MANDALA:
Jurnal Ilmu Hubungan Internasional

Vol. 5 No.2
Juli-Desember
2022

Received:11-10-2022
Accepted: 18-10-2022
Published: 31-12-2022

Securitisation of Ukrainian Critical Infrastructures: The Case of the Failure of SCADA System in Protecting the Power Grids

Dini Putri Saraswati
Lecturer of International Relations, Universitas Pembangunan Nasional 'Veteran' Jakarta
E-mail: diniputrisaraswati@upnvj.ac.id
Nurfarah Nidatya
Lecturer of International Relations, Universitas Pembangunan Nasional 'Veteran' Jakarta
Email: nurfarahnidatya@upnvj.ac.id
Muhammad Kamil Ghiffary Abdurrahman
Lecturer of International Relations, Universitas Pembangunan Nasional 'Veteran' Jakarta
Email: ghiffaryabdurrahman@upnvj.ac.id

Abstract

Critical infrastructures are an important element to support social cohesion in a certain area. Therefore, it is necessary to protect critical infrastructures in order to maintain the sustainability of the assets. There are many attempts by states to control the security of their critical infrastructures, one of them is using the Supervisory Control and Data Acquisition (SCADA) system, a control system in which to monitor and retrieve data under the supervision of an operator. However, although countries are aware of the preventive action over their critical infrastructures, it is still possible to fail. In this case, Ukraine which has a relatively secure control system failed in protecting its power grids from multiple hacker attacks which contributed to blackouts in December 2015. The devastating failure of Ukraine's security system has led public opinion to point a finger at Russia since the relationship between both countries is at stake. In this sense, Ukraine issued a speech act to securitise its critical infrastructures. By exercising securitisation theory, this article would discuss further the fruitfulness of the speech act after the failure of the security system in protecting Ukraine's power grids.

Keywords: *SCADA, Ukraine, Russia, power grid, and securitisation*

Abstrak

Infrastruktur kritis merupakan elemen penting dalam mendukung kohesi sosial di suatu wilayah. Oleh karena itu, perlu dilakukan perlindungan terhadap infrastruktur kritis guna menjaga keberlangsungan aset tersebut. Terdapat banyak upaya negara untuk mengontrol keamanan infrastruktur kritis mereka, salah satunya adalah menggunakan sistem yang bernama Supervisory Control and Data Acquisition (SCADA), sebuah sistem kontrol untuk memantau dan mengambil data di bawah pengawasan operator. Namun, meskipun negara-negara menyadari tindakan pencegahan atas infrastruktur kritis mereka masih mungkin untuk gagal. Misalnya saja seperti yang terjadi di Ukraina, di mana Ukraina mengalami kegagalan dalam sistem kontrolnya dalam melindungi jaringan listriknya dari berbagai serangan peretas yang berkontribusi pada pemadaman listrik pada Desember 2015. Kegagalan sistem keamanan Ukraina ini menyebabkan

munculnya opini publik yang menuding Rusia sebagai salah satu aktor yang berperan dalam kegagalan dalam sistem control Ukraina. Hal ini membuat hubungan kedua negara dipertaruhkan. Menanggapi hal ini, Ukraina mengeluarkan pidato untuk mengamankan infrastruktur kritisnya. Dengan menggunakan teori sekuritisasi, artikel ini akan membahas lebih lanjut tentang upaya yang dilakukan Ukraina pasca kegagalan sistem keamanannya dalam melindungi jaringan listrik Ukraina.

Kata Kunci: SCADA, Ukraina, Rusia, jaringan listrik, dan sekuritisasi

Introduction

Critical infrastructures are the critical elements that keep a nation's longevity sustainable. Infrastructures can act as the conduit for communication across physical distances, bringing people from different places and establishing the foundation for modern economic and social systems (Larkin, 2013). In other words, critical infrastructures are made up of resources and systems, whether virtual or physical, that are so crucial to the country's economic health, national security, public health, and safety, or any combination of these, that any interruption of the services could have a catastrophic effect (Alcaraz & Zeadally, 2015). Thus, the development of infrastructures results in the creation of infrastructural systems that aid the organization of people's daily lives (Hughes, 1987, 1993 in Larkin, 2013). Since infrastructures are crucial for both economic and social elements, if critical infrastructures are weak, economic and social progress will be difficult (Yusta et al., 2011).

Critical infrastructures are vulnerable to threats and, thus, should be protected to reduce potential risks and vulnerabilities. According to Yusta et al. (2011), Bill Clinton's establishment of the Commission on Critical Infrastructure Protection in 1996 marked the beginning of the discussion on infrastructure protection. The United States (US) also notes that its critical infrastructures are essential for its economic prosperity, military capacity, and political vitality (Collier & Lakoff, 2008).

