Cybersecurity in the energy industry of Ukraine: protection measures and challenges in the context of energy security

Cibersegurança na indústria energética da Ucrânia: medidas de proteção e desafios no contexto da segurança energética

Ciberseguridad en la industria energética de Ucrania: medidas de protección y desafíos en el contexto de la seguridad energética

How to cite:
Borychenko, O., Cherniavskyi, A., Muliarevych, O., Yurii Shelekh, Y. & Sabat, M. (2024). Cybersecurity in the energy industry of Ukraine: protection measures and challenges in the context of energy security. Revista Gestão & Tecnologia (Journal of Management & Technology), v. 24, n.4. p. 67-90

Olena Borychenko
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
https://orcid.org/0000-0002-6127-2945

Anatolii Cherniavskyi
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
https://orcid.org/0000-0003-2858-8224

Oleksandr Muliarevych
Lviv Polytechnic National University, Lviv, Ukraine
https://orcid.org/0000-0002-4644-7962

Yurii Shelekh
Lviv Polytechnic National University, Lviv, Ukraine
https://orcid.org/0000-0002-0283-993X

Myroslav Sabat
Lviv Polytechnic National University, Lviv, Ukraine
https://orcid.org/0000-0001-7448-0615

Scientific Editor: José Edson Lara
Organization Scientific Committee
Double Blind Review by SEER/OJS
Received on 19/07/2024
Approved on 21/09/2024

Abstract

The conflict between Ukraine and Russia is a hot topic in international geopolitics and geostrategic discussions. Ukraine's energy crisis was caused by the tactic of hitting Russia straight at the point of a crucial national object, especially the power plant. This was preceded by a cyberattack at the Chornobyl Nuclear Power Plant, followed by a traditional physical attack from the air. Numerous industries are impacted by the ensuing conflict, including the food, energy, and supply chains, particularly in the months leading up to the conflict (end of 2021). This quantitative study aims to investigate the cybersecurity environment in the energy sector of Ukraine in-depth. The study intends to uncover important protective strategies and obstacles by examining data from Google Scholar and Ukrainian websites. This will provide insightful information for improving the energy sector's resilience against cyber-attacks. In order to defend Ukraine's energy sector against cyber threats, the study's recommended countermeasures include modernizing vital infrastructure, creating a culture that values cybersecurity, safeguarding Industrial Control Systems (ICS), ongoing monitoring, staff training, cooperation, compliance with laws, and creating incident response plans. This study's conclusion emphasizes how crucial it is to work together and adapt continuously in order to strengthen Ukraine's energy security. Maintaining strong cybersecurity measures while maintaining operational efficiency is essential. Maintaining a constant focus on information exchange, resilience-building, and best practices is essential to protecting the energy infrastructure from ever-evolving cyber-attacks.

Keywords: Cyber war, Ukraine, Industrial Control system, Challenges, Protected measures

Resumo

O conflito entre a Ucrânia e a Rússia é um tema quente na geopolítica internacional e nas discussões geoestratégicas. A crise energética da Ucrânia foi causada pela táctica de atingir a Rússia directamente no ponto de um objectivo nacional crucial, especialmente a central eléctrica. Isto foi precedido por um ataque cibernético à Central Nuclear de Chornobyl, seguido de um tradicional ataque físico aéreo. Numerosas indústrias são afetadas pelo conflito que se segue, incluindo as cadeias alimentares, energéticas e de abastecimento, especialmente nos meses que antecederam o conflito (final de 2021). Este estudo quantitativo visa investigar em profundidade o ambiente de segurança cibernética no setor energético da Ucrânia. O estudo pretende descobrir importantes estratégias e obstáculos de proteção, examinando dados do Google Scholar e de sites ucranianos. Isto fornecerá informações perspicazes para melhorar a resiliência do setor energético contra ataques cibernéticos. A fim de defender o sector energético da Ucrânia contra ameaças cibernéticas, as contramedidas recomendadas pelo estudo incluem a modernização de infra-estruturas vitais, a criação de uma cultura que valoriza a segurança cibernética, a salvaguarda dos Sistemas de Controlo Industrial (ICS), a monitorização contínua, a formação de pessoal, a cooperação, o cumprimento das leis e a criação de incidentes. planos de resposta. A conclusão deste estudo sublinha a importância de trabalhar em conjunto e de se adaptar continuamente para reforçar a segurança energética da Ucrânia. É essencial manter fortes medidas de segurança cibernética e, ao mesmo tempo, manter a eficiência operacional. Manter um foco constante na troca de informações, na construção de resiliência e nas melhores práticas é essencial para proteger a infraestrutura energética contra ataques cibernéticos em constante evolução.

Palavras-chave: Guerra cibernética, Ucrânia, Sistema de controle industrial, Desafios, Medidas protegidas

Resumen

El conflicto entre Ucrania y Rusia es un tema candente en las discusiones geopolíticas y geoestratégicas internacionales. La crisis energética de Ucrania fue causada por la táctica de atacar a Rusia directamente en un objeto nacional crucial, especialmente la central eléctrica. Esto fue precedido por un ciberataque a la central nuclear de Chernóbil, seguido de un tradicional ataque físico desde el aire. Numerosas industrias se ven afectadas por el conflicto resultante, incluidas las cadenas de alimentos, energía y suministro, particularmente en los meses previos al conflicto (finales de 2021). Este estudio cuantitativo tiene como objetivo investigar en profundidad el entorno de ciberseguridad en el sector energético de Ucrania. El estudio pretende descubrir importantes estrategias y obstáculos de protección examinando datos de Google Scholar y sitios web ucranianos. Esto proporcionará información valiosa para mejorar la resiliencia del sector energético contra los ciberataques. Para defender el sector energético de Ucrania contra las amenazas cibernéticas, las contramedidas recomendadas en el estudio incluyen modernizar la infraestructura vital, crear una cultura que valore la ciberseguridad, salvaguardar los sistemas de control industrial (ICS), monitoreo continuo, capacitación del personal, cooperación, cumplimiento de las leyes y creación de incidentes. planes de respuesta. La conclusión de este estudio enfatiza lo crucial que es trabajar juntos y adaptarse continuamente para fortalecer la seguridad energética de Ucrania. Mantener fuertes medidas de ciberseguridad y al mismo tiempo mantener la eficiencia operativa es esencial. Mantener un enfoque constante en el intercambio de información, el desarrollo de resiliencia y las mejores prácticas es esencial para proteger la infraestructura energética de los ciberataques en constante evolución.

