Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

T. Maliarchuk, Yu. Danyk, Ch. Briggs
Connections QJ 18, no. 1-2 (2019): 93-110
https://doi.org/10.11610/Connections.18.1-2.06

Research Article

Hybrid Warfare and Cyber Effects in Energy Infrastructure

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

[1] *Zhytomyr Ivan Franko State University, https://zu.edu.ua/en_index.html*

[2] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," https://kpi.ua/en*

[3] *University of Alaska, Anchorage, USA, https://www.uaa.alaska.edu/*

Abstract: Energy is an integral part of all branches of the economy and social sphere, with a special role in ensuring the security of the development of modern society. Therefore, energy infrastructure has become a critical component of the hybrid war. Destructive cyber bullying 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 present in this article the results of investigations of the features of destructive cyber defects in the national energy sector of Ukraine and the ways of counteracting and protecting critical energy infrastructure.

Keywords: hybrid warfare, power complex, energy infrastructure, cybersecurity, cyberattack.

Introduction

Discussions of hybrid warfare have often centered on definitional debates over the precise nature of the term, and whether 'hybrid' covers what other military experts describe as nonlinear warfare, full-spectrum warfare, fourth-generation warfare, or other such terms. Similarly, discussions of cyber conflict have treated the phenomenon as a separate domain, as if using cyber tools remained distinct from other forms of conflict. A hybrid war that is *de jure* being conducted on the territory of Ukraine, and *de facto* encompassing more participants all over the world in terms of its content, forms, and methods of conducting, can be considered a specific variant of fourth-generation wars (4GW).

In hybrid conflicts of any intensity, hostilities (operations) are an element of other (non-force) actions mutually coordinated according to a single plan, mainly economic, political, diplomatic, informational, psychological, cyber, cognitive, among others.[1] This creates destabilizing internal and external processes in the state that is the object of aggression such as concern and discontent in the population, migration, and acts of civil disobedience. Hybrid wars are not declared and, therefore, cannot be completed in the classical sense of the end of wars and military conflicts. This is a kind of permanent war of variable intensity across multiple sectors, with cascading impacts and synergistic destructive manifestations, in which the entire population of the country and the international community are, to a certain extent, consciously or unconsciously involved. 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 to less obvious strategies focused on the structural vulnerabilities of adversaries, including (importantly) achieving cognitive advantage over them.

When applied to events in Ukraine since 2013, the primary focus has often been on the Russian invasion of Crimea in 2014, and the subsequent support of Russian backed enclaves in the eastern Ukrainian regions of Donbass and Lugansk. These operations, from the appearance of so-called “little green men” in Simferopol to the downing of Malaysian Airlines flight 17 several months later, focus on fairly conventional (if irregular) forms of conflict. What is often missed are the broader strategic goals of an adversary in undertaking a hybrid war campaign and the broad spectrum of tools used to achieve those goals.

As many authors have argued, hybrid warfare is not a new phenomenon, as it represents coordinated actions by both state and non-state actors to conduct a campaign of actions that span from information warfare to direct, kinetic conflict.[2] The strategies of the Russian Federation toward post-Maidan Ukraine have centered largely on the goals of destabilizing and delegitimizing the government, part of an effort to prevent Ukrainian integration with Western European institutions and to prevent effective intervention by Western or NATO countries.[3]

[1] Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs, “Hybrid War: High-tech, Information and Cyber Conflicts,” *Connections: The Quarterly Journal* 16, no. 2 (2017): 5-24, https://doi.org/10.11610/Connections.16.2.01.

[2] Robert Wilkie, “Hybrid Warfare: Something Old, Not Something New,” *Air and Space Power Journal* 23, no. 4 (Winter 2009): 13-18; NicuPopescu, “Hybrid Tactics: Neither New Nor Only Russian,” *EUISS Issue Alert* 4 (European Union Institute for Security Studies, January 2015), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_hybrid_warfare.pdf.