The newly established emerging threats have contrasting distinctions with the framework of the Cold War, namely technological accidents, energy crisis, and terrorism, resulting its difficulties in predicting and calculating its real impact (Collier & Lakoff, 2008). Hence, the early question from the public regarding the US national security challenges in the early 1980s. Additionally, the European Union (EU) emphasizes the significance of critical infrastructure protection (CIP) to all its member states through the European Programme for Critical Infrastructure Protection (EPCIP). The European Commission published a message to address CIP to create a legal framework for transparency on CIP and promote cross-border cooperation (Alcaraz & Zeadally, 2015).

Energy, information and communication technology, water, food and agriculture, healthcare and public

health, financial systems, transportation systems, chemical industry, space, research facilities, civil administration, public, legal order, and safety are all considered critical infrastructures according to EPCIP. Accordingly, states must maintain their security based on this understanding by constructing security systems for their critical infrastructures as a preventive measure to lessen the impact of the risk. It is essential to remember that the term 'risk' in this context refers to a collection of combinations of what might occur, the likelihood of things to happen, and the consequences. Whereas the term 'threat' is associated with destructive acts on critical infrastructures, and the term 'vulnerable' indicates the weakness level of a system to disasters, attacks, or failures (Yusta et al., 2011).

Every country's economy relies on its critical infrastructures, particularly its power grid control system. Power grid control systems are the subject of inexpensive cyber-attacks that have the potential to affect entire nations or even continents. This is why cyber security safeguards for the power grid control system are crucial (Jarmakiewicz et al., 2017). In this instance, Ukraine has installed Supervisory Control and Data Acquisition (SCADA) systems to safeguard its power grid since it is aware of potential attacks that could harm its critical infrastructures. The control systems in Ukraine were also surprisingly more secure than some in the USA, according to experts, because they were well-separated from the control center business networks and had robust firewalls (Zetter, 2017).

The term 'SCADA system' was coined in the 1960s by the Bonville Power Administration and was first published at a Power Industry Computer Application (PICA) Conference. A SCADA system is a type of industrial control system (ICS). It is a standard automation system that collects data from remote sensors and instruments and transmits it to a central site for controlling or monitoring purposes (Karacor & Ozdemir, 2004). SCADA systems monitor and control infrastructure, industrial, and facility-based processes, such as oil and gas refining, telecommunications, transportation, and water control (Kim, 2012). As a result, many businesses are considering SCADA systems to provide access to real-time data display, alarming, trending, and reporting from remote equipment via various communication media, such as dial-up connection, private lease line (PLL), internet, radio modem, and satellite.

Recent technological advancements have made location transparency possible through the internet at a relatively low cost and with an acceptable level of security (Karacor & Ozdemir, 2004). SCADA systems can be relatively simple, such as those used to monitor the environmental conditions of a small office building, or highly complex, such as a monitoring system that observes all of the activity in a nuclear power plant (Kim, 2012).

States are working to improve their defenses to safeguard their critical infrastructures, but mistakes could still happen. As an illustration, consider what transpired in Ukraine on December 23, 2015, when Ukrainian Kyivoblenergo, a local energy distribution business, reported that many hacking attacks resulted in blackouts in three Ukrainian regions, notably Kyiv, Prykarpattia, and Chernivtsi. Up to 225,000 people were impacted by the power disruptions in the areas for roughly six hours (Whitehead et al., 2016). In addition, the crisis placed harm and economic losses on the nation and plunged Ukraine's land into hybrid warfare and civil unrest (Park et al., 2017). They disclosed that a third party had illegally accessed the company's computer and SCADA system (Lee et al., 2016). More than fifty affected substations had remote controls to which the operators could not regain access. The attackers also launched a telephone denial-of-service attack targeting customer call centers to stop the operators from communicating. After six hours of manual power system control attempts to resolve the issue, it eventually resumed functioning regularly (Whitehead et al., 2016).

The failure of the SCADA system is not surprising because it is now more vulnerable than it was in the past. When the network protocol was proprietary, and the SCADA system was an isolated, vendor-controlled system without connections to other systems, only a select few individuals, such as developers and hackers, knew that SCADA installations existed. The current SCADA system is networked and extensively diffused, nevertheless. The system is susceptible to external cyber assaults because it depends on open internet protocol standards (Kim, 2012).

In addition, specific risks can affect modern SCADA systems in two ways. The first is the risk of unauthorized access to the control software, including changes made by humans, viruses, and other threats present on the control host machine. In contrast, the second is the risk of packet

access to the network segments hosting SCADA devices (Kim, 2012).