Palabras clave: Guerra cibernética, Ucrania, Sistema de control industrial, Desafíos, Medidas protegidas

1. INTRODUCTION

The Russian Federation violated the UN Charter on February 24, 2022, when it launched another military invasion of Ukraine. Aside from the harm and impact on people, there are worries over the security of civilians and civilian infrastructure from cyberattacks as well as kinetic strikes resulting from the continuing international armed conflict (Aviv & Ferri, 2023). Malware and viruses that are delivered remotely have the ability to jeopardize linked power systems, hospitals, airports, military installations, and any other location where computers connected to the internet are utilized to perform vital tasks. The integration of new communication technologies gives limitless opportunities for the appropriate collection of information as the world moves toward greater digitization, generating a basic dependency on good functioning in all spheres of society. While such dependency presents a wonderful potential for the development of an intelligent and efficient society, it also poses serious risks to the functioning of important utilities and crucial infrastructure (Aljohani, 2022). The digitalized world is projected to revolve around safety concerns arising from illicit activities that compromise the confidentiality, integrity, and availability of information in cyberspace, potentially causing harm to communication networks and information resources. It is especially concerning when cyberspace is used to further certain social, political, and military goals. Industrial control systems (ICS) in energy utilities, financial organizations, government agencies, and official servers have become the primary target of regular cyberattacks in recent years, primarily targeting data and information resources. The dramatic increase in cyberattacks indicates that politically driven cybercrime organizations, usually working for state governments, have been carrying out increasingly frequent and infringement-causing assaults on both public and private organizations, causing significant losses over time. For instance, due to allegations that it has launched cyberattacks on its opponents in order to further its military and political goals, Russia—which is renowned for its highly developed cyber capabilities—is viewed as the major antagonist in cyberspace (Plėta, Tvaronavičienė, Della Casa, & Agafonov, 2020).

United Kingdom, United states of America, Canada, Australia, and New Zealand together released an advice on April 20, 2022, alerting enterprises to the possibility that Russia's invasion of Ukraine might spark hostile cyber assaults throughout the globe. The adversarial actions are a reaction to the historic economic sanctions placed on Russia and the military support given to Ukraine by the United States and its allies to help it repel the Russian invasion (Advisory, 2022). Even if worries about energy cybersecurity were apparent even before the crisis, their importance has increased with the development of the war in Ukraine. The rapid use of renewable energy sources and the digitization of energy networks have made energy systems even more vulnerable. Transportation and industrial operations must be electrified in a future dependent on low-carbon technology (Bederna, Rajnai, & Szadeczky, 2020).

Currently, energy systems under digital management are being connected to sectors of the financial system that were formerly powered by fossil fuels, which makes them a simple target to hackers. Furthermore, a net-zero carbon emission future suggests the adoption of a more decentralized generating system. A network of distributed rooftop solar panels and windmills will be used to provide electricity instead of a few large fossil fuels- or gas-fired power plants. The addition of comprehensive communication technologies that connect the power lines, substations, and storage units to ensure fast and intelligent control makes these facilities far more vulnerable to attacks on the energy system. It's still unclear exactly what kind of widespread cyber and digital warfare attacks exist (Singh & Mahajan, 2021).

One instance of the growth in cyber threats and cyber activists targeting vital infrastructures, particularly energy systems, is the ongoing war between Russia and Ukraine. In 2015 and 2016, Russia severely interfered with Ukraine's electricity supply. This was followed in 2017 by the devastating NotPetya malware assault, which caused billions of dollars' worth of damage and affected the whole world. Russia has been using Ukraine as a field to test its newly developed cyber weapons ever since it invaded the country for the first time in 2014 (Desai & Manabat, 2022). With its historical Soviet infrastructure, which may have contributed to the successful execution of hundreds of cyberattacks that primarily targeted the energy infrastructure with the intention of gathering intelligence on Ukrainian forces and vital bases, it is possible to comprehend Ukraine's grid framework and technological potential. Therefore, Russia's choice to invade Ukraine may have been influenced by their employment of offensive cyber and technological warfare in the lead-up to and early stages of the 2022 conflict, perhaps providing them with an edge on the ground. According to–Massachusetts Institute of Technology evaluation research, major hacking attacks were undertaken against the Ukrainian electricity utilities during the initial stages of the most current military incursion (Zografopoulos, Hatziargyriou, & Konstantinou, 2023).

It was discovered that the assaults aimed to erase data from the targets' energy control rooms, yet the effect of these hacks on military operations is still unknown. Before the invasion, harmful software, vandalism, and distributed denial of service (DDoS) attacks on Ukrainian websites were believed to have come from Russia and its representatives. Russian military hackers are attempting to get into electricity substations in Ukraine which may have caused the loss of power for two million people were detected and stopped by the Ukrainian cyber response teams. However, the volunteer group known as the "IT Army," which is made up of a variety of hacktivists, has been assigned the duty of launching DDoS attacks against the governments of Belarus and Russia, targeting their banking and energy infrastructure in particular, in addition to identifying and reporting Russian disinformation campaigns. For example, to slow down the transfer of Russian troops and supplies, the Belarusian Cyber Partisans have concentrated more on wreaking havoc on the country's rail infrastructure (Tvaronavičienė, Plėta, Della Casa, & Latvys, 2020). The decentralized hacker collective "Anonymous" also revealed that they are formally engaged in a cyberwar targeting the Russian government. Government-owned energy systems, radio and television stations, and communication networks are its primary targets. Additionally, this has sparked appeals from the opposition, where Russian-aligned criminal organizations have openly endorsed the current conflict and threatened to retaliate against any country that attacks Russia's infrastructure. It is noteworthy to highlight that according to the Cyber-Peace Institute, by August 2022, Ukrainian authorities had compiled a list of over 300 vicious cyberattacks that targeted strategic locations around the nation (Gjesvik & Szulecki, 2023).

Worldwide, all other Critical National Infrastructure domains, including industry, transportation, communications, financial services, and defense, rely on electricity. The government and national security authorities should place a high priority on controlling the risks connected with the energy sector, as it is the foundation of all other sectors. Since its inception in the 1800s, the electricity industry has understandably concentrated on safety-related concerns; however, this is beginning to change, with cybersecurity threats emerging as a significant factor. Policy makers and important stakeholders in the electricity sector (generation, transmission, distribution, and consumption) are increasingly concerned about the substantial amount of interconnection in national and international energy systems and the cyber risks posed by this interconnection. It is obvious that a prolonged period of power outage in a sizable area will have detrimental effects on enterprises, governments, and larger society. It is also evident that the frequency and intensity of cyberattacks against the electrical industry are rising, and security professionals observe that threat actors are becoming more numerous and more capable. Only two other sectors—critical manufacturing and communications—report more occurrences involving attacks than the power industry, which is among the top three targeted industries in the US (Spînu, 2020).

There is a worldwide challenge here, as evidenced by the increasing complexity of threat actors observed in Europe, the Middle East, and Asia-Pacific. The cyberattacks that occurred in 2015 and 2016 on the Ukrainian power network marked a paradigm change in the ways that enemies may impact vital national infrastructure (Gjesvik & Szulecki, 2023).

