Space Critical Infrastructures as Part of Critical Infrastructures: Threats and Methods of Protection

Maksym Sokiran

Ph.D. in Law, Doctoral Student, Scientific Institute of Public Law
(Kyiv, Ukraine)

E-mail: maxim.sokiran@gmail.com
https://orcid.org/0000-0002-1682-2012

Sokiran, Maksym (2020) National Space Activities: Modern Realities and Legal Challenges. *Advanced Space Law*, Volume 5, 101-107. https://doi.org/10.29202/asl/2020/5/11

This article is devoted to the problem of protecting critical space infrastructure as one of the main elements ensuring national security in general, as well as the safety of the population. This article will discuss such concepts as critical infrastructure and critical space infrastructure as one of its parts, the threats faced by states, and ways of protection. It will also consider several national strategies for protecting such infrastructures, the need for cooperation at various levels, which will ensure security in this area, and a quick response to threats. The author offers the following definition of critical infrastructure. The critical infrastructure of Ukraine is systems and resources, physical and virtual, that ensure the normal functioning of the state, ensure an adequate standard of living for the population, extraneous interference in the work of which will lead to negative and unforeseen consequences in the life of the society and may constitute threats to national security.

Keywords: critical infrastructure, space critical infrastructure, space, cyberspace, cyberthreats

Received: March 03, 2020; accepted: April 04, 2020

Introduction

The rapid development of the modern world carries many advantages on the one hand, but also hides many threats. Today it is difficult to imagine a typical day, without the use of modern technology. We perform many daily operations using cyberspace: work processes, payment for services, information transfer, and many other things. Advanced technology is penetrating deeper into our lives. In confirmation of this, we can cite the example of the Internet of things, which is gradually being increasingly introduced into our homes. Ordinary everyday things of life are able to collect and send information.

© Sokiran, Maksym, 2020

But are we adequately prepared for the threats that such integration of cyberspace into the physical world carries? Experts predict that IoT devices run the risk of becoming the primary targets for hackers, since all these gadgets were created without taking into account the need for protection against cyber threats.

If the most ordinary things can become tools of cybercriminals, then what can we say about equipment that is of strategic value to states and is part of a critical infrastructure. Unfortunately, world experience is such that it is almost impossible to predict the nature of the attack and where it will come from. What remains for states is to repel attacks and adapt defense systems after the fact, enhancing protection based on previous threats and their analysis.

One way to respond quickly is to enact appropriate legislation, a protocol and response instructions, staff training, and so on. One of the most important aspects is cooperation between states, between states and the private sector.

Concepts and features of critical information infrastructure

To date, there is no single unified international concept of critical infrastructure. Different states give their definitions of what critical infrastructure is. It should be noted that in spite of the proximity of definitions of the term in the legislation of various countries and international organizations, there are some differences that obviously reflect national or organizational specifics of the application of the term (Biryukov, 2012).

Below we will consider some definitions of what critical infrastructure is.

According to Art. 2 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of critical European infrastructures and the assessment of the need to improve their protection "critical infrastructure" means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions (Council, 2008). Also, this Directive contains four-step instructions for determining what constitutes critical infrastructure, which Member States should be guided by.

A slightly different definition contains American legislation. The American Heritage Dictionary defines the term "infrastructure" as "The basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions including schools, post offices, and prisons" (The American, 2000).

The Council established by P.L. 98-501, provided yet another definition of "infrastructure." The Council's report characterized "infrastructure" as facilities with high fixed costs, long economic lives, strong links to economic development, and a tradition of public-sector involvement. Taken as a whole, according to the Council, the services that they provide "form the underpinnings of the nation's defense, a strong economy, and our health and safety." Under this definition of "infrastructure," the Council included highways, streets, roads, and bridges; airports and airways; public transit; intermodal transportation (the interface between modes); water supply; wastewater treatment; water resources; solid waste; and hazardous waste services (Fragile, 1988).

In Germany, critical infrastructure includes "the organizational and physical structures and objects so vital to the society and economy of the country that their failure or deterioration will result in persistent supply disruptions, significant disruption of national security or other dramatic consequences" (National, 2009).

As previously stated, we can see that the definition of critical infrastructure is different in different countries.