According to Ehud Shamir, Chief Information Security Officer (CISO) at American security firm SentinelOne, the SCADA systems and ICS are typically run on standard Windows personal computers (PCs), making them prone to mainstream malware like Black Energy. He continued that the power grid operator needed to be more knowledgeable and connect some industrial control system interfaces to the Local Area Network (LAN). A modular Black Energy malware component acts as a network sniffer, discovering data, such as user credentials, that allows the attacker to access the ICS and undermine it (McLellan, 2016).

Following the attacks, Sluzhba Bezpeky Ukrayiny (SBU), or Ukraine Security Service, claimed that Russia was responsible for all of the clutter based on the data at hand, including that acquired in conjunction with antivirus companies that hacked Ukraine's financial system, transportation network, and energy facilities using TeleBots and Black Energy (da Silva, 2017). Since Russia annexed Crimea, Ukraine, in 2014, the two nations' tense ties have also led to charges against Russia (Zetter, 2016). There was, however, little concrete evidence that Russia was the actor behind the power outages.

On February 15, 2016, Ukraine established its National Cyber Security Strategy by Presidential Decree in response to these challenges. The strategy's primary goal is to create the conditions that ensure secure cyberspace and its usage in the interests of the government, society, and individuals, along with an annual Action Plan for its implementation. According to the Global Forum (n.d.), there are three main strategic objectives: 1) Developing the national cyber security system; 2) Increasing capabilities throughout the security and defense sector; and 3) ensuring the cyber security of critical information infrastructure and government information resources.

The national cyber security system put in place by the strategy ensures collaboration between all government agencies, local authorities, military units, law enforcement agencies, research and educational institutions, civic groups, businesses, and organizations, irrespective of their form of ownership, that deal with electronic communications and information security or are owners of critical information infrastructure (Global Forum on Cyber Expertise, n.d.).

The study examines the effectiveness of Ukraine's implementation of critical infrastructure securitization following the failure of the SCADA system to safeguard the nation's power grids adequately. It does this by drawing on the background mentioned above case. We would include a crucial sub-question about the strategies formulated and implemented by the Ukrainian government to defend against the cyberattack to help direct the analysis. We will divide this paper into five parts. Firstly, we will explain the theoretical framework used in this paper. We would employ two theories, namely the CIP theory by Claudia Aradau and the securitization theory by Barry Buzan et al. Second, we would talk about how Ukraine views the threat – in this case, Russia – as a threat. The reasons why Ukraine views Russia as a threat will be further elaborated. Thirdly, we would analyze the Decree of the President of Ukraine No. 32/2017, which we consider to be a securitizing action after the Ukrainian crisis. And then, we would talk about the National Cyber Security Strategy as the breaking free of the rules of Ukraine. Lastly, we would conclude by addressing the research issue and supporting the theories above-mentioned.

Theoretical Framework

The European Commission Migration and Home Affairs define critical infrastructure as an asset or system necessary to keep vital societal activities. Critical infrastructure damage, destruction, or interruption by terrorism, crime, or malevolent behavior may significantly affect a country's security and residents' well-being (European Commission Migration and Home Affairs, n.d.). Critical infrastructure protection (CIP) is required for the nation because critical infrastructures appear to promote societal cohesiveness, the replication of national security, and service provision. Critical infrastructures play a significant role in society (Aradau, 2010). Furthermore, CIP is to safeguard pre-existing things. Their functionalities as the primary purpose of CIP is to ensure that critical operations can continue without 'undue interruptions and that crucial, sensitive data are protected' (Dacey, 2002 in Aradau, 2010); security professionals have concentrated on the technologies and policies implemented to guarantee the reliability and robustness of critical infrastructures. These efforts to safeguard infrastructures from catastrophic failures eliminate several other activities and their significance for the operation or interruption of critical infrastructures

(Aradau, 2010). Based on the definition of critical infrastructure above, power grids are categorized as critical infrastructure. Moreover, by using the theory of CIP, we would examine the SCADA systems as a CIP for protecting Ukraine's power grids from potential threats.

We would also include the securitization theory to back up the CIP theory. However, we must first understand what security is in order to discuss securitization properly. According to Buzan et al. (1998), security is the maneuver that puts politics beyond the established rules of the game and frames the issue as a particular sort of politics or as above politics. Security is a self-referential discipline, meaning that only inside this practice does a problem become a security problem. It is more likely because the problem is presented as such a concern than because a genuine existential threat is discovered. Although politicization can be assumed to be a more violent form of securitization, theoretically, Buzan et al. (1998) added that any public issue can be classified along a spectrum from non-politicized, where the state does not deal with it. It is not necessarily a matter of public debate and decision through politicized, where the issue is part of public policy. It requires res government decision to securitize, where the issue is presented as an existential threat, and it is, therefore, subject to (Buzan et al., 1998).