The report assesses growing sources of cyber risk in the electricity sector and identifies evolving threats, threat actors, and vulnerabilities. It examines the key challenges to improving cybersecurity in the electricity sector, including contrasting security requirements, the cyber skills shortage, and their protection measures. Finally, the report offers recommendations for improving cybersecurity and looks at future trends – including the rise of "smart" technologies – that could bolster cybersecurity or pose new challenges.

This research aims to thoroughly examine the cybersecurity environment in Ukraine's energy sector, emphasizing challenges and protections in connection with energy security. The main goal is to locate and evaluate the cybersecurity policies and procedures the Ukrainian energy industry uses to protect critical infrastructure. At the same time, the report seeks to draw attention to the industry's ongoing problems, such as possible weak points, shifting cyber threats, and geopolitical effects. By examining these facets, the study offers significant perspectives that may advise and direct the creation of strong cybersecurity plans customized to the particular requirements of Ukraine's energy industry. Last but not least, the research aims to improve Ukraine's overall energy security by tackling and reducing cybersecurity threats inside its essential energy framework.

2. METHODOLOGY

This study uses a range of secondary data from different sources, the desk study technique, and a synthesis of the literature. A qualitative analysis grounded on the idea of incremental policy from several experts who swiftly embrace the new policy is also employed in this study. This is due to the fact that extra regulations that are only in effect temporarily can be used to predict large price spikes. The methodically analyze pertinent analyst reports, media articles, and yearly reports before gathering all the data in order to get knowledge about energy policy strategies, cybersecurity, and the connections between the two. We use additional information to shed insight into any situations when the investigation and review results conflict with those of other papers (Järvinen & Mik-Meyer, 2020).

The goal of this quantitative study approach is to offer an in-depth evaluation of the cybersecurity environment in the energy industry of Ukraine. The study intends to provide significant insights into the industry's issues and protection measures by utilizing searches on Google Scholar and authorized Ukrainian websites. These insights will be based on quantitative data and reliable sources

3 RESULTS AND DISCUSSION

3.1 The Energy Sector – Changes in Cyber Security

In the energy industry, the goal of cyber security is to maintain resilience and dependability even in the face of cyberattacks. A control system under assault in the energy industry cannot simply be unplugged from the network, unlike IT systems, as this may lead to safety hazards, brownouts, or even blackouts. Three well recognized protective objectives are identified in cyber security: confidentiality, integrity, and availability (CIA). The top goal in the energy field is determined by applications unique to the sector. For instance, integrity and availability are crucial in both generation and transmission. Device misconfiguration brought on by tampered or delayed data may eventually affect system dependability. The most important factor for the sophisticated metering infrastructure is maintaining the privacy of consumer personal information. Cybersecurity, sometimes known as computer safety, is a subset of nuclear security (Nguyen, 2023).

The protective aims of computer security are to prevent cyber activities that might directly or indirectly result in the unlawful disposal of nuclear or other radioactive substances, damage of radioactive substances or nuclear facilities, or theft of nuclear private data. The Ukraine's power grid strike in 2015 revealed the potential effect of cyberattacks on the electrical sector. The total cyber danger has risen as people utilize more digital gadgets and communicate in more complex ways. For example, as the substations are updated, digital technology replaces analog equipment. These new gadgets incorporate commercially accessible operating systems, communication protocols, and applications, resulting in a greater attack surface. This, along with interconnectedness, increases the complexity of managing specific cyber threats and provides possibilities for prospective adversaries to conduct cyber assaults. More instances of attacks on the energy industry may be found in the World Energy Council's report which includes examples from several sub-divisions of the energy sector (Kuzior, Lobanova, & Kalashnikova, 2021). Reports from the NTI and Chatham House provide examples from the nuclear realm. Threat agents include state and non-state actors, scriptwriters, disgruntled workers, skilled hackers and hacker organizations, organized criminals, hacktivists, and terrorists (Unal & Lewis, 2018). There are also not harmful cyber security incidents, such as user/administrator mistakes or technological flaws, that resemble or could ultimately have the same impact as a concerted assault regardless of the root cause of a cyber-security event, the potential impact on the energy industry is the same, such as brownouts, blackouts, or incorrect configuration of control systems (Ang & Utomo, 2017; Tarasenko et al., 2022).

3.2 Protection Concepts Reflecting Current Threats and Risks

Based on a study of the directions for reforming the Internet services market, this paper recommends a plan based on reform requirements, changes in macroeconomic indicators, and a desire for orientation and integration into the worldwide economic community. This plan envisions the creation of a framework for restructuring the Internet services market depending on the identified core themes, which include reforming the banking industry, upgrading small and medium-sized enterprises, attracting international investors, and increasing public activities. This policy should enable cost-effective and rapid utilization of Internet services, as well as the shift from an information to a communications society. The use of digital technologies ought to be developed, used, and regulated in a way that makes sure reliable, free, and fair trade, avoids unfair discrimination, gives individual users effective choices, promotes fair competition and innovation, promotes and protects human rights, and encourages groups involved in offering or receipt of online services (Cherniaieva et al., 2023).

This dilemma is significant to the entire energy industry. Historically, investment phases in the energy sector have followed the life spans of major equipment like as transformers or generators, which can last anywhere from 15 to 40 years. Secondary equipment for control and automation has a lifespan of up to 15 years. Before lately information and communication technology (ICT) was viewed as a support technology for power system stability. Nevertheless, these technologies are becoming increasingly important in ensuring a desirable degree of stability and resilience in the energy industry. The implementation of ICT in energy-related systems has been utilized for information sharing and automation for decades, but its popularity has skyrocketed recently (Davydiuk & Zubok, 2023). ICT enables utilities to handle systems better interactively, making new and old (aged) infrastructure more efficient. While combining ICT components is critical for modernizing the energy industry and reaping its advantages, the same networks increase complexity while also introducing new interdependencies and possible risks. New gadgets are vulnerable to the same flaws as general-purpose ICT equipment, which have a shorter lifespan than utility devices. Protection ideas are often developed during the procurement of a system, taking into account the risks and dangers that are recognized at the time. Threats and dangers are changing, and outdated systems and devices utilized in the network may not always meet with current operational and/or security requirements. This highlights a fundamental difficulty in today's energy systems. Furthermore, cyber safety in a multi-vendor system necessitates interoperability, with components relying on the same number of safety standards and criteria, which, of course, change depending on operational context (Maliarchuk, Danyk, & Briggs, 2019).

Protection strategies must address the diverse safety features of assets in a dynamic threat environment. Furthermore, commonly used legacy (ancient) network technology might not have an equal edition on the marketplace or may be incompatible with cutting-edge security needs. In addition, continuous operation without maintenance periods owing to high energy availability needs may result in known vulnerabilities in outdated equipment that occasionally need to be patched or addressed. Obsolete systems and proprietary technology raise further worries about the defense against current hazards and threats. This issue impacts generation, transmission, and distribution, and it exists in all energy subsectors. Important security and safety measures (such as physical protection) employed at nuclear sites are isolated from the internet and IT networks (Green, 2022).