[3] Emmanuel Karagiannis, “The Russian Interventions in South Ossetia and Crimea Compared: Military Performance, Legitimacy and Goals,” *Contemporary Security*

While the occupation of Crimea and the continued conflict in eastern Ukraine help to serve this purpose, a larger but less visible array of actions have been undertaken to target the resilience of Ukrainian institutions. Rather than focus on the hybrid war itself, or cyber as a separate domain, the purpose of this article is to illustrate and explain the use of cyber weapons against the energy infrastructure.

Again, while not a new strategy, whether by insurgents or strategic bombing campaigns, the targeting of energy infrastructure is an effective way to increase the 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 that small groups can inflict widespread damage while avoiding normal attribution and the rules of deterrence.[4] During the Cold War, the United States conducted hybrid operations in countries such as the Philippines in the early 1950s and Vietnam in the 1960s, using an array of techniques from establishing newspapers and radio stations, to supporting insurgents and mercenaries, to the active involvement of US combat troops. The US experience may be instructive, in that it provides illustrations of two very different strategic goals in employing hybrid techniques – of either trying to stabilize or destabilize a foreign regime. While, in some cases, such as the Philippines, stabilization efforts were largely successful, in examples from Vietnam to Afghanistan, the US has had far less success in its stabilization efforts. Destabilization, on the other hand, appears to be a more commonly successful use of hybrid warfare techniques as, for example, in the controlled US actions in Central America and Chile, or in Iran in 1953.[5]

For purposes of this and subsequent articles, hybrid warfare is defined as the full-spectrum use of state and non-state instruments to shift the stability and legitimacy of key systems and institutions in a given region. Note that this, theoretically, means that hybrid warfare methods can be used to legitimate purposes as well as to destabilize, and this is often done when attacking an adversary while concurrently promoting support of one's own state and allies/ proxies. While the dual use of hybrid tools is not as obvious in the energy sector, this article is one of a series that also examines social resilience and the role of foreign intervention (e.g., the European Union's relations with Ukraine) where playing multiple

Policy 35, no. 3 (2014): 400-420, https://www.tandfonline.com/doi/abs/10.1080/13523260.2014.963965; Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare" (Washington: Institute for the Study of War, 2015), http://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

[4] Dinos Kerigan-Kyrou, "Critical Energy Infrastructure: Operators, NATO, and Facing Future Challenges," *Connections: The Quarterly Jpurnal* 12, no. 3 (Summer 2013): 109–17, http://dx.doi.org/10.11610/Connections.12.3.06.

[5] Max Boot, *The Road Not Taken: Edward Lansdale and the American Tragedy in Vietnam* (New York: Liveright Publishing, 2018).

roles becomes more important, and where cyber techniques make these efforts ever more difficult to track. Energy infrastructure and cyberattacks are a useful place to start because of the existing history of attacks, and the similarities shared between states in their need to protect energy supplies and their vulnerabilities to cyber tools.

These are not capabilities limited to Russia. The Stuxnet worm (possibly attributed to Israel and the US) was effective in 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. 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.[6] Likewise, China and even smaller powers such as North Korea possess anti-energy cyber capabilities, and non-state actors such as Al Qaeda and ISIS have also exhibited notable cyberattack capabilities against energy.[7]

The Concept of Resilience

As Conklin and Kohnke wrote, much of cybersecurity 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 rather than on individual attacks, a focus that already exists in the energy sector but indicates a mismatch between energy security and the vulnerabilities present in infrastructure from cyber-related systems.[8] Energy security from cyberattacks, therefore, relies on a broader concept of resilience, one tied not only to actual production and transmission of energy but to those systems that energy supports and legitimates. If energy is removed from a society, particularly a highly industrialized and technology-dependent one, then the proverbial rug is being pulled out from under all support systems.

Resilience networks can be modeled according to the type and pattern of

[6] Ralph Langner, “Stuxnet: Dissecting a Cyberwarfare Weapon,” *IEEE Security & Privacy* 9, no. 3 (May-June 2011): 49-51.

[7] Lukáš Tichý and Jan Eichler, “Terrorist Attacks on the Energy Sector: The Case of Al Qaeda and the Islamic State,” *Studies in Conflict & Terrorism*, 41:6 (2018): 450-473, https://doi.org/10.1080/1057610X.2017.1323469.