As a result, Buzan et al. (1998) concluded that the true definition and criteria of securitization are constituted by the intersubjective production of a salient enough existential danger to have a significant political impact. Furthermore, according to Buzan et al. (1998), a case of securitization is performed if, in terms of the priority and urgency of an existential threat, the securitizing actor has managed to break free from either procedures or rules that they would be bound by.

In theory, the securitization process is referred to as a speech act, which, unlike a sign referring to something more tangible, is more akin to the utterance itself. As Austin (1975 in Buzan et al., 1998) argued, saying the words do something, such as betting, making a promise, or naming a ship. Furthermore, objects generally regarded as dangerous, such as polluted waters or tanks, aid in securitization (Buzan et al., 1998). Energy outages and transportation breakdownsforth could all be interpreted as facilitating conditions for the speech act. Furthermore, a securitizing actor must

authorize the securitization (Buzan et al., 1998).

A speech act is successful when both the intrinsic features of speech and the group authorize and recognize the speech. In Ukraine, an energy blackout caused by a cyberattack on power grids prompted the government to form a speech act by issuing a Decree of the President of Ukraine No. 32/2017. Ukraine attempted to secure its critical infrastructures, in this case, power grids, by forming a set of speech acts.

A successful securitization has three components: 1) an existing threat, 2) emergency action, and 3) the effects on interunit relations by breaking free of rules. In theory, however, presenting something as an existential threat to a referent object does not create an instant securitization. Securitization only happens if and when the public can accept it as such (Buzan et al., 1998).

Securitization is achieved not only through rule-breaking (which can take many forms), nor through existential threats (which can lead to nothing), but through cases of existential threats that legitimize rule-breaking. On a small scale, many actions can take this form, such as a family securitizing its lifestyle as dependent on keeping a specific job (and thus using dirty tricks in competition at the firm) or the Pentagon designating hackers as a 'catastrophic threat' and a 'serious threat to national security' (San Francisco Chronicle, 1996 in Buzan, et al., 1998), which could potentially lead to actions within the computer field but with no cascading effects on other (Buzan, et. al., 1998).

Research method

This research employs a qualitative approach with explanatory writing techniques to explain the phenomenon using two variables. According to Sugiyono (2017), explanatory research is a method used to explain the variables studied to test a hypothesis. In this study, the author collects data from secondary sources using a library research method.

We employ qualitative data analysis techniques to analyze the research data. This analysis is used to describe various analytical practices using existing data from other researchers and an institution in the form of new research and to re-examine the principal research statement for evidentiary purposes.

Discussion

Ukraine Is Pointing a Finger at Russia: Russia as a Threat?

Shortly after the attack, Ukrainian government officials claimed that a cyber attack caused the blackout and that Russian security services were to blame. Following this claim, Ukrainian investigators, private companies, and the US government conducted an analysis and offered assistance in determining the root cause of the outage (Lee et al., 2016). At a press conference, Ukraine's Security Service Chief of Staff Oleksandr Tkachuk stated that the attacks were orchestrated by the Russian Security Service with the assistance of criminal hackers and private software firms and appeared to be created by the same people who designed the malware known as Black Energy (Zinets, 2017).

However, there was no concrete evidence that Moscow was to blame for the outage. iSight Partners, an American information technology and services firm, examined some of the code found on infected computer systems in Ukraine and concluded that the attack was almost certainly carried out by a hacking group called Sandworm, which is thought to have ties to Russia. Sandworm used a standard hacking tool known as Black Energy, and the presence of that program on one of the affected Ukrainian computer systems is critical evidence that has led iSight to blame the group (Groll, 2016).

In 2014, US authorities warned industrial control system operators that Black Energy could be used to infect their systems. Furthermore, iSight Partners discovered that the infected Ukrainian systems contain the KillDisk wiping tool – a program that deletes computer data and can be used to cover up the evidence of a cyberattack – which was also found in cyberattacks in Ukraine around the time of last year's elections. However, the cyber security community is deeply divided about what the presence of Black Energy and KillDisk means. KillDisk is merely a wiping program, and industrial security experts claim that deleting data is insufficient to cause a power outage. Black Energy can grant hackers remote access to a system, but it cannot be used to bring an electricity grid down on its own (Groll, 2016). As a result, based on such analysis guided by iSight Partners, it is still unclear whether Sandworm is affiliated with the Russian government or is simply another hacking group aiming to exacerbate the political situation between the two countries by conducting a cyber attack through Ukraine’s SCADA system to paralyze its power grids.

On the other hand, tensions between Ukraine and Russia are high because both countries have a long history. At least eight problems exist in Ukraine-Russia relations, including the issue of Crimea, the Russian black sea fleet, the approximately 8 million ethnic Russians living in Ukraine, and approximately 50% of Ukrainian citizens who speak Russian as their first language, the question of regional diversity of Ukraine, the issue of energy supplies, the question of Ukraine's position between the EU and the North Atlantic Treaty Organization (NATO) on the one hand and Russia and its political and economic allies on the other, apparent asymmetry in relations between the two countries and peoples, made more complicated by the fact that many Ukrainian citizens share these views, at least in part (Kappeler, 2014). Moreover, a survey conducted by Simmons et al. (2015) shows that 39% of the NATO public also blames Russia for the Ukraine crisis.

