UDC 001.8

# Features of Ensuring Cybersecurity of the Critical Infrastructure of the State

Yuriy Danyk[1], Chad Briggs[2], Tamara Maliarchuk[3]

[1] *Ivan Chernyakhovsky National Defense University of Ukraine, Kyiv, Ukraine*
[2] *University of Alaska, Anchorage, USA*
[3] *Ivan Franko Zhytomyr State University, Zhytomyr, Ukraine*

## Abstract

One of the most important tasks of national security in modern conditions is to ensure the security and stable functioning of critical infrastructure of the state. Control systems are an integral and most vulnerable part of critical infrastructure facilities. This determines the importance of ensuring they are protected from destructive cyber actions. Destructive cyber actions in it is accompanied, as a rule, by chain effects and synergistic effects that systematically influence and cover all other spheres of the life of society and the state, both in ordinary and, especially, in critical conditions. The authors systematically and comprehensively analyzed and presented in the article the results of investigations of the features of destructive cyber actions in the critical infrastructure of state, counteracting them and protecting from them.

*Keywords*: cybersecurity; cyberspace; cyber-attack; cyber defense; high tech war; hybrid warfare; critical infrastructure

## Introduction

In high tech conflicts of any intensity, hostilities (operations) and other (non-force) actions, mainly economic, political, diplomatic, informational, psychological, cyber, cognitive, etc. [1], are mutually coordinated according to a single plan. The impacts are felt on all spheres of life, on all sectors of society and throughout the state. Thanks to the use of innovative technologies, it became possible to shift conflict from predominantly overt and forceful (kinetic) means [2], to less obvious strategies focused on the structural vulnerabilities critical infrastructure and society of adversaries in cyberspace.

What are often missed are the broader strategic goals of an adversary in undertaking a modern war campaign, and the broad spectrum of tools used to achieve those goals. The purpose of this article is to illustrate and explain the use of cyber weapons against critical infrastructure of the state.

The targeting of critical infrastructure is an effective way to increase vulnerability of a state or society, while signaling to other potential adversaries their own vulnerabilities and the potential to cripple large sectors of the economy. Cyber tools provide an asymmetric advantage without regard to geographic distance, meaning small groups can inflict widespread damage while avoiding normal attribution and rules of deterrence [3].

Critical infrastructure and cyber attacks are a useful place to start because of the existing history of attacks, and the similarities shared between states in their need to protect the critical infrastructures control system, and their vulnerabilities to cyber tools.

In modern conditions, these opportunities are used with high efficiency to achieve various goals by both state and non-state actors. The Stuxnet worm (possibly attributed to Israel and the US), was effective at inflicting physical damage on nuclear fuel centrifuges not connected to any outside network and regarded by the Iranians as safe from outside interference or attack [4]. Stuxnet was an elegant piece of programming that could easily move from computer to computer without detection, not harming or interfering in any system until it finally found its way to specific computer-controlled centrifuges in Iran. Once there, the worm would make slight changes to the operation of the high-speed machines, shifting the calibration just enough to damage or destroy them, without raising suspicion that an outside attack was occurring. Likewise, China and even smaller powers such as North Korea possess anti-infrastructures cyber capabilities, and non-state actors such as Al Qaeda and ISIS have also exhibited notable cyber-attack capabilities against critical infrastructure [5].

## Features of protecting the critical infrastructure of the state from destructive cyber impact in modern conditions

As Conklin and Kohnke wrote, much of cyber security has been built around the concept of 'walling off' computer systems to outside intruders, and protecting data rather than focusing on the resilience of the system as a whole. Their argument was to focus more on functionality than individual attacks, a focus that already exists in the critical state infrastructure, for example, energy sector but indicates a mismatch between energy security and the vulnerabilities present in infrastructure from cyber-related systems [6]. We will consider the features of protecting the critical infrastructure of a state from destructive cyber impact in modern conditions using the energy sector as an example, since energy security

from cyber-attacks is based on a broader concept of sustainability, which is associated not only with the actual production and transmission of energy, but for those systems that have energy supports and legitimizes. Remove energy from a society, particularly highly industrialized and technology-dependent countries, and it is pulling the proverbial rug out from under all support systems.

