Theoretical Approaches to the Definition of "Critical Space Infrastructure"

Maksym Sokiran

Ph.D. in Law, Post-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) Theoretical Approaches to the Definition of "Critical Space Infrastructure." *Advanced Space Law*, Volume 6, 54-63. https://doi.org/10.29202/asl/6/6

The article analyzes various scientific approaches to the definition of such interdependent concepts as "critical space infrastructure" and "critical information infrastructure." To clarify these concepts, the legislative initiatives of different countries are compared. It is concluded that despite the lack of a legitimate definition of "critical space infrastructure," it is a complex system consisting of physical and virtual information resources that need to be controlled and secured because if it is vulnerable (not resistant to risks), it can lead to a crisis many vital systems of any state in general or in a particular industry — in particular. Therefore, it needs new approaches to protect it from attacks.

Keywords: space, critical infrastructure, attacks, protection, critical objects, law, information

Received: 1 November 2020 / Accepted: 27 November 2020 / Published: 10 December 2020

Introduction

Critical space infrastructure is closely linked to two factors: space and critical information infrastructure. Space exploration began in the mid-20th century, and interest in critical information infrastructure was linked to the initiatives of several governments, which since the late 1990s have recognized the importance of its smooth functioning for the well-being of their populations, economies, and so on.

The modern world generates a staggering amount of data and therefore continues to grow exponentially in the capacity to store, broadcast and calculate this information, with experts suggesting that the installed capacity for storing information in the coming years will reach 2.5 zetabytes (2.5 x 1021 bytes) (Yiu, 2012). Research by the International Data Corporation shows that the world's digital information doubles every two years and has increased fifty-fold between 2011 and 2020 (Gantz & Reinsel, 2011).

The public and private sectors are increasingly using these vast amounts of data using a variety of methods, from sophisticated market analysis to creating a new business model. Therefore, key sectors of modern society, including the national security sector, using space resources to improve the digital society, rely on interdependent national and international management software systems for their smooth, reliable and continuous operation.

Critical space infrastructure is a relatively new area related to space systems, facilities and technologies, as well as the multifaceted interaction required to maintain vital social functions (is health, safety, economic and social well-being), loss or breach of which could have a significant impact on almost any nation (Georgescu et al., 2019).

Thus, before we reveal the concept of "critical space infrastructure," it is necessary, as we defined above, to define what is "critical information infrastructure." Hence, we analyze all elements of this concept, namely "critical," "information," and "infrastructure."

The concept and meaning of the term "infrastructure"

The term "infrastructure" comes from the Latin infra — "below," "under" and structura — "building," "location" and was used in ancient Rome when it came to aqueducts and a complex sanitation system (Nakamura et al., 2019). And given that they were, for the most part, located underground, hence the name — infrastructure (that which is located under the building), this is relevant today because the systems that are part of the infrastructure, such as gas, water, sewerage and other is located underground.

Infrastructure is a set of specific forms, methods and processes, as well as various structures and communications that provide general conditions and normal functioning of economic, social, environmental and other spheres of society, its reproduction and development. These conditions are created by a complex of economic branches, a system of technical and technological, organizational, social, communication interrelations of all infrastructure elements (Savchenko, 2020).

The large explanatory dictionary of the modern Ukrainian language gives the following definition of infrastructure — a set of industries and activities that serve the productive and non-productive sectors of the economy (transport, communications, utilities, general and vocational education, health care, etc.) (Large, 403).

Thus, in the present conditions, under infrastructure refers to any object that we use, perceived as something ordinary — because it works for us in the background. Infrastructure refers to the basic systems and services that a country or organization needs to function properly and includes all physical systems, as well as services that can be provided by law enforcement, emergency services, health, education, and others. Thus, infrastructure may include road and rail systems (for example, tunnels and bridges); transit system (for example, planes, buses, subways, trains, etc.); energy generating system (for example, power plants, wind power plants, hydroelectric power plants, etc.); power grid (for example, power lines and connections); communication system (telephone cables and mobile phone towers); reservoirs and dams; pumping stations and sensors; ports, airports, waterways and canals; firefighting equipment and personnel; health services, hospitals, clinics and emergency response systems; educational institutions, including schools, colleges, universities and other educational institutions for adults and children; police and prisons; facilities for garbage removal and storage, sewerage and treatment facilities.