In 2015, Ukraine also prepared and published Green Paper on the protection of Ukraine's critical infrastructure. The Green Paper is designed by the objectives of the Annual National Program of cooperation between Ukraine and NATO in 2015. The Green Paper raised the issue of establishing in Ukraine system of critical infrastructure protection. The formulated strategic goals of public policy in the protection of critical infrastructure in Ukraine, the principles of protection of critical infrastructure and objectives of such protection.

In Ukraine, the term "critical infrastructure" is often used in legal documents. For the first time in official documents term "critical infrastructure" appeared in 2006 in the text "Recommendations of parliamentary hearings on the development of the information society" but without further development. In the National Security Strategy "Ukraine in a Changing World" (2012), the term mentioned in determining ways to strengthen energy security and the directions information security. In the new National Security Strategy of Ukraine (2015), the term "critical infrastructure" used in more detail. First, among "actual threats to national security" threats to critical infrastructure distinguishes also a separate section "Cybersecurite threats and security of information resources" (Biryukov, 2012). In July 2019, the Cabinet of Ministers of Ukraine approved the general requirements for cyber defense of critical infrastructure. The decision was made in the framework of the implementation of the Law of Ukraine "On the basic principles of ensuring cybersecurity of Ukraine".

The Green Paper on Critical Infrastructure Protection in Ukraine offers the following definition: "Critical Infrastructure of Ukraine is systems and resources, physical or virtual, that provide functions and services that will lead to the most serious negative consequences for society, socio-economic development countries and national security" (Biryukov, 2012).

According to the author, the emphasis on the fact that these are physical and virtual systems and resources is significant. Such a description corresponds to the real situation of the modern world, namely the transition to cyberspace.

In turn, the author offers the following definition of critical infrastructure. The critical infrastructure of Ukraine is systems and resources, physical and virtual, that ensure the normal functioning of the state, ensure an adequate standard of living for the population, extraneous interference in the work of which will lead to negative and unforeseen consequences in the life of the society and may constitute threats to national security.

Existing threats to critical infrastructure and how to protect it

Critical infrastructure failures can occur for various reasons and can be caused by many factors. In most cases, they are the result of intentional (vandals, criminals, terrorists, hacker attacks, and others), accidental (natural disasters, human factors, force majeure circumstances), or due to incorrect decisions (whether in the field of design, management or regulation). It is also important to note that critical infrastructure failures can occur regardless of whether the equipment is connected to the global network or is operating in closed mode. The functioning

of critical processes in most critical infrastructure increasingly depends on information and communication technologies. Therefore, the undisturbed functioning of critical infrastructure depends on the security of information assets, hardware, software, information-based processes, and internal an external communication networks and links. These assets include process control systems and networks that monitor and control the physical processes of critical infrastructure (Luiijf, 2012).

The tasks of protecting critical infrastructure are many and complex problems because they can consist not only of system systems, but also of interconnected and international software management systems, where individual violations can be associated with unexpected consequences and entail a domino effect. In this case, it is necessary to have a reliable and reliable infrastructure, which can be crucial from the point of view of economic, economic or social points of view and will help to accelerate the elimination of the consequences of interference with critical infrastructure (Roman et al., 2007).

Today, there are two main areas of threat to critical infrastructure. It is technical and human.

Technical level. Since, as previously mentioned, critical infrastructure facilities are directly related to the life of the state and citizens. Earlier, the author described how deeply integrated technology into our lives. With addiction comes vulnerability. At the first level, this vulnerability is associated with the danger of system failures, which can have cascading effects that affect not only an individual, but also disrupt the regular operation of entire sectors of social activity and security (Glorioso & Servida, 2012).

Various technical malfunctions, malfunctions in the software, hardware, foreign interventions, attacks, failures due to the human factor are one part of a possible source of disturbances in the operation of critical infrastructures. The second is the various catalysis, natural interventions, and natural wear of equipment. All these factors must be considered when developing instructions and programs for protecting critical infrastructures.

Actor level. Triggered by the pervasive societal dependence upon information and communication technology, the second area of vulnerability is the one linked to the potential malevolent agency. The panoply of malevolent agents deploying their activities in and/or through cyberspace is vast, but can be generally categorized into four elements. These include — in decreasing order of gravity — state-sponsored actors, ideological and politically extremist actors, frustrated insiders, organized criminal agents, and individual criminal agents (Glorioso & Servida, 2012).