Resilience networks can be modeled according to the type and pattern of connections (topology) between different parts of the system, whether these are individuals, electrical connections, or ecological relationships. Since network connections are functional, they are rarely random, and instead center on critical nodes which provide crucial links within the system. In ecological sciences, these critical nodes are often referred to as "keystone species," which even if they are not the most visible representatives of an ecosystem, are crucial to its effective functioning. In social systems, these critical nodes may be key individuals or centers of community activity, which provide a focus in connection between people who otherwise may not interact. And with the Internet, critical nodes are either the more visible centers of activity such as Google, or can be represented in terms of key servers or communication lines. In all of the above cases, however, these networks are often known as "scale free," meaning they tend to be resilient because random failures at any part in the system can be compensated for [7].

Energy networks are often configured differently, as instead of being resilient and allowing for rerouting of power in the case of failure; traditional energy infrastructure has been constructed on centralized nodes. The pattern of energy infrastructure from the twentieth century was one of large power plants (either fossil or nuclear fueled), which then transmit electricity to population centers, with corresponding subnetworks of electrical transformers [8]. Much of the work on increasing resilience of energy systems has focused on preventing cascading failures in electrical networks, where failure of a few critical nodes propagates blackouts over large geographic areas, as witnessed numerous times in North America. This was a form of resilience, but one coupled with aspects of fragility, meaning the system was brittle and could easily be broken with enough external force. The experience of Puerto Rico in the wake of Hurricane Maria in 2017 has been an unfortunate case in point [9]. Civilian resilience for the energy sector focus less on the power plants themselves, although increasingly environmental factors have overwhelmed the ability of large power plants to withstand flooding and other environmental hazards. While the Fukushima disaster in 2011 was the most visible example, increasingly energy utilities in North America and Europe have become more vulnerable [10].

Social, political, and energy networks do not operate independently, but are instead "nested" in one another. Highly resilient social and political bonds are based on activities that cannot operate for long without more fundamental energy and environmental networks. This leaves even the healthiest of social networks vulnerable should supporting energy networks be compromised. As a basic need, utilities such as energy, water, and sewage reflect upon the legitimacy of governing powers, and trust in these institutions quickly weakens when basic services cannot be met. In Kosovo, for example, despite high public trust in security provided by NATO/KFOR in the country, the electrical utilities KEK and KEDS are publicly maligned and distrusted, and although privatized still negatively and severely affect public perceptions of government legitimacy and trust in security [11]. In Iraq, US armed forces carried out research that indicated those areas of Baghdad (particularly Sadr City) where insurgents had cut access to water, electricity, and sewage, were highly correlated with support for the insurgency [12]. Sparking instability with basic services can be an effective and deniable way to undermine a society and leaving it more vulnerable. For countries such as Ukraine, with its traumatic experience of the Chernobyl disaster in 1986, the links between energy security and government legitimacy may be even more fragile.

## The use of information and cyber technologies for destructive actions in the energy sector in modern high-tech wars (hybrid wars, conflicts)

Modern society almost completely depends on the state of security of information and cyber-infrastructure in all spheres of human activity. Not only government structures of states, but also criminal and terrorist organizations have the opportunity to use information and cyber technologies, information and communication networks to achieve their goals. It provoked the provision of cyber and information security of critical infrastructure of the state became a critical condition for ensuring the state's defense capability, its economic and social development. The destructive geopolitical actors (DGAs - *the destructive geopolitical actors are states, terrorist organizations or groups of people conducting attacks against national security of the state*) have been willingly and diverse to use the cyberspace of Ukraine as a cyber art theater and a cyber weapons' testing ground. In many cases, cyberattacks were aimed at the Ukrainian electricity distribution system, disabling for a long time objects of economy, infrastructure and housing.

The deep penetration of energy in all sectors of the economy and in the social sphere determines its special role in ensuring the security of modern society development. Energy security characterizes the degree of energy (power) complex performance of its functions to society, the state in ordinary, critical and extraordinary circumstances [13]. Enterprises and institutions of the energy sector play a leading role in the development of the state [14]. Industry remains the main consumer of electricity, although its share in total electricity consumption in the world is decreasing. Electricity in industry is used to activate various mechanisms and directly technological processes. Nowadays the coefficient of electrification of the power drive in the industry

is 80%. In this case, about 1/3 of electricity is spent directly on technological needs [15]. The objects of the energy sector are strategically important objects and must function continuously and qualitatively [16].

On the territory of Ukraine, in each region there are energy structures that belong to the critical infrastructure. Each of them possesses so-called "critical nodes", which when disrupted lead to a breakdown in network functionality and potentially spark cascading failures across networks.