However, the understanding of infrastructure covers not only the above facilities but also operational procedures, management practices, and development policies that interact with public demand and the physical world to facilitate the transportation of people and goods, drinking water and other miscellaneous uses, the safe disposal of society's waste, the provision of energy where needed, and the transfer of information within and between communities.

Infrastructure systems usually require large initial investments because they are important for productivity in the economy. Most projects are either fully funded by the government or substantially subsidized. Therefore, in the Keynesian economy, the term "infrastructure" referred only to government assets that facilitate production — it did not include private assets for the same purpose. However, in post-Keynesian times, this term is becoming increasingly popular. Its meaning has also expanded. Today, it also includes any technological system or business organization (Nebava, 2020).

But as for developing countries, the development of the private infrastructure system in them was not as dynamic as in developed countries. This had a number of objective reasons: due to the limited supply of long-term foreign currency financing for infrastructure projects; lack of local currency financing options to support infrastructure, largely due to the limited development of the local capital market; lack of banking projects developed by the private sector to facilitate private sector investment; and limited government capacity to support the development of public infrastructure projects. Therefore, in 2002, the Private Infrastructure Development Group (PIDG) was established, an innovative infrastructure development and financing organization that provides the infrastructure in the poorest and most volatile countries. By funding private initiatives for affordable and sustainable infrastructure services in low-income and fragile states to combat poverty and promote economic growth (Our history, 2020).

The world community and its institutional structures, such as the World Bank Group, also help developing countries build smart infrastructure that supports inclusive and sustainable growth, expands markets, creates opportunities for work, promotes competition and promotes a cleaner future. Infrastructure improves lives by connecting people to opportunities (Infrastructure, 2020).

Thus, by infrastructure, we mean the resources and assets that are necessary for the smooth functioning of the economy and society.

In turn, space infrastructure is a set of facilities and structures of industrial, technical, transport, information and social spheres for effective research and use of outer space in the national interests, international cooperation and security (Soroka, 2020).

Criticality and its elements

Now let us analyze the next element of the studied phrase — the word "critical." The large explanatory dictionary of the Ukrainian language gives the following definition of the concept of critical — it is in a state of crisis (in an extremely difficult, dangerous, predicament situation). That is, if this definition is applied to infrastructure, it becomes critical if, in the event of its failure, the entities that use it become extremely complex, difficult, dangerous and difficult.

According to Carl von Clausewitz, in order to better understand the sign of criticality, it is necessary to investigate the following elements (Gnatyuk et al., 2015; 271):

a) *critical capabilities* — abilities (power) of the object that make it key in the context of a particular scenario, situation, or task;
b) *critical needs* — conditions, means, resources, methods or methods of action that allow the object to achieve critical capabilities;
c) *critical vulnerability* — the most vulnerable need or component, the failure of which will not allow objects to achieve critical capabilities or perform a task.

On the one hand, need a clear and stable definition of critical assets (objects) to know what assets to protect and how well they protect. Otherwise, there is a risk of protecting too many objects, protecting the wrong objects. On the other hand, if you arbitrarily limit their number due to lack of funds, you can miss a dangerous vulnerability. Clear criticality criteria are also important for actors in shaping future critical infrastructure rules. Thus, if we do not understand what the concept of "criticality is," it can lead to inefficient use of already limited resources of the state.

The list of objects that can be considered critical in different countries is different. It depends on national traditions, social and political beliefs, as well as geographical and historical characteristics of each state. Different scientists also use different theoretical models to understand what criteria to use to determine which objects are critical and which schemes to use to protect them.