They are also secured by cyber and physical security measures mandated by their various national regulators. Furthermore, nuclear power facilities are intended to close down safely if their equipment is able to detect a disruption (for example, an interruption in the energy grid). Even though the nuclear business is heavily regulated and routinely inspected, not all countries have explicit legislation in place for cyber defense in nuclear places (Holdridge, 2021).

3.3 Challenges in energy industry in Ukraine

The energy business, especially in Ukraine, confronts multiple cybersecurity concerns that are inextricably linked to the larger setting of energy security. Here are some major challenges (Ahamer, 2021; Naumenkova et al., 2022):

Table 1
Challenges in energy industry in Ukraine

Challenges	Description
Critical Infrastructure Vulnerabilities	The electricity plants, grids and control systems are essential parts of a country's infrastructure. They are the perfect targets for online attacks, which may result in significant electrical outages and disruptions
Geopolitical Tensions	Ukraine's geopolitical context makes the energy industry vulnerable to cyber assaults from state actors. Cyberattacks can be used to obtain a strategic advantage or to disrupt the country.
Legacy Systems and Outdated Technology	Many energy plants in Ukraine may now use antiquated systems and technologies. These systems may lack the appropriate security measures and upgrades, rendering them more vulnerable to cyber attacks
Lack of Cybersecurity Awareness and Training	Personnel in charge of managing energy infrastructure may lack cybersecurity training and awareness. Cyber attackers may exploit this information gap
Insufficient Investment in Cybersecurity	Inadequate financial resources may limit the energy industry's capacity to invest in effective cybersecurity solutions. This might lead to poor defense against growing cyber threats

Supply Chain Vulnerabilities	The interconnectedness of the energy supply network creates weaknesses. Cybercriminals might go after suppliers or a third-party service provider, obtaining illegal access to vital systems via insecure entry points
Increased Frequency of Cyber Attacks	Cyberattacks in the energy industry have increased internationally, including in Ukraine. Attacks by ransomware, breaches of information, and other malicious actions can have serious implications for energy security and infrastructure
Regulatory and Policy Challenges	Implementing effective cybersecurity legislation and procedures may be tough. A lack of defined norms or enforcement procedures may expose the energy sector to possible cyber risks.

To solve these issues, Ukraine's energy sector ought to prioritize security measures, invest in modernizing and safeguarding vital infrastructure, improve personnel training, and work with foreign partners to exchange intelligence on threats and best practices. Creating a comprehensive and adaptable cybersecurity plan is critical for protecting the energy industry and guaranteeing total security of energy in the country (Ahamer, 2021).

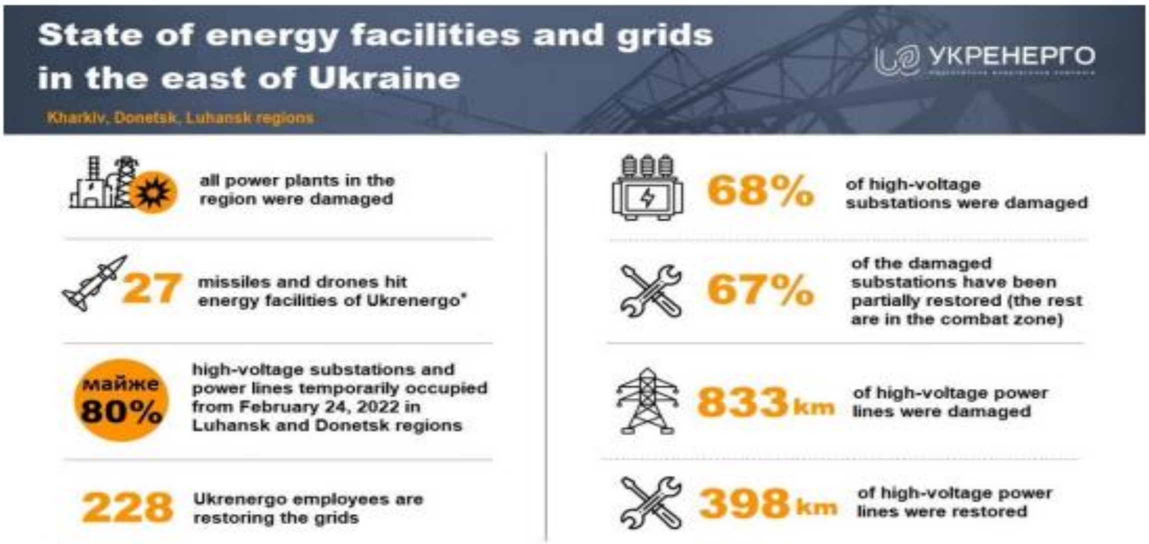

Figure 1. Ukrenergo- stats of energy facilities and grids in east Ukraine
Source: (Charter, 2023)

In April 2023, NEC "Ukrenergo" released early estimates of the company's losses and damage in the Kharkiv, Donetsk, and Lugansk areas as a consequence of Russian attack (Charter, 2023).