The energy structural elements all relate to a certain hierarchy, control system and security system. The basis of electricity is the united power system of Ukraine, which centralizes the supply of electricity to domestic consumers, as well as its exports and imports. The system combines 8 regional power systems (Dniprovska, Donbas, Western, Crimean, Southern, Southwest, Northern, Central), interconnected by system-generating and interstate high-voltage transmission lines. According to the State Statistics Committee of Ukraine, the largest share of electricity is produced in thermal power plants - about 50%, at NPPs (nuclear power plants) - 45%, and in hydroelectric plants - 5%.

## Threats in the Energy Sector

The whole set of threats that can affect the functioning of power systems can be conventionally divided into ordinary threats (probable failures and accidents) and extraordinary (unique due to the origin, nature of development and consequences). Various forms of reserving capacities, the development and transportation of fuel and energy resources, systems of guaranteed energy supply and the creation of reserves of fuel and energy resources serve to counteract unusual threats in power systems. Such ordinary phenomena almost exclude threats to energy security in conditions of development and functioning of national economy. In contrast, unusual effects can negatively affect the energy complex as a whole. Among the extraordinary threats, the cyber threats play a leading role. Cyber threats are able to provoke such problems as the violation of the provision of energy resources and emergency situations in the power complex of the state. They are implemented in the form of a variety of destructive cyber effects.

Destructive Cyber Effects can be

- Targeted attacks (Advanced Persistent Threat);
- Effect on control systems;
- Effect through social networks;
- Attacks on banking systems (theft of money);
- Hardware bugs (instrument bugs) in chips and firmware of computer and network equipment.

Such cyber threats can be realized by influencing both the entire all critical infrastructure of the state as a whole and its individual elements separately, as well as with the achievement of synergy of the results. The impact can be carried in a complex, simultaneously, sequentially or mixed on an automated control system, personnel, on the financial system, on the hardware and software complex. The most vulnerable place in the objects of critical infrastructure of the state is automated control systems.

## Analysis of Cyber Effects on Objects of Critical Infrastructure of the Energy Sector

The problem of cyber security of state energy sector is crucial for national security and defense, economic and social development.

In 2014-2018 well-planned synchronized cyber effects were conducted on objects of Power Complex different states of the World. It gave the opportunity of control to violators for some period of time, and in some cases even of destruction of management and normal functioning of elements of Power Complexes. The possible goal of these attacks could be check of cyber security system reliability of state critical infrastructure and peculiarities of cyber security system functioning of power companies and their reactions to different cyber effects and incidents. It was shown that too complex control over information systems make objects of critical infrastructure of the state vulnerable for cyber-attacks. The most dangerous cyber effects on objects of critical infrastructure of the state are those, which provoke or are accompanied by destructive chain effects as directly on power object so and on connected with them objects of other objects of infrastructure and everyday life spheres of the state.

One more peculiarity of the cyber-attack on objects of Power Complex different states was the initial dispersion with final direction on defined systematic multispectral result and diverse effects.

During the analysis of cyber-attacks, it was found that the attacks were not solitary, but were conducted synchronously. All of them had a destructive effect on the control system of energy objects. The main synchronous destructive cyber effect was focused on the vulnerable elements of control systems. Before the main cyberattack, a preliminary cyberattack was conducted on the system of service and dispatching with the purpose of denial in service of consumers. For example in Ukraine the use of several destructive concentrated cyber-attacks on the power complex was carried out within the framework of a large-scale cyber operation aimed at violating simultaneously several objects of the power complex of Ukraine.

The groups responsible for many of the Ukrainian cyber-attacks, Telebots, Black Energy and Grey Energy, have been closely or more loosely linked with the intelligence agencies of the destructive geopolitical actors [17]. The lack of any direct attribution, however, does not diminish the strategic use of such tools to destabilize and delegitimize the Ukrainian state. On the contrary, such maskirovka approaches to conflict are prime examples of how cyber tools can be used in modern conceptions of hybrid warfare, where vulnerabilities of critical infrastructure are attacked in order to weaken state support and function, and increase distrust by potential outside partners. A secondary goal of cyber-attacks on energy infrastructure may be

to signal to others (e.g. UK, US, Germany) their own vulnerabilities, where Ukrainian attacks serve as proofs of concept. In either case, the activities of cyber attackers are highly coordinated, difficult to trace and attribute, and are highly asymmetrical, non-kinetic attacks. These attacks represent newly technical areas of conflict, particularly in cases where an unending state of instability is the goal, rather than the traditional concept of 'total victory' on the battlefield.