The political situation in both countries, mainly since Russia annexed Crimea, has created a perception of a threat from Ukraine to Russia. "President Petro Poroshenko signed a decree that enacted the decision of Ukraine's National Security and Defence Council from September 2, 2015 'On the new edition of Ukraine's Military Doctrine'", according to Ukraine's President's website. Furthermore, the source stated that Russian military action, which includes the short-term control of Crimea and aggression in some of the Donetsk and Lugansk areas, is the current military danger to Ukraine (Anon, 2015).

While discussing Russia's aggressive military action in Crimea, Poroshenko stated in his speech at the 72nd Session of the United Nations General Assembly (UNGA) in New York, USA, "Russia is not a contributor to international security, but its biggest threat" (Poroshenko, 2017). Furthermore, he stated on the sidelines of the World Economic Forum (WEF) in Davos, Switzerland, that joint global efforts were required to halt Russian aggression, both military and cyber, saying, "There is a global cyber war of Russia against (the) entire world, there is much evidence. This is a global threat, and the entire world must work together to combat it" (Adler & Rao, n.d.).

From Ukraine's President's statements and actions toward Russia, as well as Ukrainian perceptions of Russia, Russia is a real threat to Ukraine. According to the securitization theory,

presenting something as a threat to a referent object does not result in securitization, but is a securitizing move (Buzan et al., 1998). However, the audience must acknowledge that a specific object is portrayed as a threat. Cheskin (2017) asserted that the Ukrainian citizenry is more likely to support an orientation toward the EU and away from Russia due to the Ukraine-Russia crisis. As a result, from this vantage point, Ukraine is making a securitizing move by portraying Russia as a threat, and the audiences, in this case, the people, have accepted Russia's threat perception as a result of the ongoing conflict between the two countries.

Decree of the President of Ukraine No. 32/2017 as a Ukraine's Speech Act

In response to the cyber attack, Poroshenko issued Decree of the President of Ukraine No. 32/2017 on 13 February 2017, approving the National Security Defence Council (NSDC) decision made on 29 December 2016 on securing Ukraine against evolving cyber threats (Martinenko, 2017). The NSDC decision outlines actions to increase overall cyber security to effectively tackle and combat cyber crimes and threats such as propaganda, espionage, and cyberattacks.

The leading cyber security measures envisaged by the NSDC Decision, as cited from Ukaz Prezydenta Ukrayiny (2017), include the following:

1. Advising the President of Ukraine to choose the General State Customer of the National Programme of Informatisation while taking into account current threats to the cyber security of the state
2. The Cabinet of Ministers shall propose draft laws to parliament to implement the Convention on Cyber Crime, introducing, among others:
   A. The capacity of the law-enforcement bodies to impose mandatory orders on the owners of electronic data (e.g., telecom operators and providers) for the immediate recording and storage of electronic data required to investigate crimes for a period of ninety days to three years
   B. The duty of telecom operators and providers to provide all data necessary to identify service providers and data routes to law enforcement bodies upon their request

C. The possibility of blocking informational resources (e.g., websites) by court decision
D. A legal framework that effectively allows the use of electronic evidence in criminal court proceedings

3. The National Bank of Ukraine shall develop a legal framework allowing it to restrict payment systems held by entities of the state-aggressor (e.g., Russian Federation) on the territory of Ukraine

The Decree of President No. 32/2017 issued by Poroshenko is known as the securitization procedure or a speech act. Ukraine was forced to take emergency action in the form of a speech act by issuing a Decree of the President of Ukraine No. 32/2017 due to an energy blackout brought on by a cyberattack on the power grids. By forming the Decree of the President, the Ukrainian government, through the President of Ukraine as a securitizing actor, attempted to securitize its critical infrastructures. According to the Decree of the President, the cabinets and the people will obey the order that the President sets. In other words, the audiences accept the speech act.

National Cyber Security Strategy: Ukraine's Breaking Free of Rules?

On February 15, 2016, shortly after the Presidential Decree of Ukraine No. 32/2017 had been issued, Ukraine formulated a National Cybersecurity Strategy. This strategy is linked to an annual Action Plan for its implementation, with the overarching goal of creating a safe cyberspace and the conditions that ensure its use for the benefit of individuals, society, and government (Koval, n.d.). The strategy focuses on three axes: developing a national cybersecurity system, strengthening capabilities across the security and defense sectors, and ensuring the cyber security of critical information infrastructure and national intelligence resources. The main threats to Ukrainian cybersecurity fall into four categories: military-style cyber threats, espionage, cyber terrorism, and cybercrime (Global Forum on Cyber Expertise, n.d.).