In addition to the above theory of Carl von Clausewitz, there are others. For example, the authors Sergiy Gnatyuk, Victoria Sydorenko, Oksana Duksenko in work "Modern approaches to the detection and identification of the most important objects of critical infrastructure" singled out the following: the theory of self-organizing networks Albert-Laszlo Barabashi; graph theory; asset priority model; identification of critical infrastructure objects based on categorization or simulation (Gnatyuk et al., 2015; 271). Analyzing all the above theories, the authors conclude that today there are a sufficient number of approaches to identifying the most important critical infrastructure. However, to assess the feasibility and effectiveness of their use to identify critical infrastructure, it is necessary to analyze them according to the following basic criteria (Gnatyuk et al., 2015: 272):

a) *clarity of formalization* (clarity and intelligibility of mathematical calculations);
b) *ease of implementation* (no overly complicated procedures);
c) *flexibility and versatility* (the ability to change certain parameters as needed and used in various fields of human activity);
d) *accuracy* (high degree of approximation of the true value of a certain parameter);
e) *efficiency* (ability to perform calculations correctly and quickly);
f) *information component* (taking into account the peculiarities of the construction of information systems and networks, cyberspace architecture);
g) *objectivity* (possibility of completely independent evaluation).

Thus, summarizing the existing approaches to identifying and identifying the most important critical infrastructure, the following conclusions can be drawn: they are all focused on military, technogenic, economic, environmental, and other security systems of the state, while not paying enough attention to the information component.

As we have already noted, the legal definition of critical infrastructure in most countries has evolved over the years and has varied according to national priorities. The generalization of the existing legal framework for the definition of this term allows us to state that critical

infrastructure is systems or assets that are vital for the country (Council, 2008). Refusal to use such systems or their temporary incapacity will have a detrimental effect on security, the economy, or other important indicators for the country. Critical infrastructure protection is now seen as an integral part of the national security of many countries around the world. It can be argued that critical infrastructure is a "vulnerability generator," the location and interdependence of which can spread risk in any area.

Along with the concept of "critical infrastructure" in the scientific literature often uses the term "critical objects," drawing attention to the social and organizational context, not focusing only on technical resources, but different interpretations are more related to institutional practice than to significant differences in the terms themselves.

In Ukraine, the term "critical infrastructure" is also beginning to be used frequently in legal documents. The term "critical infrastructure" first appeared in official documents in 2005 in the text of the "Recommendations of Parliamentary Hearings on the Development of the Information Society." Where in paragraph 6. "Information security," it was recommended to prepare proposals for the identification and protection of critical information infrastructures (Recommendations, 2005). And then, for ten years, there was a law-making pause on this issue.

Only on 23 August 2016, the Resolution of the Cabinet of Ministers of Ukraine "On approval of the Procedure for forming the list of information and telecommunications systems of critical infrastructure of the state" was adopted, which defined critical infrastructure, according to which critical infrastructure is defined as "a set of infrastructure states that are most important for the economy and industry, the functioning of society and public safety and the decommissioning or destruction of which may affect national security and defense, the natural environment, lead to significant financial damage and human casualties" (On approval, 2016).

In turn, the objects of critical infrastructure are enterprises and institutions (regardless of ownership) of industries such as energy, chemical industry, transport, banks and finance, information technology and telecommunications (electronic communications), food, health, utility economy, which are strategically important for the functioning of the economy and security of the state, society and population (On approval, 2016).

In the latest National Security Strategy of Ukraine "Human Security — Country Security," which was put into effect by the Decree of the President of Ukraine of 14 September 2020 No 392/2020, the country's leadership recognized that in order to carry out digital transformation, provide administrative services through secure "single window" with the use of modern information technologies, it is necessary to develop a system of cybersecurity, which is a guarantee of cyber resilience and cybersecurity of the national information infrastructure, in particular in the context of digital transformation (National, 2020).

Thus, critical information infrastructure systems are becoming increasingly interconnected with the introduction of online service systems and other space technologies. And with the growth of interdependencies of critical information infrastructure, an increase in threats follows and creates the risk of disrupting most vital systems' work. Not only are information systems susceptible to failure, but they are also potentially attractive targets for malicious attacks. Since they provide a wide range of services on which people and society as a whole depend, any damage or interruption to critical information infrastructure will cause fluctuations in other important systems of the state.

Thus, although critical information infrastructure is an element of critical infrastructure, information and communication technologies have become comprehensive, connecting other infrastructure systems, they become interconnected and interdependent. In this regard, the information component is becoming increasingly important.

Information component

An important component of the critical information infrastructure is its information component, which we will analyze. The term "informational" comes from the word "information," which is information about any events, someone's activities, etc., a message about something (Large, 2001).