The control system is the most important components of the any power system. The control system of the power system plays a leading role in the functioning of the entire energy (power) complex of any state. A powerful cyber effect can be executed on the automated control system, which may lead to a violation of the control of a particular object of energy or the power complex as a whole. The automated control system of the power system should be resilient to cyber effects and have corresponding Complex Counteract System against cyber-attacks.

In December 2015, the Advanced Persistent Threat ("Advanced Persistent Threat") was fixed to an automated control system of power system. The internal networks of the Ukrainian power company PJSC "PrykarpattyaOblenergo" were attacked [18]. As a result of the cyber-attack, for several hours a large part of the region and the regional center remained without power supply. Thirty substations were shut down. About 230 thousand people were deprived of energy supply within one to six hours. During the attack, the malicious software Black Energy was applied [19]. The Black Energy group launched an attack on the Ukrainian power grid using the Black Energy and Kill Disk families. This was the latest known use of Black Energy malware in the real world. After the attack, the Black Energy group is divided into at least two subgroups: TeleBots and Gray Energy.

The main goal of the TeleBots group is to implement cyberattacks for sabotage in Ukraine, which is achieved through attacks on computer networks (CNA). The group has committed many devastating attacks, including:

- A series of attacks in December 2016 using an updated version of the same malicious Kill Disk software developed for Windows and Linux operating systems.
- A known Petya / NotPetya attack in June 2017 with a backdoors built into the MEDOC Ukrainian accounting program.
- An attack using the BadRabbit family in October 2017.

ESET specialists had been tracking the activity of the Grey Energy group for several years. The Grey Energy group uses a unique family of malware called Grey Energy. The design and architecture of this malicious software is very similar to the already known Black Energy family. In addition to the conceptual similarities of the malicious software, links point to the fact that the group behind the malicious software Grey Energy, closely cooperates with the group Tele Bots. In particular, the Grey Energy team developed a worm similar to NotPetya in December 2016, and later, an even more advanced version of this malicious program was used by the Tele Bots group during an attack in June 2017. It is worth noting that the Greenery group has broader goals than the Tele Bots group. Grey Energy is primarily of interest to the industrial networks of various critical infrastructure organizations, and unlike Tele Bots, the GreyEnergy group is not limited to Ukraine alone.

At the end of 2015, ESET specialists first spotted the malware GreyEnergy aimed at a power company in Poland. But later, as with Black Energy and TeleBots, the focus of the Grey Energy group was on Ukraine. The attackers first showed interest in the energy sector, and then to transport infrastructure and other important goals. The latest use of malware in GreyEnergy was reported in mid-2018.

The GreyEnergy malware is modular, and unlike Industroyer, ESET specialists have not detected any ICS-driven module, meaning targeted specifically for industrial control systems, yet such system can still be targeted using other methods. At least one case has been detected by the operators of this malicious software deployment. The module can clear the disk to disrupt business processes in the company and hide traces [20]. One of the most striking details revealed during the ESET study is that one of the detected samples of GreyEnergy was signed by a valid digital certificate, which was probably stolen from a Taiwanese company that manufactures ICS equipment. In other words, the GreyEnergy group literally followed Stuxnet development methods.

Moreover, synchronous attacks were carried out on power companies "Chernivtsioblenergo" and "Kyivoblenergo", but with lesser consequences. On December 23, 2015, unauthorized interference with the information technology system of remote access to telecontrol over equipment of substations of 35-110 kV PJSC "Kyivoblenergo" was carried out by an unauthorized group of people. From 15:31 to 16:30 local time, fifteen cities, towns and villages were completely or partially blacked out in Myronivsky, Makariv, Bila Tserkva, Fastovsky, Skvira, Rokitnyansky, Kaharlyk, Ivankivskyi and Yagotyn administrative districts. There were over 80,000 consumers without electricity. As a result of the attack there were failures in the system of remote access, 30 tie-stations were disconnected, which supply several strategic objects of the region: enterprises, institutions, organizations and the population. Electricity was restored at 18:56 on December23, 2015 [21].

The control system was vulnerable to cyber-attacks of this kind. The response to such a cyber-attack was not timely, and the security system failed to fulfill its functions. With malicious software, a cyber-attacker can control, and in certain applications, manage a part or whole automated control system. The consequences of such an attack may have been carried out in order to verify the functioning of the security system and the response system to the critical situation of the power company.