There also are guiding standards withinside the method, particularly appreciating human and civil rights and freedom; cooperation with the non-public sector, civil society, and global community; medium risk-primarily based cyber safety measures; precedence given to preventative measures; inevitable punishment for cyber crimes; precedence

recognition at the improvement of home medical and technical commercial ability; and making sure democratic civil manipulate withinside the vicinity of cyber safety.

The country-wide cyber safety gadgets installed location with the aid of using the method gives collaboration among all authorities agencies, nearby authorities, navy units, regulation enforcement agencies, studies and academic institutions, civic groups, businesses, and organisations, regardless of their shape of ownership, that address digital communications and statistics safety or are proprietors of essential statistics infrastructure (Global Forum on Cyber Expertise, n.d.). There are five key regions of making sure cyber safety in Ukraine, consisting of the improvement of safe, sustainable, and dependable cyberspace; cyber safety of the authorities' digital statistics resources; essential infrastructure cyber safety; improvement of cyber safety ability withinside the protection sector; and combating cyber crimes (Global Forum on Cyber Expertise, n.d.).

We will recognize the evaluation of Ukraine's cyber method on essential infrastructure cyber safety because, on this connection, the gadget defines that cyber protection of essential infrastructure ought to consist, amongst others, mainly of enhancing the complicated prison framework of important infrastructure cyber protection, organization, and protection of the country sign up of the digital items of infrastructure, and improvement and implementation of the mechanism for statistics trade among authorities bodies, non-public sector, and residents concerning threats to essential statistics infrastructure (Koval, n.d.). The critical infrastructure cyber safety itself is derived into three key aspects: enhancing legislation, altering the necessities for the cyber safety of essential infrastructure, and expanding public-non-public partnerships to save you from cyber threats (Global Forum on Cyber Expertise, n.d.).

In October 2017, Poroshenko signed into law "About the basic principles of providing cyber security of Ukraine." It is a legislation framework from which numerous other statutory acts will have to be born and subordinate (Holmov, 2017). There are several legal bases for ensuring cyber security in Ukraine, such as the Constitution of Ukraine, the Laws of Ukraine based on national security, the Principles of internal and foreign policy, electronic communications, protection of state information resources and

information, the requirement for protection of which is established by law, the Convention on cybercrime, other international treaties, the consent to be bound by the Verkhovna Rada of Ukraine, Decrees of the President of Ukraine, and Acts of the Cabinet of Ministers of Ukraine (Zakon Ukrayiny, 2017).

However, the legal bases mentioned above are improved. As per reports, the bill summarises several vectors for mitigating cyber threats with a key focus on protecting critical infrastructures (Cisomag, 2017).

To carry out the legislation, the government promotes both public and private interaction in preventing cyber threats to critical infrastructure objects, responding to cyber attacks and cyber incidents, in eliminating their consequences, in particular in times of crisis, emergency, and martial law, and during a particular period (Zakon Ukrayiny, 2017). In addition, the law also mentions that the government will consolidate institutional responsibilities such as the Computer Emergency Response Team of Ukraine (CERT UA), the National Service for Special Communications and Information Protection of Ukraine, and the National Cyber Defense Center. Increase. The National Police, the "authorities" such as the SBU and the Foreign Intelligence Service of Ukraine (FISU), the Ministry of Defense, and the National Bank of Ukraine are all now affiliated with the NSDC (Holmov, 2017).

Ukraine participates in international organizations to protect the nation from cyber threats before an incident occurs. An essential step in implementing this strategy was establishing the National Cyber Security Coordination Center, a working arm of the NSDC. It has a supervisory role, performing tasks related to analyzing the national cybersecurity state and readiness to counter threats and predicting and detecting potential threats. It also organizes and conducts international and cross-departmental cybersecurity training (Global Forum on Cyber Expertise n.d.).

Moreover, Ukraine is working towards fully implementing the convention as a State Party to the Budapest Convention on Cyber Crime. Draft legislation has been set and is currently discoursed in parliament, which involves the establishment of the liability for cyber crimes and defines the critical terminology and update of responsibilities of the Internet Service Providers (ISPs)

according to the convention (Global Forum on Cyber Expertise n.d.).