[8] William Arthur Conklin and Anne Kohnke, “Cyber Resilience: An Essential New Paradigm for Ensuring National Survival,” in *Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018*, National Defence University, Washington D.C., USA, 8-9 March 2018, ed. Dr. John S. Hurley and Dr. Jim Q. Chen (Reading, UK: Academic Conferences and Publishing International Limited, 2018), p. 126.

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 that 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.[9]

Energy networks are often configured differently, as, instead of being resilient and allowing for re-routing 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.[10] Much of the work on increasing the resilience of energy systems has focused on preventing cascading failures in electrical networks, where the 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.[11] Civilian resilience for the energy sector focuses 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.[12]

[9] Sarah Dunn and Sean Wilkinson, "Hazard Tolerance of Spatially Distributed Complex Networks," *Reliability Engineering & System Safety* 157 (2017): 1-12.

[10] Dong Hwan Kim, Daniel A. Eisenberg, Yeong Han Chun, and Jeryang Park, "Network Topology and Resilience Analysis of South Korean Power Grid," *Physica A: Statistical Mechanics and Its Applications* 465 (January 2017): 13-24, https://doi.org/10.1016/j.physa.2016.08.002.

[11] Maria Gallucci, "Rebuilding Puerto Rico's Grid," *IEEE Spectrum* 55, no. 5 (May 2018): 30-38, https://doi.org/10.1109/MSPEC.2018.8352572.

[12] Cleo Varianou Mikellidou, Louisa Marie Shakou, Georgios Boustras, and Christos Dimopoulos, "Energy Critical Infrastructures at Risk from Climate Change: A State of the Art Review," *Safety Science* 110, Part C (December 2018): 110-120, https://doi.org/10.1016/j.ssci.2017.12.022.

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 the security provided by NATO/KFOR in the country, the electrical utilities KEK and KEDS were publicly maligned and distrusted, and although privatized, still negatively and severely affected public perceptions of government legitimacy and trust in security.[13] In Iraq, US armed forces carried out research that indicated a high correlation with support for the insurgency in those areas of Baghdad (particularly Sadr City) where insurgents had cut access to water, electricity, and sewage.[14] Sparking instability with basic services can be an effective and deniable way to undermine society and leave 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 maybe even more fragile.

Attacks and Vulnerabilities in Ukraine

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 both information and cyber technologies and information and communication networks to achieve their goals. Motivated by this, the provision of the cyber and information security of the critical infrastructures of the state became a crucial condition for ensuring the state’s defense capability and its economic and social development. In January 2018, the US Senate issued a report[15] in which it was noted that, since 2014, Russia has been relentless and diverse in its use of the cyberspace of Ukraine as a cyber art theater and a cyber weapons’ testing ground. In many cases, cyberattacks were aimed at the Ukrain-

[13] Mentor Vrajolli, *Kosovo Security Barometer,* Seventh Edition (Pristina: Kosovar Centre for Security Studies, 1 February 2018), http://www.qkss.org/en/Reports/Kosovo-Security-Barometer-Seventh-Edition-1050.

[14] David E. Mosher, Beth E. Lachman, Michael D. Greenberg, Tiffany Nichols, Brian Rosen, and Henry H. Willis, *Green Warriors: Army Environmental Considerations for Contingency Operations from Planning Through Post-Conflict* (Santa Monica, CA: Rand Corporation, 2008), 90-91.

[15] “Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security,” A Minority Staff Report Prepared for the Use of the Committee on Foreign Relations United States Senate, One Hundred Fifteenth Congress, Second Session (U.S. Government Publishing Office, January 10, 2018), https://www.hsdl.org/?view&did=806949.

ian electricity distribution system, disabling for a long time the areas of the economy, infrastructure, and housing. After the Russian attack on the Ukrainian power grid, US officials from the Department of Energy, the Department of Homeland Security, the FBI, and the North American Electric Reliability Corporation increased their involvement. Recognizing the need to study these cyber-impacts, they worked together to understand the tactics and practices of the Russian government, forecast the types of future cyberattacks, and develop effective protection measures against them. Collaboration with Ukraine on countering these threats is also considered a critical element of the United States cyber defense.