In general, the cyber-attack was comprehensive, and to a certain extent systemically organized, namely:

- Preliminary infection of networks with the help of counterfeit emails;
- Capture control over the automated control system by executing shut down of operations at substations;
- Failure of the elements of the automated control system;
- Deleting information on servers and workstations (Kill Disk utility);
- Attack on the telephone network of call centers, in order to ensure the failure to service current subscribers.

During the period from January 19-20, 2016, a cyber-attack was conducted with the help of the cyber tool JCATS (Joint Conflict and Tactical Simulation Enhancements), which was also aimed at disrupting the control system by installing malicious software that is sent by e-mail [22]. Another cyberattack, which was carried out at night from December 17 to December 18, 2016, was less scale-for-effect. The substation "Severnaya" of the power company "Ukrenergo" was disrupted. Consumers of the northern part of the city of Kyiv and the surrounding areas remained without electricity. The attackers did not cause significant damage, the purpose of the attack was "demonstration of force". As in previous cases, this attack was a part of an operation against state institutions of Ukraine [23].

The main features of Advanced Persistent Threats are the following:

- As a rule, they are targeted at elements of critical infrastructure;
- Conducted by a group of highly skilled hackers;
- Carefully masked using specially designed software tools (specialized Shell Codes, Root Kitta, etc.);
- Remain unknown for a long time;
- Reinforced by intelligence or destructive actions. APT are elements of intelligence and subversive operations.

The main cyberattacks differ in effects and way of operating. The attacks that were carried out in 2015 on energy companies were not fully self-organized. In 2016, malware already foresaw self-organization of actions in the process of attacks and actions became more operational. Also, experts from the company ESET, having conducted the research, stated that "Crash Override" is capable of physical destruction of power systems. Crash Override software [24] has the ability to send commands to the power grid to enable or disable power supply. According to their data, Crash Override can use the known vulnerability of Siemens equipment, in particular, the digital relay Siprotec. Such relays are installed for the protection, control and control over distribution and power supply networks. Mike Assante, from the American cyber security company SANS Institute, has determined that disconnection of the digital relay can lead to thermal overload of the power grid. This is a very serious threat to transformers and equipment that is under voltage. Thus, Crash Override can provide a planned attack on several "critical nodes" of the power complex. Then there is a probability of a power cut-off on the entire state, as the load moves from one region to another.

Automated power systems of power complexes are vulnerable to cyber-attacks. As a result of our analysis of the cyber-attacks we can separate individual categories of possible cyber-attacks:

- Target components: electronic computing devices such as Remote Terminals (RTUs) or the Human Machine Interface (HMI) [25] typically have an interface for remote setup or control. Through remote access, the attacker can intercept device control and cause malfunctions, e.g. make changes in the data transmitted to the operator, damage the equipment, complete or partial failure of the device.
- Protocols aimed at: nearly all modern data transfer protocols are well documented and their description is open source. For example, the DNP3 standard is common in North American energy control systems [26]. Its specification is available to anyone who wants a low price. An attacker can make changes to information that can lead to significant financial costs due to overproduction of electricity, switching on the power line during work on them, damage to the equipment, overloading the system.

On June 27, 2017, a large-scale destructive hacker attack ("Petya") was carried out on Ukrainian institutions and organizations. The "critical nodes" of the energy industry (Ukrenergo, Kievoblenergo, Dniproenergo, Zaporizhzhiaoblenergo, and Chernobyl Nuclear Power Station) also came under direct attack. The cyber-attack was aimed at violating the work of company web sites and the customer support systems. The damage to the information systems of Ukrainian companies was due to the updating of the software intended for reporting and document circulation - M.E.Doc. That is the installation of a backdoor in the M.E.Doc software update package. Simultaneously with the installation of the update package on the computers of the institutions and organizations, a backdoor was installed, which further promoted the installation of the virus "Petya".

On May 23, 2018, Cisco experts warned about the infection of more than 500,000 routers and systems in 54 countries, but the main goal for large-scale cyber-attacks could have been Ukraine [27]. The destructive software "VPN Filter" can be used to conduct such an attack, which allows attackers to intercept all traffic passing through the affected device (including authorization data and personal data of payment systems), collect and unload information, remotely control an infected device, and even make it out of order. There are also features for monitoring the Modbus SCADA protocols used in automated control systems.