The word "information" is Latin. Over its long life, its value underwent an evolution, expanding or extremely narrowing its boundaries. Therefore, the author interprets the term "information" in a rational way, and Academician Nikita Moiseev even believed that due to this concept's breadth, there is no and cannot be a strict and sufficiently universal definition of information **(**Moiseev, 2001).

Information and its properties are the subjects of research in a number of scientific disciplines, such as information theory (the mathematical theory of information transmission systems), cybernetics (the science of communication and control in machines and animals, as well as in society and human beings), semiotics (the science of signs and sign systems), the theory of mass communication (the study of the media and their impact on society), informatics (the study of the processes of collection, transformation, storage, protection, search and transmission of all types of information and means of their automated processing) and a number of others (Types, 2020).

From a worldview point of view, information is a reflection of the real world. Information — building up knowledge, developing knowledge, updating knowledge that arises in the process of goal-setting intellectual activity of a person. No information, no knowledge appears immediately: their appearance is preceded by the stage of accumulation, comprehension, systematization of experimental data, opinions, views, their comprehension and rethinking. Knowledge is the product of this stage and this process. Thus, information is a certain sequence of information, the knowledge that is actualized (received, transmitted, transformed, compressible and/or recorded) using some signs (symbolic, figurative, gesture, sound, sensorimotor type) (Kaziev, 2001).

Information can be of different types. For example, it can be positive or negative; religious, scientific, every day, aesthetic, and so on.

Victor Kaziev gave the following classification of information: by stage of use (primary, secondary); for completeness (excessive, sufficient, insufficient); in relation to the purpose of the system (syntactic, semantic, pragmatic); in relation to the elements of the system (static, dynamic); in relation to the structure of the system (structural, relative); in relation to system management (managing, advising, converting, mixed); in relation to the territory (federal, regional, local, related to a legal entity, related to an individual, mixed); by access (open or public, closed or confidential, mixed); by subject area, by the nature of use (statistical, commercial, normative, reference, scientific, educational, methodical, etc., mixed) and others (Kaziev, 2001).

Regarding the legal definition of the term "information," it is provided in the basic Law of Ukraine "On Information," which states that information is any information and/or data

that can be stored on physical media or displayed electronically (About information, 1992). Without going into a discussion about the completeness of this definition, then in formulating the definition of "critical information infrastructure," we will proceed from the legislative definition of information.

Analysis of the concept of "critical information infrastructure"

As we have noted, in the information age, information infrastructure has become one of the most important critical infrastructures, as it now lays the foundation for the management and integration of all other critical infrastructures, as well as new forms of communication, information exchange and trade. For example, we can see that Internet services have become so widespread that the Internet is now critical to the infrastructure of countries. Moreover, some countries include Internet services in their legal frameworks for critical infrastructure protection.

Today, there is no single common definition of what a critical information infrastructure is. It should be noted that despite the similarity of the definitions of this term in the legislation of different countries and international organizations, there are some differences that obviously reflect the national or organizational specifics of the term.

In turn, the lack of the concept of "critical information infrastructure" in the legislation of some countries can be explained by the fact that the information component is part of the concept of infrastructure in general (is critical infrastructure) and is not identified as a specific link (Gnatyuk et al., 2014).

But let us analyze the legislation of countries such as Australia, Britain, Canada, the Netherlands, and the United States. We can conclude that they have developed a common view of critical information infrastructure. In their regulations, these countries understand the term "critical information infrastructures" as "information systems (software, hardware and data) and services that support one or more critical infrastructure objects, the disruption or disconnection of which causes serious damage to the functioning of dependent critical infrastructure" (International, 2009). In addition, in some countries (such as Malaysia) especially emphasizes the value of critical infrastructure for the nation, even the concept of "critical information infrastructure" is used in the sense of "critical national information infrastructure" (Gnatyuk et al., 2014).

Thus, the analysis of regulations of different countries on the definition of the term "critical information infrastructure" shows that there is no common and sustainable definition; there are both differences and commonalities that are common to most countries that have adopted such documents; it is common that critical information infrastructure is considered in the context of national security.