In recognizing the need for strong international cooperation and capacity building to address cybersecurity needs and threats highlighted in the new strategy, Ukraine has been cooperating with several partners across the cyber domain. In the area of cybercrime, Ukraine has been a partner in the joint European Union and Council of Europe projects 'CyberCrime@EaP II' and 'CyberCrime@EaP III' that have a regional dimension involving all countries of the Eastern Partnership (e.g., Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, and Ukraine). The first project focuses on refining mutual legal assistance for international cooperation on cybercrime and electronic evidence and strengthening the role of 24/7 contact points. And a second project, launched in Kyiv in April 2016, deals with the issue of public-private cooperation. Cooperation with ISPs and the Council of Europe's recommendation that national authorities initiate an organized dialogue with his ISPs to act as a confidence-building exercise to understand and respond to mutual needs. Additionally, our partners in the UK and Estonia have provided Ukrainian law enforcement agencies with the latest hardware and software to perform specialized computer forensics and investigate cybercrime more thoroughly (cyber expertise global forum, n.d.).

Ukraine cooperates with the NATO Cyber Defense Trust Fund in cyber defense to improve the country's technical capabilities to counter cyber threats. As a part of NATO's Comprehensive Assistance Package (CAP) for Ukraine, this support includes establishing incident management centers to monitor cybersecurity events and labs to investigate cybersecurity incidents, as well as training in using this technology and equipment. The SBU has a leading role within the NATO Cyber Defense Trust Fund. At the same time, NATO partners include Romania as a major country, with additional financial and in-kind contributions from Albania, Estonia, Hungary, Italy, Portugal, Turkey, and the United States. Ukraine and its NATO partners conduct cyber defense exercises and training, training all relevant national stakeholders to respond to large-scale cyber attacks on national defence infrastructure (Cyber Specialist Global Knowledge Forum, n.d.). The cybersecurity cooperation between NATO and Ukraine is essential as Russia's cyber

operations in Luhansk and Donetsk regions do not target the Ukrainian government only but also NATO's media outlets through a Distribution Denial-of-Service (DDoS) attack (Kostyuk, 2015).

Ukraine participates in international initiatives in the field of countering cyber threats and contributes to the development of regional initiatives. A Ukrainian initiative has set up a cybersecurity working group within the Organization for Democratic and Economic Development of Georgia, Ukraine, Azerbaijan, and Moldova (GUAM) and prepared a Memorandum of Understanding (MoU) for adoption by their respective governments. At the same time, we have already set up a secure communication system that allows the secure exchange of data online and the conduct of video conferences (Global Forum on Cyber Expertise, n.d.).

Conclusion

This paper discusses the securitization of critical infrastructure in post-crisis Ukraine for SCADA systems. First of all, Ukraine recognizes that the presence of a power grid is essential for maintaining social cohesion. That is why Ukraine protects its power grid with its SCADA system to prevent potential threats. Ukraine has installed its SCADA system to protect its power grid. The primary function of SCADA systems is to monitor and control critical infrastructure by displaying real-time information about the system. The SCADA system used by Ukraine is called CIP and protects critical infrastructure from failures that could disrupt social cohesion in the region.

However, a SCADA system used in Ukraine was hacked and went down, causing a power outage in critical parts of Ukraine for about eight hours. The blackout paralyzed the city's transportation system and industry. There was much speculation that Russia was behind the incident. There was no objective evidence that Russia did this. All they found were traces of a Russian hacking group called Sandworm. This group launched the Black Energy and KillDisk viruses on SCADA systems. However, neither cyber threat was enough to bring down the power grid.

Rising tensions between Russia and Ukraine exacerbated the problem. Ukraine accused Russia of the attack, which Ukraine denied. In his statements at various international conferences, Poroshenko even believes that Russia poses a threat to Ukraine and the world. Ukrainians also have cold feelings towards Russia, which has a long history. Shortly

after the attacks, the NSDC proposed a set of rules to combat cyber threats, which Poroshenko endorsed in Ukraine Presidential Decree No. 32/2017. The Decree of the President of Ukraine No. 32/2017 consists of orders to the Cabinet of Minister Poroshenko to ensure the requirements of cyber defense and ensure the cyber security of critical infrastructure objects. Based on speech acts, the Decree of the President of Ukraine No. 32/2017 designates such securitization processes facilitated by cyber-attacks as speech acts. The Ukrainian government seeks to protect critical infrastructure from any Russian threat by forming a speech act. Moreover, the Ukrainian people also acknowledged the government's speech act because they perceived an existential threat.

After the issuance of the Decree of the President of Ukraine No. 32/2017, the government will draw up a cybersecurity strategy to create conditions for the safe operation of cyberspace and its use for the benefit of individuals, society, and the state. Did. To ensure Ukraine's cybersecurity, the strategy includes five main points: The sustainable use of cyberspace, cyber security on the government's critical infrastructure, safe cyberspace of government electronic devices, development of capacity in the department of nation's defense, and acts against cybercrimes.