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 societal development. Energy security characterizes the degree of energy (power) complex performance of its functions in society and the state in ordinary, critical, and extraordinary circumstances.[16] Enterprises and institutions of the energy sector play a leading role in the development of the state.[17] 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 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.[18] The objects of the energy sector are strategically important objects and must function continuously and provide for the delivery of quality services.[19]

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

Schematically, this complex is represented in Table 1.

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 eight 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

[16] Concept of the Development of the Security and Defense Sector of Ukraine, Introduced by the Decree of the President of Ukraine dated March 14, 2016, No. 92/2016.

[17] Cybersecurity Strategy of Ukraine, approved by Decree of the President of Ukraine dated March 15, 2016, No. 96 (Officer Vision of Ukraine, 2016), # 23.

[18] The Law of Ukraine "Basic Principles for the Cybersecurity of Ukraine," No. 2163-VIII of October 5, 2017, http://zakon.rada.gov.ua/laws/show/2163-19.

[19] The National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine, May 26, 2015, № 287/2015, http://zakon.rada.gov.ua/287/2015.

Table 1. Power Complex of Ukraine.

Fuel Industry		***Electrical Energy Industry***				***Generation Infrastructure***
1. Coal Mining Industry		**1.Thermal Power Stations**				**1. Transport**
2. Gas Industry		State Regional Power Station		Combined Heat and Power Plant		a) Pipeline
3. Oil Industry		**2. Hydroelectric Power Stations**				b) Railway
a) Oil Mining	b) Oil Refining	Hydroelectric Power Plants		Pumped Storage Power Plant		c) Water
4. Peat Industry		**3. Nuclear Power Plant**				d) Automobile
						e) Air
5. Shale Industry		**4. Alternative Energy Sources**				**2. Power Lines**
6. Chemical Industry		a) Wind Power Stations	b) Solar Power Stations	c) 3D Alternative PPC	d) Biofuel Power Stations	**3. Water Supply** a) Control System; 4**. Staff Support System**
		e) Fuel Power Station		f) Geothermal Station		

share of electricity is produced in thermal power plants (about 50%), at 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 threats (these are 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 the development and functioning of the national economy. In contrast, unusual effects can negatively affect the energy complex as a whole. Among the extraordinary threats, 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)

- Effected on control systems
- Effected 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 power complex 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 in mixed ways on an automated control system, by personnel, on the financial system of energy, on the hardware and software complex. The most vulnerable place in the united power system is the automated control systems.

An Analysis of Cyber Effects on the Objects of Critical Infrastructure of the Energy Sector in 2014-2018

The issue of cybersecurity of a state energy sector is crucial for national security and defense and for economic and social development.

In 2014-2018, well-planned synchronized cyberattacks were conducted on elements of the Ukraine Power Complex. For a period of time, it gave the violators the opportunity to control the complex and, in some cases, even to destroy both the control system and normal functioning of elements of the Power Complexes. The possible goals of these attacks were, perhaps, to check on the reliability of the cybersecurity system of this state-critical infrastructure, the peculiarities of the cybersecurity system functions of power companies, and their reactions to different cyber effects and incidents. It was shown that an overly complex control over information systems could make power complex objects vulnerable to cyberattacks. The most dangerous cyber effects on objects of power complex are those which provoke, or are accompanied by, destructive chain effects directly onto a power object, which is then connected to other objects of infrastructure and spheres of the everyday life of the nation.

One more peculiarity of the cyberattack on objects of the Ukraine Power Complex was the initial dispersion with final direction on defined systematic multispectral results and diverse effects.

During the analysis of the cyberattacks, it was found that the attacks were not solitary, but were conducted synchronously. All of them had a destructive effect on the automated control system of energy objects. The main synchronous destructive cyber effect was focused on the vulnerable elements of automated control systems. Before the main cyberattack, a preliminary cyberattack was conducted on the service and dispatching system with the purpose of denial of service to consumers. The use of several destructive, concentrated cyberattacks 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 cyberattacks, Telebots, BlackEnergy, and Grey Energy, have been closely or more loosely linked to the Russian state by intelligence agencies similar to UK's GCHQ.[20] The lack of any direct attribution, however, does not diminish the strategic use of such tools to destabilize and delegitimate 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 cyberattacks 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 new 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.