The Green Paper identifies the following categories of threats which should be set to the protection of critical infrastructure:

a) accidents and technical failures, including aviation disasters, nuclear accidents, fires, accidents in the power system, the emissions of dangerous substances, the rejection of accidents and emergencies caused by negligence, institutional mistakes etc.;
b) natural hazards, including extreme weather conditions, forest, steppe and peat fires, seismic phenomena, epidemics and pandemics, cosmic phenomena, hurricanes, tornadoes, earthquakes, tsunamis, floods, etc.;
c) malicious acts, including malicious actions of individuals or groups such as terrorists, criminals and saboteurs, and military operations in war (Biryukov, 2012).

Protecting critical infrastructure is strategically important. At the same time, it is decentralized, interconnected, interdependent, and controlled by many actors (includes partial

ones) and includes various types of technologies. The consequences can be serious, even if interruptions do not last long (Cukier, 2005).

The standards governing the protection of critical infrastructures are placed in various regulatory documents at various levels. They can be divided into national defense strategies, documents governing the protection of specifically critical infrastructures, and documents governing a particular area taken.

Slightly more specific protection goals are found on the second level of critical infrastructure protection strategies. They are more precise and specific than the protection principles, but still follow a systemic-abstract logic, as they refer to the totality of all critical infrastructures rather than to one sector or one infrastructure. Examples for "protection goals" on this aggregated level are the goals of "identifying critical infrastructures and key resources," "enhancing resiliency," or "analyzing interdependencies and vulnerabilities." These goals, formulated for all critical infrastructures, can be described as "protection policies," as they define in a general way what must be protected from which threats in what way. The third level is the sector-specific dimension. On this level, the "protection goals" are more concrete. Examples are the goals to ensure "the availability, integrity and confidentiality of information and information technology" or "sustain protection of public health and the environment." They may be referred to as (sector-specific) "protection goals" (Cavelty & Suter, 2012).

It is essential to understand that protecting critical infrastructures is not a one-off event. This is an area that must constantly be dynamic, develop, use new technical solutions, improve and update equipment, and at the same time, remain flexible and quickly respond to any changes and quickly cope with any external factors that threaten any element of the infrastructure.

Space infrastructure

One of the most vulnerable sectors of critical infrastructures, on which the stability of other components can also depend, is space infrastructure. Orbital stations, space satellites, other space equipment, perform an incredibly important function in the modern world. In addition to scientific research, space equipment performs many tasks that directly affect our lives. For example, it is meteorological satellites, communication satellites that provide signal relay between points on the surface of the earth, satellite navigation systems. To date, satellites are actively used in rescue operations. They allow the researcher to take pictures, for example, from territories that are under the influence of any natural disasters, without endangering people and continue to carry out rescue operations. Outer space is also actively used for military purposes. There is a separate category of satellites, such as military, the placement of weapons in space, which is controlled from the ground. On the one hand, for a simple layman, space may seem so far away, and on the other hand, the threats, with unauthorized access to space infrastructure, are more than real and carry great danger.

As we can see, space equipment is actively used in various fields, including ensuring the normal functioning of the state and individuals. Today, there are a number of regulatory acts, national and international, that regulate outer space, allow it to be used in a civilized manner by various states, provide for registration and accounting of space equipment, and regulate the safety of space operations.

Another aspect that complicates the development of defensive strategies is the confidentiality and secrecy of data related to attacks on space infrastructures, if any. Unlike most other critical

infrastructures, where the private sector is widely present, space infrastructures are under state jurisdiction.

In the course of studying this topic, the author found a study that simulates an attack on space infrastructure and shows its vulnerability. This study is described in the article "Cyber Defense of Space-Based Assets: Verifying and Validating Defensive Designs and Implementations" (Byrnea et al., 2014). In this paper, the researchers modeled a reconnaissance attack on space mission systems that were considered safe. Safety was ensured by following standard punctures and a safety plan.

The knowledge that was obtained as a result of this experiment made it possible to find and identify vulnerable areas that should be strengthened in the future in order to build more reliable systems to counter cyber threats. The study demonstrates how individual machines, which themselves are protected, when assembled into one single system, become unsafe. Having obtained a result in which the system is not secure, the researchers planned work to create rigorous methodologies and tools for repeated cyber defense testing. Along with this, a specialized stand for cyber defense is being developed, which in the future will help simulate attacks and improve defense systems.