All known cyber-attacks that have affected the functioning of critical infrastructure objects in the energy sector have been assessed in the preceding sections.

## Conclusions

The article considers ways and directions for the choice and implementation of rational approaches in solving the complex protection from destructive cyber effects of the state power complex. All major cyberattacks carried out at Ukraine Power Complex in 2014-2018 have been analyzed, which influenced the functioning of the objects of critical infrastructure. It was found that the cyberattacks were not solitary, but were conducted systematically. They had a complex destructive effect on energy management systems. It was established that the main destructive cyber effects were concentrated on the vulnerable elements (critical nodes) of the control systems of power complex objects. Before the main cyberattack, a cyber-attack was conducted on the system of maintenance and dispatching, with the purpose of refusing to serve the consumers. The use of several destructive concentrated cyber-attacks on the power complex was carried out within the framework of a large-scale cyberattack, which was aimed at simultaneously violating several objects of the energy industry.

It is established that critical infrastructure of the state depends on the level of cyber resistance of power objects. An analysis of cyber-attacks has shown that the minimum value of the level of stability can lead to the destruction of the power system (object, network).

The methods of realization of hybrid distributed cumulative cyberattacks with a chain effect on objects of critical infrastructure are described. The vulnerabilities of these objects are determined. It was established that cyberattacks, which were carried out through e-mail, provided access to the main servers to receive information about the state of the system's operation, to intercept the management of objects of the critical infrastructure of the state as a whole, and then to change the parameters of their functioning.

The authors developed a technique for detecting hybrid distributed-concentrated cyberattacks with chain effects using a model for intelligent recognition of cyber threats. They designed as well the organizational and technical measures to ensure cybersecurity in the critical infrastructure of the state. It has been shown that systematic measures aimed at timely detection of cyber threats, preventing and counteracting cyberattacks, will provide the necessary level of functional stability of critical infrastructure systems to destructive cyber effects. It will ensure their adequate respond to actual and potential threats, rationally using existing capabilities and resources of the state.

Aspects of cybernetic destructive actions in modern wars and armed conflicts are investigated on the basis of the analysis of the features of the hybrid war. It is substantiated that the provision of effective counteraction to destructive cybernetic influences requires the availability of cyber range. Definitions, principles and concept of construction of a complex cyber range for the study of hybrid cyber actions are proposed, as well as a list of problems to be solved to create a complex cyber range. The questions of methodology and applied aspects of creation and application of complex cyber range are considered. The basic structure and procedure for the practical creation and use of a comprehensive cyber range are presented.

Formation of the requirements for the structure and content of databases and knowledge bases of the proposed cyber range based on the results of its practical application and research of functioning during the specified tasks activities.

## References


[1] Y. Danyk, T. Maliarchuk, and C. Briggs, "Hybrid war: High-tech, information and cyber conflicts," *Connections*, vol. 16, no. 2, pp. 5–24, 2017. URL: http://connections-qj.org/article/hybrid-war-high-tech-information-and-cyber-conflicts.

[2] R. Wilkie, "Hybrid warfare: Something old, not something new," *Air & Space Power Journal*, vol. 23, no. 4, pp. 13–18, 2009. NicuPopescu. "Hybrid tactics: neither new nor only Russian." EUISS Issue Alert 4 (2015).

[3] Kerigan-Kyrou and Dinos, "Critical energy infrastructure: Operators, nato, and facing future challenges," *Connections (18121098)*, vol. 12, no. 3, pp. 109–117, 2013.

[4] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[5] L. Tichy and J. Eichler, "Terrorist attacks on the energy sector:," *The Case of Al Qaeda and the Islamic State, Studies in Conflict & Terrorism*, vol. 41, no. 6, pp. 450–473, 2018.

[6] W. A. Conklin and A. Kohnke, "Cyber resilience: An essential new paradigm for ensuring national survival," *In ICCWS 2018 13th International Conference on Cyber Warfare and Security*, p. 126, 2018. Academic Conferences and publishing limited, 2018.

[7] S. Dunn and S. Wilkinson, "Hazard tolerance of spatially distributed complex networks," *Reliability Engineering & System Safety*, no. 157, pp. 1–12, 2017.

[8] D. H. Kim, D. A. Eisenberg, Y. H. Chun, and J. Park, "Network topology and resilience analysis of south korean power grid," *Physica A: Statistical Mechanics and its Applications*, no. 465, pp. 13–24, 2017.

