situation in the immediate environment, etc.);

- State of transport, and connections in the environment;

- Cooperation with civil institutions in the environment;

- Required number of personnel and material and technical means and

- The type, strength, and tasks of the personnel guarding the facility.

The protection of each object of critical infrastructure is specific for itself or has specifics that make it different from the others. The constituents of critical infrastructure protection can be divided into three segments: security management that plans, organizes, and implements tasks in the field of critical infrastructure protection; physical security and technical security.

Looking at the characteristics of critical infrastructure from a security point of view is not just a simple sum of factors for which an assessment is made. According to their purpose, such facilities are highly dependent on their way of organizing protection and directly and indirectly dependent on critical infrastructure protection systems in the country.

It should be borne in mind that critical infrastructure will be, in the future, a priority issue for consideration by the government, social, and private sectors. International cooperation and intra-state apparatuses in the modern world provide guidelines, strategies, doctrines, assessments, and other legislative acts that direct development and technical-technological progress, while due to capitalism and the era of globalization, private companies (with or without a share of state capital) specialized in certain disciplines take over jobs.

The destruction of the critical infrastructure elements or destruction in its entirety can cause long-term consequences for the socio-economic life in the area, implying pollution of the human environment, for a long period (no agriculture, investments, transportation, or other activities in that area).

Paying attention to preventive measures is crucial. These measures aim to minimize the likelihood and impact of accidents, and they are:

- measures foreseen by the selection of technical and technological solutions that ensure the safe transport of hazardous materials within the company;

- measures that ensure high-quality and timely maintenance of the technical and technological level of the facility - plant, level of knowledge, level of work, and technological discipline;

- measures intended for the maintenance of communication roads and passages in buildings, plants, and plants;

- measures provided for in the security system: supervision, management of security and protection systems, detection and identification of hazards. (Micovic, 2016:161)

The main prerequisite for preserving infrastructure as an international entity is to organize its protection. Experience shows that three models of protection can be determined: centralized, decentralized, and integral. Which model individual countries will approach depends on several conditions, the most important of which are the state of security in the country, contractual obligations between the state and the private sector, the geographic position of the critical infrastructure facility, the development of information technologies, etc.

4. METODOLOGY

The main hypothesis in this work is: The contemporary security environment in the world is very challenging in the context of critical infrastructure protection taking into consideration that the biggest geopolitical players are interested in protecting critical infrastructures as long as it is not against their interest.

In this paper, the conclusions were driven, through some examples of the world's important structures and the way the geopolitical players are dealing with them and through analysis of the importance of those infrastructures for the world and their influence in case of malfunctions or destruction.

5. DISCUSION

To understand challenges in critical infrastructure protection, the best way is to show some real examples. Those situations are interesting from the position of great powers and the geopolitical perspective of world security. The way the countries deal with critical/key infrastructure/entities and the influence of destruction is important but most of the world's critical infrastructures do not depend on them. That kind of infrastructure is in the hands of just 1% of the wealthy Western population. Every day people rely on essential infrastructure like communication, food, and water. However, they lack the ability to safeguard that and to persuade leaders to maintain her safety.

One of the freshest examples is the destruction of the North Stream. In the context of this work, it is not important who did it, it is something else. The North Stream was and is a key infrastructure for the German economy, and it means the European Union economy. Also, it is a key infrastructure for Russia taking into consideration the capacity of the stream and the costs to build it. It became a key infrastructure for two continents. In the end that structure was destroyed. It caused big economic losses for Germany/EU and Russia. Moreover, this structure was destroyed on purpose. One of the conclusions from this example can be that there is no 100% security and there is no structure that cannot be destroyed, on purpose or not. One of the triggers to destroy some infrastructure on purpose can be the geopolitical and economic interest of some states but more and more for big corporations and even individuals who see an opportunity to earn money if that infrastructure is destroyed or damaged. They do not care

for ordinary populations and the needs of ordinary people. It is egoism which was not seen up to now, through all history of mankind.

Submarine cables play a critical role in global interconnected networks, carrying about 99 percent of international communications traffic (Brake, 2019). According to "TeleGeography", in early 2023, there were 552 active and planned submarine cables which are nearly 1.4 million kilometers long (Submarine Cable, 2023). There is a huge amount of information that are going through those cables. Destruction of some of them will have an impact on the world. There are about 200 failures each year and the vast majorities are caused by humans (Griffiths, 2019). However, those are short failures and not made on purpose in most of the cases. Also, natural disasters can cause failure of that infrastructure, too. That key infrastructure exists and works as long as it is important for all to exchange information, earn money, and communicate with each other. Destruction of those cables would cause losses in money and no one is prepared to destroy some of them, yet. Also, there is no full security and it is not possible to protect that entire infrastructure for all time.