One of the important components of the power system in Ukraine is the control system. The control system of the power system plays a leading role in the functioning of the entire energy (power) complex of Ukraine. 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 a corresponding Complex Counteract System against cyberattacks.

In December 2015, the Advanced Persistent Threat (APT) was fixed to an automated control system of the power system. The internal networks of the Ukrainian power company Prykarpattya Oblenergo (PJSC) were attacked.[21] As a result of this cyberattack, a large part of the region and the regional center remained without a power supply for several hours. Thirty substations were shut down. About 230 thousand people were deprived of an energy supply for one to six hours. During the attack, the malicious software BlackEnergy was used.[22] The BlackEnergy group launched an attack on the Ukrainian power grid using the BlackEnergy and KillDisk families. This was the latest known use of BlackEnergy

[20] Jack Stubbs, "Hackers Accused of Ties to Russia Hit Three East European Companies: Cybersecurity Firm," *Reuters*, October 17, 2018, https://uk.reuters.com/article/us-russia-cyber/hackers-accused-of-ties-to-russia-hit-three-east-european-companies-cybersecurity-firm-idUKKCN1MR1BO.

[21] Kim Zetter, "Russia's Hacking Attack on the Ukrainian Power System: How It Was," *Texty.org.ua*, http://texty.org.ua/pg/article/newsmaker/read/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak.

[22] Bruce Middleton, *A History of Cyber Security Attacks: 1980 to Present* (New York: Auerbach Publications, 2017).

malware in the real world. Following the attack, the BlackEnergy group was found to consist of at least two subgroups: TeleBots and GrayEnergy.

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

- a series of attacks in December 2016 using an updated version of the same malicious KillDisk software developed for Windows and Linux operating systems
- a known Petya/NotPetya attack in June 2017 with 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 GreyEnergy group for several years. The GreyEnergy group uses a unique family of malware. The design and architecture of this malicious software are very similar to the already known BlackEnergy family. In addition to the conceptual similarities of the malicious software, links point to the fact that the group behind the malicious software GreyEnergy closely cooperates with the group TeleBots. In particular, the GreyEnergy 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 TeleBots group during an attack in June 2017. It is worth noting that the GreyEnergy group has broader goals than the TeleBots group. GreyEnergy is primarily interested in the industrial networks of various critical infrastructure organizations and, unlike TeleBots, 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 BlackEnergy and TeleBots, the focus of the GreyEnergy group shifted to Ukraine. The attackers first showed interest in the energy sector, and then to transport infrastructure and other important targets. The latest use of malware by GreyEnergy was reported in mid-2018.

The GreyEnergy malware is modular, and unlike Industroyer, ESET specialists have not detected any ICS-driven module, meaning that it is targeted specifically at industrial control systems, yet such a 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 a company and hide the traces.[23] 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.

[23] "GreyEnergy: A Successor to BlackEnergy," White Paper (GreyEnergy, October 2018), www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf.

Moreover, synchronous attacks were carried out on power companies "Chernivtsioblenergo" and "Kyivoblenergo," but with lesser consequences. On December 23, 2015, an unauthorized group of people interfered with the information technology system of remote access to telecontrol over the equipment of 35-110 kV substations of PJSC "Kyivoblenergo." From 15:31 to 16:30 local time, fifteen cities, towns, and villages were completely or partially blacked out in Myronivsky, Makariv, BilaTserkva, 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 stations, which supply several strategic objects of the region: enterprises, institutions, organizations, and the population, were disconnected. Electricity was restored at 18:56 on December 23, 2015.[24]

The control system was vulnerable to cyberattacks of this kind. The response to such a cyberattack was not timely, and the security system failed to fulfill its functions. With malicious software, a cyberattacker can control and, in certain applications, manage a part of or a 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 cyberattack was comprehensive and, to a certain extent, systemically organized, by:

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

During the period from January 19-20, 2016, a cyberattack was conducted with the help of the cyber tool Joint Conflict and Tactical Simulation Enhancements, which was also aimed at disrupting the control system by installing malicious software that was sent by e-mail.[25] Another cyberattack, which was carried out during the night from December 17 to December 18, 2016, was less scale-for-effect. The substation "Severnaya" of the power company "Ukrenergo" was disrupted. Consumers in the northern part of the city of Kyiv and the surrounding

[24] "The Largest Cyber Attacks against Ukraine since 2014," *Novoe Vremya*, no. 24, July 7, 2017, https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html.