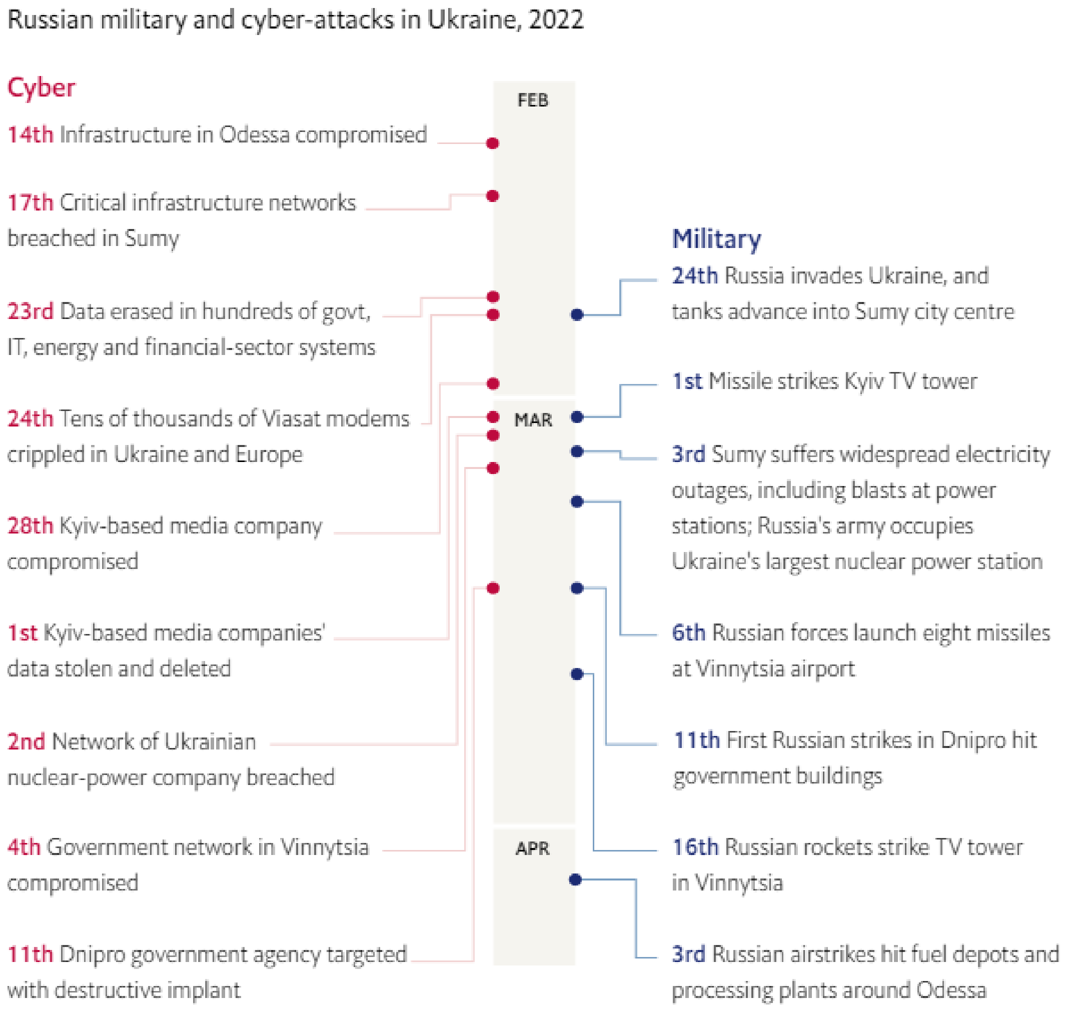
Russian military and cyber-attacks in Ukraine, 2022
Cyber
14th Infrastructure in Odessa compromised
17th Critical infrastructure networks breached in Sumy
23rd Data erased in hundreds of govt, IT, energy and financial-sector systems
24th Tens of thousands of Viasat modems crippled in Ukraine and Europe
28th Kyiv-based media company compromised
1st Kyiv-based media companies' data stolen and deleted
2nd Network of Ukrainian nuclear-power company breached
4th Government network in Vinnytsia compromised
11th Dnipro government agency targeted with destructive implant
FEB
MAR
APR
Military
24th Russia invades Ukraine, and tanks advance into Sumy city centre
1st Missile strikes Kyiv TV tower
3rd Sumy suffers widespread electricity outages, including blasts at power stations; Russia's army occupies Ukraine's largest nuclear power station
6th Russian forces launch eight missiles at Vinnytsia airport
11th First Russian strikes in Dnipro hit government buildings
16th Russian rockets strike TV tower in Vinnytsia
3rd Russian airstrikes hit fuel depots and processing plants around Odessa

Figure 2: Microsoft Digital Security Unit (Russia Seems to Be Co-Coordinating Cyber-Attacks with Its Military Campaign (n.d.)) (economist, 2022)

In the early stages of the Russian assault, American authorities predicted that Russian cyberattacks would devastate Ukraine's energy grid, banking system, and other infrastructure. To their amazement, this did not occur. However, a research produced by Microsoft reveals that Russian army and cyber assaults have worked closely throughout the battle, albeit on a lower scale than predicted (Charter, 2023).

3.4 Cyber war between Russia and Ukraine

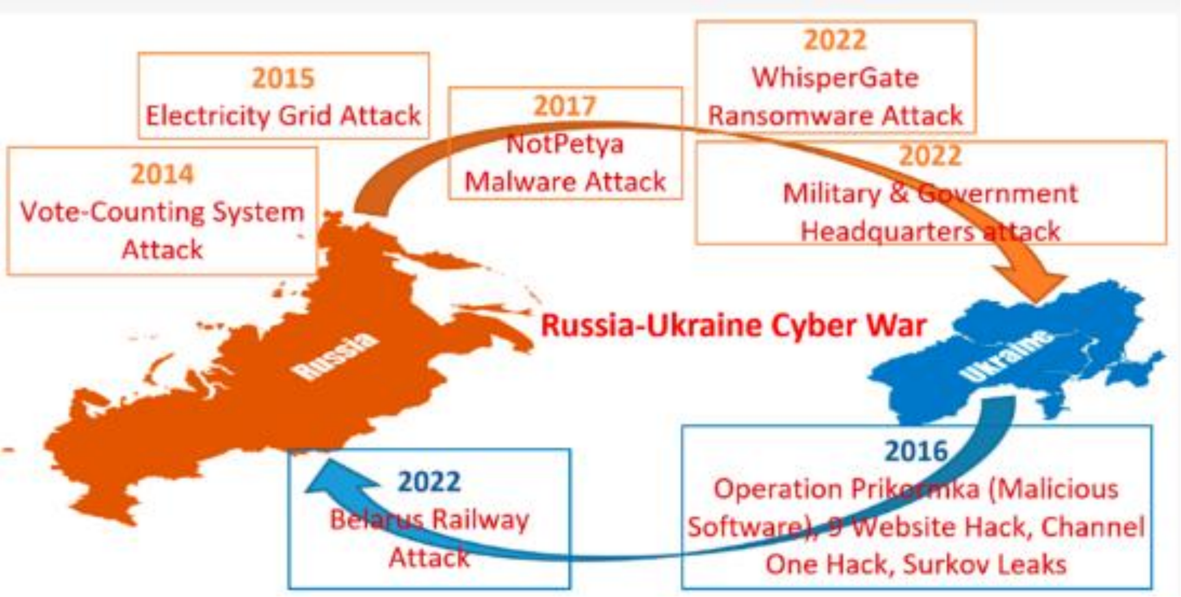
2015
Electricity Grid Attack
2014
Vote-Counting System Attack
2017
NotPetya Malware Attack
2022
WhisperGate Ransomware Attack
2022
Military & Government Headquarters attack
Russia
Russia-Ukraine Cyber War
Ukraine
2022
Belarus Railway Attack
2016
Operation Prikormka (Malicious Software), 9 Website Hack, Channel One Hack, Surkov Leaks

Figure 3. Background of Russia–Ukraine cyber war
Source: (Sufi, 2023)

According to Willett (2023), Russia employed aggressive cyberspace twice before the 2022 conflict. The barring of Georgian access to the internet was the connecting thing to a major disruption, with the bulk of events involving low-level cyber destruction. During the Russia-Ukraine war in 2022, Russia sought to interrupt services and infect Ukrainian networks with harmful malware. This includes phishing, denial-of-service assaults, and exploiting software weaknesses (Willett, 2023). According to a separate article from the Center for International and Strategic Studies (Lewis, 2022), one business uncovered eight unique families of destructive malware Russia used in these attacks. According to (Gibney, 2022), Russia utilized cyber warfare in its most recent actions, including the attacks on Georgia in 2008 and Crimea in 2014. Since then, Russia's cyber operations have utilized Ukraine as a "training ground".