Very important world infrastructures are some channels such as Suez Channel and Panama Channel. The last incident with the mega-ship Ever Given, which got stuck in the canal in March 2021, showed all the importance of the channel for the world economy. The same situation is with the Panama Channel which has also a similar role. Moreover, this incident showed that jamming the Suez Channel was very simple to do. That key world infrastructure showed that is very vulnerable. However, the geopolitical players have interests in the Suez Channel depending on their global position and economic benefits. At the moment when some of the world powers decide that the destroyed or jammed Suez Channel could be used for their interests they would easily block it, even destroy it.

In accordance with European Directive 2022/5557 on the resilience of critical entities the space is one of the sectors of critical entities. In that context categories of entities are operators of ground-based infrastructure, owned, managed, and operated by Member States or by private parties, that supports the provision of space-based services, excluding providers of public electronic communications networks. One of those space-based services is communication. Satellite communication services are used every day for telecommunications, TV and radio broadcasting, high-speed Wi-Fi and mobile broadband, navigation and GPS (Global Positioning System) etc. From this point is very important to notice that space and infrastructure over the Earth are crucial for the life of people in these contemporary times. The existence of just one Global Positioning System, which could be vulnerable, and easily blocked or interrupted, pushed other cosmic powers to make and develop their systems similar to GPS (Russian Глобальная навигационная спутниковая система – GLONASS and China The BeiDou - Navigation Satellite System), or to launch their satellites to be independent. In that direction are heading also India, The European Union, and Japan. This kind of communication is very fast but also very sensitive. Today, there are many weapon systems that can intercept signals from satellites, make some interruptions, or even destroy satellites. However, satellites are useful to everyone and all powers are using them. On another hand, satellites can be destroyed very easily and it can cause a world crisis.

Those are just four examples related to infrastructure that can be important for most of the world even if it looks local. That infrastructure depends on the will of geopolitical power would it be destroyed or not and in what percentage, It is a big danger for the world and ordinary people. In that kind of scenario, it is possible to point the finger at some countries, but there will be no consequences for them. It means that 99% of the world's population is at the mercy of global players and the global elite. On them is the decision would we have the internet, access to a bank account, information, what should we watch on TV, what kind of food and

from which part of the world would be delivered, how big prices would the population pay for basic needs, etc.

6. CONCLUSION

The importance of infrastructure is directly related to the number of people who could be affected if it were destroyed or stopped from working due to various reasons, such as human actions, technology issues, or natural disasters. While there are numerous sectors and subsectors that can be significant, critical infrastructure should provide essential services such as transportation, energy, finance, healthcare, water, food, communication, and administration. To provide these services, countries use different types of infrastructure and rely, most of the time, on critical infrastructure for global services such as transportation, internet, communication, energy, etc.

However, most of the countries have limited control over this infrastructure. Mostly major geopolitical players ultimately decide whether it will be in functions or accessible, based on their own interests. This means that a single individual or one country can determine whether people worldwide can access certain resources and infrastructures or not.

REFERENCES

Brake D. (2019). Submarine Cables: Critical Infrastructure for Global Communications. Available from: https://itif.org/publications/2019/04/19/submarine-cables-critical-infrastructure-global-communications/ Accessed: 20023-08-23

COM (2004) 702. Communication on Critical Infrastructure Protection in the fight against terrorism. Final, Brussels. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52004DC0702 Accessed: 2023-07-28

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114 Accessed: 2023-07-28

Council Directive 2022/5557/EC of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available from: https://eur-lex.europa.eu/eli/dir/2022/2557/oj Accessed: 2023-07-28

EMDAT. (2023). 2022 Disasters in numbers: Climate in action, Available from https://cred.be/sites/default/files/ 2022_EMDAT_report.pdf Accessed: 2023-05-12.

Griffiths J. (2019). The global internet is powered by vast undersea cables. But they're vulnerable. Available from: https://edition.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html Accessed: 2023-08-19

Maksimovic G. (2013). Model upravljanja kriznim situacijama u Republici Srpskoj, Fakultet za bezbjednost i zastitu. Banja Luka.

Micovic M. D. (2016). Bezbednosni apekti funkcionisanja kriticne infrastrukture u vanrednim situacijma – doktorska disertacija. Univerzitet u Beogradu. Fakultet bezbednosti. Beograd.

Submarine Cable Frequently Asked Questions. Available from: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions Accessed: 2023-08-20