Regarding the scientific definition of the term "critical information infrastructure," we also have different views. For example, the authors of the article "Legal aspects of the formation of security systems of critical information infrastructure in Ukraine" give the following definition: information flows, organizational structures, has a regulatory mechanism that ensures their effective functioning. The special place of the critical information infrastructure determines their key role in ensuring the proper functioning of almost all spheres of society and the state — political, economic, social, environmental, military and information (Yesimov et al., 2018).

Critical information infrastructures can be described as the part of the global or national information infrastructure that is necessary to ensure the continuity of critical infrastructure services. They have a physical component consisting of high-speed interactive narrowband and broadband networks; satellite, terrestrial and wireless communication systems; computers, televisions, telephones, radios, and other products that people use to access infrastructure (Cavelty & Suter, 2012).

Critical information infrastructure is considered as the basis of other critical infrastructures. This is because the constant exchange of data is important for the operation of the infrastructure and services provision. Therefore, today it is more important to give priority, first of all, to the protection of information infrastructure, rather than work on the protection of the entire critical infrastructure.

Speaking of Ukraine, it has only just begun to identify critical information infrastructure concepts and develop a cybersecurity strategy for Ukraine. It can be argued that the key factor in this was the attack of the Black Energy virus. The procedure for forming the list of critical information infrastructure facilities, which was approved by the Resolution of the Cabinet of Ministers of Ukraine of 9 October 2020 No 943 "Some issues of critical information infrastructure facilities" in which critical infrastructure is also defined as a set of critical information infrastructure facilities (Procedure, 2020). As for the definition of "critical space infrastructure," today there are only a few publications on this issue, so there is a real problem regarding the legal regulation and, consequently, the legal protection of critical infrastructures in general and space systems in particular.

Conclusions

Thus, critical space infrastructure is a complex system consisting of physical and virtual information resources that need to be controlled and secured because if it is vulnerable (not resistant to risks), it can lead to a crisis of many vital systems of any state in general or a particular industry — in particular. And which needs new approaches to protect it from attacks. Cyber-attacks have persuaded the world community to pay attention to "cascading" events and their impact on the global network society, as they are highly complex and have non-linear pathways leading to secondary events and consequences.

Thus, a critical information infrastructure that is not stable in terms of security, together with space technologies, has the effect of a "force multiplier," which makes it possible to achieve a much greater impact even with a relatively small threat. Therefore, it is necessary to adopt the Law of Ukraine "On the Protection of Critical Space Infrastructure."

🕮 References

About the Statement of the Order of Formation of the List of Information and Telecommunication Systems of Objects of a Critical Infrastructure of the State (2016) The Resolution of the Cabinet of Ministers of Ukraine from 23 August, No 563. Available online: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF

About Information (1992) Law of Ukraine, 2 October, No 2657-XII. Available online: https://zakon.rada.gov.ua/laws/show/2657-12

Cavelty, M., and M. Suter (2012) *The Art of CIIP Strategy: Tacking Stock of Content and Processes*. Springer -Verlag Berlin Heidelberg, 15-39

Gantz, John and David Reinsel (2011) *Extracting Value from Chaos*. June. Available online: http://www.emc.com/digital_universe

Georgescu, Adrian Gheorghe, Marius-Ioan Piso, and Polinpapilinho F. Katina (2019) Critical Space Infrastructures. *Risk, Resilience and Complexity*. Springer International Publishing. https://doi.org/10.1007/978-3-030-12604-9

Council Directive 2008/114/EC (2008) 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG

Gnatyuk, Sergiy, Miroslav Ryaby and Victoria Lyadovska (2014) Definition of Critical Information Infrastructure and its Protection: Analysis of Approaches. *Communication*, No 4. Available online: http://con.dut.edu.ua/index.php/communication/article/view/1102/1041

Gnatyuk, Sergiy, Victoria Sydorenko and Oksana Duksenko (2015) Modern approaches to critical infrastructure object detection and identification. *Ukrainian Scientific Journal of Information Security*, Vol. 21, Issue 3, 269-275. https://doi.org/10.18372/2225-5036.21.9690

Infrastructure (2020) *World Bank*. Available online: https://www.worldbank.org/en/topic/infrastructure

International Critical Information Infrastructure Protection Handbook 2008-2009 (2009) Edited by A. Wenger, V. Mauer & M. Cavelty. Center for Security Studies, ETH Zurich.