Starting with the Ukrainian case, this paper uses a theoretical framework and case studies to answer research questions regarding the success of Ukrainian securitization and Ukrainian strategies for countering cyber threats. Aradau's CIP theory and Buzan's securitization theory analyze a case study of securitization in Ukraine. Aradau explained that CIPs protect existing ones and their functions, and Buzan argued that he has three elements (or steps) to a successful securitization. They are existential threats, contingency measures, and the impact on unit relationships of breaking away from the rules.

It confirms Buzan's theory that the securitization process conducted by Ukraine is successful because three factors are met in the case of Ukraine. First of all, there is the existential threat that Ukraine, and hence Russia, perceives. Claims of aggression against Russia without concrete evidence prove that Ukraine emphasizes Russia as a threat to the state, especially given the long histories of the two countries. We consider this act of speech to be an order of the President of Ukraine as an emergency measure, as it was issued shortly after the attack and contains

measures to protect Ukraine from cyber threats. Finally, as the Ukrainian government has reduced regulations related to cybersecurity, especially critical infrastructure, after an attack, the National Cybersecurity Strategy will influence relations between entities by moving away from the rules. In addition, Ukraine joined relevant agencies and cooperated with other countries to address cyber threats.

References

Alcaraz, C. & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, 53 – 66.

Aradau, C. (2010). Security that matters: Critical infrastructures and objects of protection. *Security Dialogue*, 41(5), 491 – 514.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cheskin, A. (2017). Russian soft power in Ukraine: A structural perspective. *Communist and Post-Communist Studies*, 50(4), 277 – 287.

Collier, S. J. & Lakoff, A. (2008). The vulnerability of vital systems: How "Critical Infrastructure" became a security problem. In M. D. Cavelty & K. S. Kristensen (Eds.), *The politics of securing homeland: Critical infrastructure, risk, and securitisation* (pp. 1 – 33). Routledge.

European Commission Migration and Home Affairs. (n.d.). *Critical infrastructures*. https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en.

Global Forum on Cyber Expertise. (2017). *Cybersecurity in Ukraine: National strategy and international cooperation*. https://www.thegfce.com/news/news/2017/05/31/cybersecurity-in-ukraine.

Jarmakiewicz, J., Parobczak, K., & Maślanka, K. (2017). Cybersecurity protection for power grid control infrastructures. *International Journal of Critical Infrastructure Protection*, 18, 20 – 33.

Karacor, M. & Ozdemir, E. (2004). Mobile phone-based SCADA automation. *Measurement and Control*, 37(9), 268 – 272.

Kappeler, A. (2014). Ukraine and Russia: Legacies of the imperial past and

competing memories. *Journal of Eurasian Studies*, 5, 107 – 115.

Kim, H. J. (2012). Security and vulnerability of SCADA systems over IP-based wireless sensor networks. *International Journal of Distributed Sensor Networks*, 8(11), 1 – 10.

Kostyuk, N. (2015). Ukraine: A cyber safe haven? In K. Geers (Ed.), *Cyber war in perspective: Russian aggression against Ukraine* (pp. 113 – 122). NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia.

Koval, M. (n.d.). *Ukraine's new cybersecurity strategy, the measures, and priorities set out in the strategy: The current state of cybersecurity law*. Ilyashev and Partners. http://attorneys.ua/en/publications/ukraines-new-cyber-security-strategy-the-measures-and-priorities-set-out-in-the-strategy-the-current-state-of-cyber-security-law/.

Larkin, B. (2013). The politics and poetics of infrastructure. *Annual Review of Anthropology*, 42, 327 – 343.

Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. Electricity-Information Sharing and Analysis Center. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

North Atlantic Treaty Organization. (2016). *Comprehensive Assistance Package for Ukraine* [Fact Sheet]. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_09/20160920_160920-compreh-ass-package-ukraine-en.pdf.

Poroshenko, P. (2017, September 20). *Poroshenko calls Russia 'Biggest Threat' to international security* [Video]. https://www.rferl.org/a/ukraine-russia-poroshenko-un/28747377.html.

Simmons, K., Stokes, B., & Poushter, J. (2015). *NATO publics blame Russia for Ukrainian crisis, but reluctant to provide military aid*. Pew Research Center. http://www.bruxelles2.eu/wp-content/uploads/2015/06/OpinPublicArmesUkraine@Pew150610i.pdf.

Ukaz Prezydenta Ukrayiny No. 32/2017 (2017). http://www.president.gov.ua/documents/322017-21282.

Whitehead, D. E., Owens, K., Gammel, D., & Smith, J. (2017), Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *2017 70th Annual Conference for Protective Relay Engineers* (pp. 1 – 8). Institute of Electrical and

Electronics Engineers.

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy*, 39(10), 6100 – 6119.

Zakon Ukrayiny No. 2163-VIII. (2017). http://zakon5.rada.gov.ua/laws/show/2163-19.