As the battle rages, Russian intelligence gathering is perhaps the biggest cyber threat facing Ukraine right now, based on a Carnegie Endowment for International Peace study. Russian hackers may still have more influence if they are skilled at gathering really valuable intelligence that Moscow then effectively uses (Ateman, 2022). The cyber war between Russia and Ukraine, which started in 2014 and is evident from both academic and non-academic perspectives, is briefly described in Figure 3. Over the past ten years, cyberattacks by Russia have been more dangerous than those by Ukraine (Bing, 2022).

Russian cybercriminals hacked the Ukrainian vote-counting system on the day of the general elections (2014, requiring authorities to manually tally the ballots after erasing electronic records). A hack in 2015 that was attributed to a group associated with Russian military intelligence used malware known as "Industroyer" bringing down electricity for several hours in parts of Kyiv and western Ukraine (Gorchinskaya, Rudenko, & Schreiber, 2014). It was history's first blackout brought on by a cyberattack. The same group connected to Russian military intelligence was responsible for the 2017 NotPetya attack. 10% of all Ukrainian computers were infected by the malware software before its global spread (Kleist, 2021). A US estimate puts the cost of one of the worst cyberattacks ever to have cost businesses over $10 billion. Microsoft released WhisperGate, a ransomware-posing virus, on January 15, 2022. It was designed to target IT institutions, as well as several government and nonprofit organizations in Ukraine. On January 19, 2022, Global Affairs Canada was the target of a cyberattack after statements made by Canadian officials endorsing Ukraine. Early in February 2022, Microsoft disclosed that Actinium, a group thought to have links to Russian intelligence, was attacking government and military systems in Ukraine. This targeting, which started in October 2021, aims to obtain intelligence by listening in on people (Magafas & Demertzis).

There have been reports that Ukraine attacked Russia with many smaller-scale attacks in 2016. Operation Prikormka was one of these attacks that included the dissemination of malicious software that showed the price of fishing bait. It's unclear how much harm this rogue program has caused (Berting, 2023). Nine successful hacks of the websites of the separatist movement "Donetsk People's Republic" as well as networks and websites of Russian military armed companies and Russian propaganda sites hostile to Ukraine were part of another operation. Falcons Flame, Trinity, and Rukh, three members of the Ukrainian cyber alliance, broke into the Russian Channel One computer to initiate the "Channel One" attack. In addition, in October 2016, the Surkov Leaks disclosed plans to annex Crimea and incite separatist violence in the Donbas. There were 2337 emails and a large number of attachments in the incident. The functioning of Belarus' railway system was impacted by the most recent cyberattack by a Ukrainian group on January 24, 2022, which slowed Russian forces' progress through Belarus and to Ukraine's frontiers (Forsström, 2023).

3.5 Protection measures

In the context of Ukraine's energy security, cybersecurity threat prevention measures are critical. Here are some special protective measures designed for the Ukrainian power sector (Plėta et al., 2020; Tarasenko et al., 2022):

Table 2
Protective measures in energy industry

Protective measures	Description
Risk Assessment and Vulnerability Analysis	Conduct frequent threat assessments and vulnerability evaluations to detect possible threats and vulnerabilities in the energy infrastructure of Ukraine. This facilitates the development of specialized security measures
Regulatory Compliance	Follow and execute cybersecurity requirements issued by Ukrainian authorities. Compliance with defined criteria can improve the overall safety postures of the energy industry
Secure Communication Networks	Use secured communications protocols and encryption mechanisms for data transmission over energy networks. This helps to safeguard sensitive data from interception or manipulation.
Update and Secure Industrial Control Systems (ICS):	Maintain and safeguard industrial control systems in energy plants. This involves installing security updates, configuring firewalls, and using invasion prevention and detection systems
Monitoring and Anomaly Detection	Use constant monitoring systems to identify odd or suspicious activity on energy networks. Anomaly detection systems can assist in detecting possible cybersecurity concerns before they worsen
Employee Training and Awareness	Train energy sector workers on cybersecurity best procedures, with a focus on the unique risks and difficulties of the Ukrainian industry. To lower the likelihood of insider threats, foster a security-aware culture
Collaboration with Government Agencies	Work effectively with Ukrainian government entities responsible for cybersecurity. Create communication channels to exchange threat intelligence and coordinate reactions to possible cyber events
National Cybersecurity Strategy	Help implement Ukraine's national cybersecurity plan. Connect the energy sector's security procedures with the overall national policy to provide a consistent and complete defense against cyber-attacks
Backup and Recovery Planning	Develop and verify backup and restoration plans for essential systems. This guarantees that, in the case of a computer virus, data and operations may be recovered swiftly, reducing downtime
Supply Chain Security	Improve supply chain cybersecurity through vendor and supplier verification and monitoring. Verify that security protocols are followed through the supply chain in order to avoid vulnerabilities being introduced

Public-Private Partnerships	Encourage cooperation among the public and commercial sectors. Collaborate in collaborations between the private and public sectors to solve cybersecurity issues, exchange resources, and build a more robust energy system
Continuous Monitoring and Threat Intelligence	Continuously monitor networks and systems to detect unusual activity. Use security information feeds to keep up with the newest cyber hazards and weaknesses that may affect the energy sector
Crisis Management and Incident Response	Create and evaluate a crisis administration and incident response strategy. This should include defined protocols for recognizing, reacting to, and recuperating from cybersecurity issues while minimizing interruption to energy operations

In the evolving environment of security in Ukraine's energy business, discussing protective methods and issues is vital for guaranteeing strong energy security. As the author Gjesvik & Szulecki (2023) discuss Protection measures are required to protect the nation's key energy infrastructure from an increasing number of cyber-attacks. Ukraine has the difficulty of protecting its energy infrastructure from both local and foreign threats. As geopolitical tensions rise, cyberattacks that are state-sponsored become a serious issue, necessitating the installation of sophisticated defenses.

One essential component is the ongoing investment in modernizing and safeguarding ICS, which govern crucial energy infrastructure. Some systems are obsolete, demanding extensive changes to include the most recent security measures. In the research of Yakymchuk (2022) says that simultaneously, building a cybersecurity-aware mindset among energy professionals is critical for mitigating risks caused by human mistake and social engineering efforts. Collaboration develops as a preventive mechanism, not just in the energy industry, but also in collaborations with government agencies and worldwide cybersecurity groups. Gathering threat intelligence and taking part in cooperative activities improves the collective defensive posture against changing cyber threats. Implementing a thorough incident response strategy is critical for ensuring a timely and coordinated response to attainable cyber events.