[25] "Zillya! Antivirus Has Analyzed the Cyber Attacks on Infrastructure Objects in Ukraine," February 17, 2016, Antivirus Zillya, Certificated for use by public and state authorities, https://zillya.ua/zillya-antivirus-provela-analiz-kiberatak-na-infrastrukturni-ob-kti-ukra-ni.

areas were left without electricity. The attackers did not cause significant damage; the purpose of the attack was a "demonstration of force." As in previous cases, this attack was part of an operation against the state institutions of Ukraine.[26]

The main features of Advanced Persistent Threats are that, as a rule, they:

- are targeted at elements of critical infrastructure
- are conducted by a group of highly skilled hackers
- are carefully masked using specially designed software tools (e.g., specialized Shell Codes, Root Kitta)
- remain unknown for a long time
- are reinforced by intelligence or destructive actions
- and are elements of intelligence and subversive operations.

The analysis of cyber effects is represented in Table 2.

The main cyberattacks differ in their effects and ways of operating. The attacks that were carried out in 2015 on energy companies were not fully self-organized. In 2016, malware that 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" was capable of physical destruction of power systems. CrashOverride software[27] 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 and control over distribution and power supply networks. Mike Assante, from the American cybersecurity company SANS Institute, has determined that the disconnection of the digital relay can lead to the thermal overload of the power grid. This is a very serious threat to transformers and any equipment that is under voltage. Thus, Crash Override can provide a planned attack on several "critical nodes" of the power complex. Then, there is the 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 cyberattacks. As a result of our analysis of the cyberattacks we can separate out individual categories of possible cyberattacks:

- Target components: electronic computing devices such as Remote Terminals (RTUs) or the Human Machine Interface (HMI)[28] typically have an

[26] Vitaliy Tchervonenko, "Was There an Attack on the Regional Power Company," BBC Ukraine, January 6, 2016, https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc.

[27] Middleton, *A History of Cyber Security Attacks*.

[28] Muhammad Baqer Mollah and Sikder Sunbeam Islam, "Towards IEEE 802.22 Based SCADA System for Future Distributed System," in *Proceedings of 2012 International*

Table 2. Analysis of Cyber Attacks.

Object of effect	Tools used	Way of penetration	Effect	Consequences
2015				
"Prykarpattya Oblenergo"	DoS attack on call centers by the method of “denial of service” to “Oblenergo”[29]	Network Internet	The saturation of the network equipment with a large number of external requests	Consumers could not report about power outage
	Advanced Persistent Threat	SCADA Network, installing malicious software “BlackEnergy”	Interception of the control system in the SCADA network through stolen accounts; sending commands to shut down uninterruptible power systems that have been already reconfigured. After that, shutting down the safety systems leading to interruption of the power supply	About 30 substations were switched off, about 230 thousand people were left without electricity from one to six hours
Chernivtsi Oblenergo	DoS attack on call centers by the method “denial of service” Oblenergo	Network Internet	The saturation of the network equipment with a large number of external requests	Consumers could not report about power outage
	Kill Disk utility	Network Internet	Destroying information on servers and workstations	Failure of IT infrastructure elements
	APT-attack, detection of malicious software “BlackEnergy”	SCADA network	Seizure of control of the Automated Dispatch Systems with the execution	The break in electricity supply was from 1 to 3.5 hours. Total non-delivery of 73

Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, Bangladesh, 18-19 May 2012, https://doi.org/10.1109/ICIEV.2012.6317474.