The author shares the point of view of the research that threats develop and improve much faster than tools to protect against them. Therefore, it is essential, through various experiments, to identify weaknesses in the protection of space infrastructures, since the consequences of interventions in their work can become fatal.

In the field of space infrastructure, cooperation with the private sector is also important, as in any other area where critical infrastructures are present. This cooperation should be based on the principles of trust, confidentiality, and security of information and mutual partnership.

Conclusions

Today, mankind has already entered the era of technology, and the changes that this era has brought into the usual life order are already irreversible. What awaits us in the future is a deeper integration of cyberspace into the physical world. It is foolish to deny all the privileges that it gives, how it simplifies life. And do not underestimate the threats that these changes entail. Data insecurity and the crimes associated with this, cyberattacks, hacking, and more, are no longer surprising.

In this new picture of the world, critical infrastructures seem to be unprotected, and especially space critical infrastructure. The inability to predict the source and nature of attacks reduces the effectiveness of their defense. Today, threats are adapting to protection systems in order to circumvent them, much faster than the system is able to improve to protect itself. Preventive measures are ineffective. Separate elements, which themselves are protected, gathering in a single system, can not resist threats and can cause a domino effect.

The solution to the problem lies in several planes. In addition to improving the technical base, it is necessary to adopt a series of ordinary acts at different levels that would regulate the space sphere and identify it as a critical space infrastructure, along with other critical infrastructures.

Cooperation with the private sector based on the principles of transparency, security, confidentiality, and mutual exchange of information is also essential. That would make it possible to use the principle of synergy in work between the parties and, as a result, to get a system more resistant to threats.

🕮 References

Biryukov, Dmytro (2012) Strategy of protection of critical infrastructure in the national security of the state. *Strategic priorities*, Vol. 3 (24).

Byrnea, DJ, David Morganb, Kymie Tana, Bryan Johnsona, and Chris Dorrosa (2014) Cyber Defense of Space-Based Assets: Verifying and Validating Defensive Designs and Implementations. *Procedia Computer Science* 28 pp. 522 — 530. https://doi.org/10.1016/j.procs.2014.03.064

Cavelty, Myriam Dunn and Manuel Suter (2012) The Art of CIIP Strategy: Tacking Stock of Content and Processes. *Springer-Verlag,* Berlin, Heidelberg, pp.15-39. https://doi.org/10.1007/978-3-642-28920-0_2

Council of the European Union. Council Directive (2008) 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Cukier, Kenneth (2005) Ensuring (and Insuring?) Critical Information Infrastructure Protection, *Rueschlikon Conference on Information Policy*.

Fragile Foundations: A Report on America's Public Works (1988) Final Report to the President and Congress. National Council on Public Works Improvement. Washington D.C. February. https://www.infrastructurereportcard.org/wp-content/uploads/2017/03/1988-Fragile-Foundations-ExSum.pdf

Glorioso, Andrea and Andrea Servida (2012) Infrastructure Sectors and the Information Infrastructure. *Springer-Verlag Berlin Heidelberg*, pp. 39-52. https://doi.org/10.1007/978-3-642-28920-0_3

Luiijf, Eric (2012) Understanding Cyber Threats and Vulnerabilities. *Springer-Verlag Berlin Heidelberg*, pp 52 — 68. https://doi.org/10.1007/978-3-642-28920-0_4

National Strategy for Critical Infrastructure Protection (2009) Federal Ministry of Interior, Germany. https://www.bundesregierung.de/breg-en/service/information-material-issued-by-the-federal-government/national-strategy-for-critical-infrastructure-protection-cip-strategy--736048

Roman, Rodrigo, Cristina Alcaraz, and Javier Lopez (2007) The role of Wireless Sensor Networks in the area of Critical Information Infrastructure Protection. *Information Security Technical Report*, Vol.12, Issue 1, pp 24–31. https://www.nics.uma.es/pub/papers/Roman2007a.pdf

The American Heritage Dictionary of the English Language (2000) Fourth Edition: *Houghton Mifflin Company*.