Similarly Kruszka & Muzolf, (2022) emphasis that challenges remain in the form of financial constraints, regulatory complications, and the demand for ongoing adaptation to evolving threats. Maintaining a balance between protecting essential infrastructure and preserving operational efficiency is a problem that necessitates continual efforts, resources, and a diversified strategy. Finally, the cybersecurity conversation in Ukraine's energy business acts as a catalyst for educated choices, working together, and continuous development of defensive measures to strengthen security of energy in the face of increasing cyber threats.

The impact of smart technology on economic growth and development is debatable, not just among Ukrainian experts, but also among academics from other areas and nations. Goudarzi, Ghayoor, Waseem, Fahad, & Traore, (2022) explore the relationship between smart technology adoption and economic growth. In the paper Suprunenko et al. (2023). emphasizes that mitigating the impacts of global warming while maintaining balanced socioeconomic growth is the main objective. All engineering disciplines must work closely together to achieve interdisciplinary synergy and overcome challenging technical obstacles. Resource balancing, effective energy conversion technologies, renewable energy system integration, effective closed-loop economy construction strategies, and effective process and system integration with other socially significant issues should be the main areas of study. Defined guidelines and standards for significant digital data, taxation norms, labor organization features, and unfairness elimination must all be updated to match contemporary realities to minimize disparities. Utilizing these cutting-edge technologies to promote public welfare while retaining all of their benefits will only be feasible if effective international collaboration strategies and national regulatory laws are developed.

In the paper Prokopenko (2022) discuss that political communication is the process of creating and disseminating information with the main goal of addressing political issues with society or particular target audiences. To effectively serve the issue of impact among the target groups, information is primarily used in the context of the political management method to develop specific concepts, presumptions, views, preferences, and beliefs in addition to behavioral patterns. The policy of information may be seen as a strategy that uses knowledge to further political objectives or as an approach in the field of knowledge to advance their interests. The use of knowledge to exercise, uphold, and, if required, attain power is known as information policy. The strength of the evidence supporting the use of power determines how effective it is. Information management is the activity of the subject to form, convert, store, and transmit all types of information to update and carry out their aims in society. The primary goal of information policy is to distribute power and influence among political subjects according to their capacities and capacity to influence each other through the use of information. Information policy is a field of study connected to political relations.

The authors in the paper Redko (2022) discuss that future "green" energy development may have the following socioeconomic effects: 1) lowering the environmental burden caused by humans, which will raise living standards and general well-being; 2) extensively modernizing the fuel and energy infrastructure of the post-Soviet states to promote environmental innovation and attract investment; and 3) encouraging the expansion of businesses of all kinds and the generation of new jobs by former Soviet nations through the adoption of pertinent policy initiatives. Because of their economic potential to introduce energy from renewable sources, which enables them to implement numerous "green" projects in their investments, and enhance their financial and ecological achievements, renewable energy is the most announced growing growth in post-Soviet countries.

Similarly, in the research of Oglu Macidov (2023) emphasis that the creation of an international legal framework to combat cybercrime requires the Budapest Convention. It lays the groundwork for global collaboration, which is essential in the increasingly interconnected digital world of today. Nonetheless, considering the rapid pace at which technology is developing and the type of cybercrime, this legal document has to be updated and changed often to reflect new cybersecurity issues and advancements. The European Union is putting various measures—outlined in legislative and regulatory acts—into practice to prevent illicit conduct that compromises electronic information resources. These include directives from the European Commission from 2013 on preventing cyberattacks on information systems and from 2017 on combating scams and other financial offenses on the internet. Thus, in the context of modern law, cybercrime is understood as a particular term that primarily refers to computer crime. This includes situations in which a computer or other modern device serves as the primary tool or method for illicit activity directed towards assets, safety or intellectual property rights, moral issues, etc., as well as other situations in which a computer system is the primary method or tools of criminal activity directed toward other modern devices or information systems. Darkness, anonymity, distance, variety of sorts, globalization, speed, and innovation are some of their primary traits.

Tymoshenko, Redko, Serbov, Shashyna, & Slavkova, (2022) analysis that the influence of Industry 4.0 on the growth of energy scenarios may be seen from two angles. Scenarios may be generated utilizing Industry 4.0 technologies, which serve as a tool. Industry 4.0 can help outline scenario development goals. Energy-related study writers generally agree that implementing Industry 4.0 should focus on improving energy use. Research indicates significant disparities in aims and outcomes between energy scenarios, particularly for Ukraine. Researchers offered suggestions to increase the scenarios' credibility and openness. Think about the following to increase the scenarios' authority and accountability: Clearer citations and better distribution of information sources; Outlining the data processing techniques; Offering a comprehensive set of cost estimations Analyzing how changes in cost assumptions affect study findings; establishing targets that are in line with sustainable development goals and tracking achievements; addressing the effects of scenario outcomes on the environment; and putting information disclosure into practice. Energy strategy is impacted by research findings and present conditions during combat. The Ukrainian energy sector is still robust even after significant damage, which supports the findings of this paper. It highlights important transitions in Ukraine's post-war rehabilitation, including steps to strengthen the energy supply system, which differ from this article.

3. CONCLUSION

In Ukraine's energy business emphasizes the importance of strengthening Ukraine's energy safety in the face of growing cyber threats has been discussed in this report. The proposed protective methods, which range from modernizing essential infrastructure to building a cybersecurity awareness culture, highlight the broad approach necessary to effectively manage threats. Teamwork emerges as a critical component, not just inside the sector, but also through proactive relationships with governmental agencies and worldwide cybersecurity groups.

Although substantial progress has been achieved in establishing preventive measures, problems remain. Restricted financial resources, the frequency of out-of-date systems, and the ever-changing nature of digital hazards need an ongoing dedication toward adaptation and development.

Maintaining operational efficiency while still safeguarding key infrastructure is a tricky endeavor that requires constant monitoring. The geopolitical environment adds another degree of complication, with state-sponsored hackers being a persistent danger. Ukraine's energy business must stay resilient, investing in cutting-edge technology and cybersecurity methods to mitigate any interruptions.

Cybercrime in Ukraine's energy industry acts not only as an assessment of the issues encountered, but also as a road map for future robustness. Ukraine can strengthen its energy security by continuing to collaborate, invest, and adhere to best practices, assuring a continuous supply of energy while negotiating the complex environment of modern cyber threats. The continued commitment to cybersecurity discussions and adaptive measures is critical to ensuring the continuity and competitiveness of the energy system in Ukraine in an ever-changing digital era.

REFERENCES

Advisory, J. C. (2022). Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure [Press release]. Retrieved from https://www.cisa.gov/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

Ahamer, G. (2021). Major obstacles for implementing renewable energies in Ukraine. *International Journal of Global Energy Issues, 43*(5-6), 664-691.

Aljohani, T. M. (2022). Cyberattacks on Energy Infrastructures: Modern War Weapons. *arXiv preprint arXiv:2208.14225*.