[29] State Power Company of Ukraine.

			of shutdown operations at the substations	MWh (0.015% of the daily consumption of Ukraine)
"Kiev Oblenergo"	Advanced Persistent Threat	Remote Access System	Unauthorized interference with ACS	Over 80 378 consumers without electricity. The power supply was switched off of 30 node substations, supplying a number of strategic objects, over 80 thousand consumers were without electricity within one to three hours
2016 year				
«KievOblenergo"	Malware Crash Override (the attack was fully automated)	Network Internet	Interception of control of the power system, automated discharging of substations	The substation "Pivnichna" with a power supply for own needs from the substation was completely discharged. Denergized loads of 144.9 MW of PJSC "Kyivenergo" and 58 MW of JSC "Kyivoblenergo". The Kyiv NPP was also discharged with a loss of power for its own needs

interface for remote set up or control. Through remote access, the attacker can intercept the device control and cause malfunctions, e.g., make changes in the data transmitted to the operator, damage the equipment, or produce a complete or partial failure of the device.

- Aim at protocols: 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.[30] Its

[30] Salman Mohagheghi, Mirrasoul Mousavi, J. Stoupis, and Z. Wang, "Modeling Distribution Automation System Components Using IEC 61850," in *Proceedings of the 2009*

> specification is available to anyone at a low price. An attacker can make changes to the information that can lead to significant financial costs due to the 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 the Chernobyl Nuclear Power Station) also came under direct attack. This cyberattack was aimed at violating the work of company websites and 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 circulationm M.E.Doc, through 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 cyberattacks could have been Ukraine.[31] 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 the 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 cyberattacks that have affected the functioning of critical infrastructure objects in the energy sector have been assessed in the preceding sections.

Conclusion

This article has considered ways and directions for the choice and implementation of rational approaches to solving the complex protection from destructive cyber effects on the state power complex. All major cyberattacks carried out at the Ukraine Power Complex between 2014 and 2018, which influenced the functioning of the objects of critical infrastructure in the energy sector, have been analyzed. 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 preliminary one was

IEEE Power & Energy Society General Meeting, Calgary, AB, Canada, July 26-30, 2009, https://doi.org/10.1109/PES.2009.5275841.

[31] "Global Ransomware Attack Causes Turmoil," *BBC News Ukraine*, June 28, 2017, https://www.bbc.com/news/technology-40416611.

conducted on the system of maintenance and dispatching, with the purpose of denial to serve the consumers. The use of several destructive, concentrated cyberattacks 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 has been established that the system of production and supply of electricity depends on the level of cyber resistance of power objects. An analysis of cyberattacks 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 have been 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 control of objects of the energy infrastructure as a whole, and then to change the parameters of their functioning.

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

Disclaimer

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 18, 2019 is supported by the United States government.

About the Authors

Tamara Maliarchuk, PhD, worked for LLC UkrEnergy from 2016–2018. Dr. Maliarchuk was a member of the NATO working group on DEEP program implementation in the Armed Forces of Ukraine. She was an analyst with the S.Korolov Zhytomyr Military Institute in Ukraine and has worked with US forces on language and cyber defense. She conducts research in e-learning, innovative technologies in PTSD detection and therapy, manipulative technologies in web-environment. *E-mail*: maliarchuktamara@gmail.com

Major General **Yuriy Danyk**, Professor, Doctor of Science of Engineering, Chief of Institute of Information Technologies, Ivan Chernyakhovsky National Defense University of Ukraine. He is an expert in the art of war, national defense and security, information and cybersecurity, electronic and IT technologies, robotic complexes design and application, Special forces development. He has combat experience in the application of advanced defense technologies in the conditions of modern war. *E-mail*: zhvinau@ukr.net

Dr. **Chad Briggs** is an Associate Professor and Director of Public Policy and Administration at the University of Alaska Anchorage. Dr. Briggs has field experience in information and hybrid warfare and in developing defensive strategies to protect critical systems in Eastern Europe and the Balkans. He has a PhD in political science from Carleton University in Canada, and has been previously a senior advisor for the US Department of Energy and the Minerva Chair and Professor of Energy and Environmental Security for the US Air University (USAF). He is the author (with Miriam Matejova) of *Disaster Security: Using Intelligence and Military Planning for Energy and Environmental Risks*.
E-mail: cbriggs9@jhu.edu