Kaziev, Victor (2001) Introduction to system analysis and modeling. Information and system. *3.1. The concept of information, types of information*. Available online: http://bigc.ru/theory/books/kvisam/glava3.php

Large explanatory dictionary of the modern Ukrainian language (2001) Compiler and chief. ed. W. T. Busel. Irpen: VTF "Perun."

McGaughey, Katryn (2011) *World Data More Than Doubling Every Two Years Driving Big Data Opportunity New IT Roles*. Dell Technologies. Available online: https://corporate.delltechnologies.com/en-us/newsroom/announcements/2011/06/20110628-01.htm#:~:text=%E2%80%94June%2028%2C%202011%E2%80%94EMC,which%20is%20growing%20faster%20than

Moiseev, Nikita (2001) *Universum. Information. Society.* Series "Library of the journal Ecology and Life." Series "Organization of the World." Available online: https://www.litres.ru/nikita-moiseev/universum-informaciya-obschestvo/chitat-onlayn/

Nakamura, Hideo, Kotaro Nagasawa, Kazuaki Hiraishi, Atsushi Hasegawa, KE Seetha Ram, Chul Ju Kim, and Kai Xu (2019) *Principles of Infrastructure Case Studies and Best Practices*. Asian Development Bank Institute and Mitsubishi Research Institute, Inc. Available online: https://www.adb.org/sites/default/files/publication/502801/adbi-principles-infrastructure-case-studies-best-practices.pdf

National Security Strategy of Ukraine "Human Security — Country Security" (2020) Put into effect by the Decree of the President of Ukraine of 14 September, № 392/2020. Available online: https://zakon.rada.gov.ua/laws/show/n0005525-20#Text

Nebava, M.I. (2020) Theory of Macroeconomics. *6.4 Keynesian theory of state regulation of the economy.* Available online: https://web.posibnyky.vntu.edu.ua/fmib/14nebava_teoriya_makroekonomiki/64.htm

On Approval of the Procedure for Forming the List of Information and Telecommunication Systems of Critical Infrastructure of the State (2016) The Resolution of the Cabinet of Ministers of Ukraine of 23 August 2016 No 563. Available online: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF

On the Basic Principles of Cybersecurity of Ukraine (2017) Law of Ukraine of 05.10.2017 № 2163-VIII.

Our history (2020) *PIDG LTD*. Available online: https://www.pidg.org/about-us/our-history/

Procedure for Forming the List of Critical Information Infrastructure Objects (2020) Resolution of the Cabinet of Ministers of Ukraine of 9 October 2020, No 943 "Some Issues of Critical Information Infrastructure Objects." Available online: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF/ed20201009#n24

Recommendations of the Parliamentary Hearings on the Development of the Information Society in Ukraine (2005) Resolution of the Verkhovna Rada of Ukraine of 1 December, 2005 No 3175-IV.

Savchenko, O. (2020) Infrastructure. *Institute of Encyclopedic Research of the National Academy of Sciences of Ukraine.* Available online: http://esu.com.ua/search_articles.php?id=12489

Soroka, Larysa (2020) *Administrative-legal Mechanism for the Implementation of the Space Doctrine of Ukraine*. Dissertation for the degree of doctor of law in the specialty 12.00.07. Dnipropetrovsk State University of Internal Affairs, Dnipro.

Types of Information and its Properties (2020) Wikibooks — open books for the open world. Available online: https://ru.wikibooks.org/wiki/%D0%92%D0%B8%D0%B4%D1%8B_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8_%D0%B8_%D0%B5%D1%91_%D1%81%D0%B2%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%B0

Yiu, Chris (2012) *The Big Data Opportunity: Making Government Faster, Smarter and More Personal*. London: Policy Exchange. Available online: http://ict-industry-reports.com.au/wp-content/uploads/sites/4/2013/05/2012-The-Big-Data-opportunity-in-Government-UK-Policy-Exchange-July-2012.pdf

Yesimov, Serhiy, Ruslan Skrynkovsky, Myroslav Kovaliv, and Ihor Kret (2018) Legal aspects of the formation of the security system of critical information infrastructure in Ukraine. *Traektoriâ Nauki = Path of Science*. Vol. 4, No 7. https://doi.org/10.22178/pos.36-2