Ateman, J. (2022). Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. Retrieved 10/2, 2024, from https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657

Aviv, I., & Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. International Journal of Critical Infrastructure Protection, 43, 100637.

Ayodeji, A., Mohamed, M., Li, L., Di Buono, A., Pierce, I., & Ahmed, H. (2023). Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors. *Progress in Nuclear Energy, 161*, 104738.

Bederna, Z., Rajnai, Z., & Szadeczky, T. (2020). *Attacks against energy, water and other critical infrastructure in the EU.* Paper presented at the 2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE).

Berting, F. S. (2023). The Ukraine cyber war: an analysis of the Russian cyber doctrine for comparing the Ukraine National Cyber Security Strategy with those of other western countries.

bing, J. P. C. (2022). The cyber war between Ukraine and Russia: An overview. Retrieved 11/2, 2024, from https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/

Charter, E. (2023). Ukrainian energy sector evaluation and damage assessment - IX. Retrieved from https://www.energycharter.org/fileadmin/DocumentsMedia/Occasional/2023_04_27_UA_sectoral_evaluation_and_damage_assessment_Version_IX.pdf

Cherniaieva, O., Orlenko, O., & Ashcheulova, O. (2023). The infrastructure of the Internet services market of the future: analysis of formation problems. *Futurity Economics&Law, 3*(1), 4-16.

Davydiuk, A., & Zubok, V. (2023). *Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War.* Paper presented at the 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon).

Desai, D., & Manabat, H. (2022). CyberWarfare: The Past, The Present and the foreseeable future.

Economist, t. (2022). Russia seems to be co-ordinating cyber-attacks with its military campaign [Press release]. Retrieved from https://www.economist.com/graphic-detail/2022/05/10/russia-seems-to-be-co-ordinating-cyber-attacks-with-its-military-campaign

Forsström, P. (2023). Russia's war on Ukraine: strategic and operational designs and implementation.

Gibney, E. (2022). Where is Russia's Cyberwar? Analysts Decipher Its Strategy. *cell*(2022).

Gjesvik, L., & Szulecki, K. (2023). Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout. *European Security, 32*(1), 104-124.

Gorchinskaya, K., Rudenko, O., & Schreiber, W. (2014). Authorities: Hackers foiled in bid to rig Ukraine presidential election results. *KyivPost, 25*, 14.

Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., & Traore, I. (2022). A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies, 15*(19), 6984.

Green, J. (2022). Moving Toward Strategic Cyber War Theory? Analysis of Russian State-backed Cyber Attacks.

Holdridge, C. M. (2021). Leveraging Cyberspace. Marine Corps Gazette.

Järvinen, M., & Mik-Meyer, N. (2020). *Qualitative analysis: Eight approaches for the social sciences*: Sage.

Kleist, V. F. (2021). Global Multinational Organizations: Unintended Threats from Nation-State Cyberwarfare (Vol. 24, pp. 229-234): Taylor & Francis.

Kruszka, L., & Muzolf, P. (2022). Introduction to Critical Energy Infrastructure Protection: Risks and Vulnerabilities *Critical Energy Infrastructure Protection* (pp. 1-14): IOS Press.

Kuzior, A., Lobanova, A., & Kalashnikova, L. (2021). Green energy in Ukraine: State, public demands, and trends. Energies, 14(22), 7745.

Lewis, J. A. (2022). Cyber War and Ukraine. Retrieved 10/2, 2024, from https://www.csis.org/analysis/cyber-war-and-ukraine

Magafas, L., & Demertzis, K. Russia vs Ukraine Cyberwarfare: Lessons Learned.

Maliarchuk, T., Danyk, Y., & Briggs, C. (2019). Hybrid Warfare and Cyber Effects in Energy Infrastructure. *Connections, 18*(1/2), 93-110.

Naumenkova, S., Mishchenko, V., & Mishchenko, S. (2022). Key energy indicators for sustainable development goals in Ukraine. *Problems and Perspectives in Management, 20*(1), 379-395.

Nguyen, P. (2023). All Bark and No Byte: A Case Study on Nuclear Weapons' Role in Cyber Deterrence.

oglu Macidov, S. T. (2023). Prosecuting Cybercrimes under International Legal Frameworks: Challenges and Innovations. *Futurity Economics&Law, 3*(3), 80-95.

Plėta, T., Tvaronavičienė, M., Della Casa, S., & Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases. *Insights into regional development. Vilnius: Entrepreneurship and Sustainability Center, 2020, vol. 2, no. 3.*

Prokopenko, O. (2022). Some aspects of the state information policy of the modern state: definitions of the future. *Futurity Economics&Law, 2*(4), 60-72.

Redko, K., Denyshchenko, L., Dobrovolska, O., Lukyanenko, N., & Kyryllova, Y. (2022). Development of green energy as a path to energy independence of the national economy. *Futurity Economics&Law, 2*(4), 36-42.

Singh, N. K., & Mahajan, V. (2021). Analysis and evaluation of cyber-attack impact on critical power system infrastructure. *Smart Science, 9*(1), 1-13.

Spînu, N. (2020). Ukraine Cybersecurity Governance Assessment. *Geneva Centre for Security Sector Governance/nov.*

Sufi, F. (2023). Social Media Analytics on Russia–Ukraine Cyber War with Natural Language Processing: Perspectives and Challenges. Information, 14(9), 485.

Suprunenko, S., Pylypenko, N., Trubnik, T., & Volchenko, N. (2023). Forecast of changes in the macroeconomic situation in Ukraine: smart economy of the future. *Futurity Economics&Law, 3*(3), 219-236.

Tarasenko, O., Mirkovets, D., Shevchyshen, A., Nahorniuk-Danyliuk, O., & Yermakov, Y. (2022). Cyber security as the basis for the national security of Ukraine. *Cuestiones politicas, 40*(73).

Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into regional development, 2*(4), 802-813.

Tymoshenko, M., Redko, K., Serbov, M., Shashyna, M., & Slavkova, O. (2022). The impact of industry 4.0 on modelling energy scenarios of the developing economies. *Journal on Innovation and Sustainability RISUS, 13*(4).

Unal, B., & Lewis, P. (2018). Cybersecurity of nuclear weapons systems. Chatham House.

Willett, M. (2023). The Cyber Dimension of the Russia–Ukraine War *Survival: October-November 2022* (pp. 7-26): Routledge.

Yakymchuk, A., Kardash, O., Popadynets, N., Yakubiv, V., Maksymiv, Y., Hryhoruk, I., & Kotsko, T. (2022). Modeling and governance of the Country's energy security: The example of Ukraine. *International Journal of Energy Economics and Policy, 12*(5), 280-286.

Zografopoulos, I., Hatziargyriou, N. D., & Konstantinou, C. (2023). Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. *IEEE Systems Journal*, 11, 36-47.