[9] M. Gallucci, "Rebuilding puerto rico's grid," *IEEE Spectrum*, vol. 55, no. 5, pp. 30–38, 2018.

[10] C. V. Mikellidou, L. M. Shakou, G. Boustras, and C. Dimopoulos, *Energy critical infrastructures at risk from climate change: A state of the art review.* Safety Science, 2017.

[11] K. C. for Security Studies, "Kosovo security barometer," 2018. http://www.qkss.org/en/Reports/Kosovo-Security-Barometer-Seventh-Edition-1050.

[12] D. E. Mosher, B. E. Lachman, M. D. Greenberg, B. Rosen, and T. Nichols, "Green warriors: Army

environmental considerations for contingency operations from planning through post-conflict," *Rand Corporation*, vol. 632, pp. 90–91, 2008.

[13] T. concept of the development of the security and defense sector of Ukraine, "introduced by the decree of the president of ukraine dated march 14," *No 92/2016*, 2016.

[14] C. S. of Ukraine, "approved by decree of the president of ukraine dated march 15, 2016 no 96," *Officer Vision of Ukraine*, no. 23, 2016.

[15] T. L. of Ukraine, ""basic principles for the cybersecurity of ukraine" no. 2163-viii of october 5, 2017.," 2017. [Electronic resource] - Access mode: http://zakon.rada.gov.ua/laws/show/2163-19.

[16] T. L. of Ukraine, "The national security strategy of ukraine, approved by the decree of the president of ukraine dated 05/26/2015 №287/2015.," 2015. [Electronic resource] - Access mode: http://zakon.rada.gov.ua/287/2015.

[17] Reuters, "Hackers accused of ties to russia hit three east european companies: cybersecurity firm," 2015. https://uk.reuters.com/article/us-russia-cyber/hackers-accused-of-ties-to-russia-hit-three-east-european-companies-cybersecurity-firm-idUKKCN1MR1BO.

[18] TEXTY.ORG.UA, "Russia's hacker attack on the ukrainian grid: how it was." [Electronic resource] - Access mode: https://texty.org.ua/articles/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak-66125/.

[19] B. Middleton, *A History of Cyber Security Attacks 1980 to Present*, vol. 253. New York, USA: Imprint Auerbach Publications, 1st edition ed., 2017. First Published 14 July 2017, eBook Published 28 July 2017.

[20] E. report, "Greyenergy: successor of blackenergy." Access mode: https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/.

[21] M. N. Time", "The largest cyber attacks against ukraine since 2014," 7 2017. [Electronic resource] - Access mode: https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html.

[22] Zillya!, "Antivirus has analyzed the cyber attacks on infrastructure objects in ukraine 02/27/2016, certificated for use by public and state authorities," 2 2016. Access mode: https://zillya.ua/zillya-antivirus-provela-analiz-kiberatak-na-infrastrukturni-ob-kti-ukra-ni.

[23] V. Chervonenko, "Was there a cyber attack on the power company?," *BBC Ukraine*, 1 2016. Access mode: https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc.

[24] B. Middleton, *A history of cyber security attacks: 1980 to present*. New York, USA: Auerbach Publications, 2017.

[25] M. BaqerMollah, "Sikder sunbeam towards ieee 802.22 based scada system for future distributed system," *Islam Cognitive Telecommunications Research Group, Dept. of Electrical and Electronics Engineering, International Islamic University Chittagong, Conference Paper*, 2012. Conference: Informatics, Electronics & Vision (ICIEV), 2012 International Conference Chittagong, Bangladesh, May 2012, DOI: 10.1109/ICIEV.2012.6317474, Access mode: https://www.researchgate.net/ publication/261081302_Towards_IEEE_80222_based_SCADA_system_ for_future_distributed_system [accessed Nov 14 2018].

[26] S. Mohagheghi, M. Mousavi, J. Stoupis, and Z. Wang, "Modeling distribution automation system components using iec 61850," *Power & Energy Society General Meeting.1 - 6. 10.1109/PES.2009.5275841*, 2009. Conference Paper August Conference: Power & Energy Society General Meeting, 2009, DOI: 10.1109/PES.2009.5275841. Source: IEEE Xplore.

[27] B. N. Ukraine and Technology, "Global ransomware attack causes turmoil, 28 june 2017," 2017. Access mode: https://www.bbc.com/news/technology-40416611.