DIGITALES ARCHIV

ZBW – Leibniz-Informationszentrum Wirtschaft
ZBW – Leibniz Information Centre for Economics

Kazancı, Baybarshan Ali

Article

The strategic importance of cyber security in electric energy policies

International Journal of Energy Economics and Policy

Provided in Cooperation with:
International Journal of Energy Economics and Policy (IJEEP)

Reference: Kazancı, Baybarshan Ali (2024). The strategic importance of cyber security in electric energy policies. In: International Journal of Energy Economics and Policy 14 (4), S. 599 - 605. https://www.econjournals.com/index.php/ijeep/article/download/16244/8065/38077. doi:10.32479/ijeep.16244.

This Version is available at:
http://hdl.handle.net/11159/701107

Kontakt/Contact
ZBW – Leibniz-Informationszentrum Wirtschaft/Leibniz Information Centre for Economics
Düsternbrooker Weg 120
24105 Kiel (Germany)
E-Mail: *rights[at]zbw.eu*
https://www.zbw.eu/

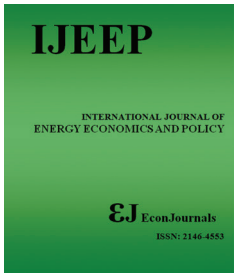
Standard-Nutzungsbedingungen:
Dieses Dokument darf zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden. Sie dürfen dieses Dokument nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen. Sofern für das Dokument eine Open-Content-Lizenz verwendet wurde, so gelten abweichend von diesen Nutzungsbedingungen die in der Lizenz gewährten Nutzungsrechte. Alle auf diesem Vorblatt angegebenen Informationen einschließlich der Rechteinformationen (z.B. Nennung einer Creative Commons Lizenz) wurden automatisch generiert und müssen durch Nutzer:innen vor einer Nachnutzung sorgfältig überprüft werden. Die Lizenzangaben stammen aus Publikationsmetadaten und können Fehler oder Ungenauigkeiten enthalten.

Terms of use:
This document may be saved and copied for your personal and scholarly purposes. You are not to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public. If the document is made available under a Creative Commons Licence you may exercise further usage rights as specified in the licence. All information provided on this publication cover sheet, including copyright details (e.g. indication of a Creative Commons license), was automatically generated and must be carefully reviewed by users prior to reuse. The license information is derived from publication metadata and may contain errors or inaccuracies.

https://savearchive.zbw.eu/termsofuse

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Mitglied der Leibniz-Gemeinschaft



International Journal of Energy Economics and Policy

ISSN: 2146-4553

available at http: www.econjournals.com

International Journal of Energy Economics and Policy, 2024, 14(4), 599-605.

The Strategic Importance of Cyber Security in Electric Energy Policies

Baybarshan Ali Kazancı*

Department of Management and Organization, Fatma Şenses Social Sciences Vocational High School, Kırıkkale University, 71460, Bahşılı/Kırıkkale/Türkiye. *Email: kazanci@kku.edu.tr

Received: 25 February 2024 **Accepted:** 15 June 2024 **DOI:** https://doi.org/10.32479/ijeep.16244

ABSTRACT

The electricity sector faces significant risks from devastating cyber events that can exacerbate global and regional instabilities, amplifying economic and security vulnerabilities worldwide. These attacks directly impact countries' electrical infrastructure, security policies, and everyday economic transactions. To comprehensively address these challenges, this study aims to conduct a thorough investigation into the politic implications of cyber threats within the realm of electrical energy, spanning both household use and production. The study concludes that the resilience of the electricity ecosystem remains low, indicating vulnerabilities. Furthermore, there's an inadequacy in the availability of cyber personnel within the markets. Additionally, an established international cybersecurity culture is lacking, highlighting a need for collective efforts to strengthen global cybersecurity measures in the electricity sector. Therefore, countries have to identify weaknesses in electricity networks and develop strategies to safeguard their infrastructure, serving as a foundational basis for the formulation of national and international strategic policies.

Keywords: Electricity Security, International Cyber Policies, Energy Security
JEL Classifications: Q40, Q43, F52

1. INTRODUCTION

With the widespread adoption of the internet and technology worldwide, the software sector, integral to nearly all economic transactions, has become indispensable for developed countries. Consequently, the advancement of technology-based industries has spurred international trade, propelling global companies to prominence. As we observe technology-intensive sectors, this pervasive progress is accelerating across all fields.

Many stages, such as instant information flow of production lines and parameters, recording of functional processes such as robotization, are realized thanks to software-based programs. On the consumption side, the consumer's needs are easily met through the digital world. War weapons such as aircraft, drones and tanks produced by countries in the defence industry are developed thanks to software-based applications. Just as software-based applications of the digital platform are used in every field, this cyber world is also used in the security and production of energy. In power plants of energy types such as nuclear, natural gas, petroleum and hydroelectric, web-based applications are used both in the production phase of energy and in its storage and protection.

The growing integration of artificial intelligence into the energy sector, driven by technological advancements, has brought both positive and negative impacts. Digital-based software in energy security has raised concerns spanning the past, present, and future. With the rising energy production, there's a corresponding increase in vulnerability to cyber attacks orchestrated by individuals or groups with malicious intent. Electricity, the backbone of modern society powering homes, industries, and critical infrastructure, sees an escalating risk of cyber attacks as our reliance on it intensifies. According to the World Economic Forum (WEF) in 2022, global geopolitical instability is forecasted to result in extensive and

This Journal is licensed under a Creative Commons Attribution 4.0 International License

disruptive cyber events in the years ahead (World Economic Forum, 2022a). This trend exposes a growingly fragmented and unpredictable landscape of concerns. These attacks not only compromise the reliability and availability of electricity but also present substantial economic and security threats. Consequently, leading countries in the energy sector face a heightened risk of cyber attacks. The energy infrastructure significantly impacts countries' security policies, daily commercial transactions, and the lives of households.

As the world navigates the ongoing digital revolution, identifying and mitigating vulnerabilities in electricity consumption becomes pivotal to ensuring the uninterrupted flow of this indispensable resource. Addressing these challenges necessitates an exploration of the global cybersecurity landscape within the energy sector, an evaluation of damages resulting from cyber attacks, and a specific examination of threats to electric energy. This study seeks to enhance comprehension of the challenges posed by cyber threats in both household and production-based energy sectors, while laying a foundation for strategic policies vital in safeguarding electricity network infrastructure. In this context, economic and political assessments were conducted, drawing insights from major cyber attacks that have impacted the energy sector.

2. CONTENT OF ENERGY SECURITY

With the evolving concept of security, energy security has gained significance and is now considered an integral part of national security. Consequently, it has become one of the foremost priorities for countries. Energy security and national security are mutually reinforcing. The assurance of energy security is crucial as it directly impacts a country's economic development and overall national security. It encompasses various aspects such as availability, accessibility, affordability, and sustainability of energy, and spans across political, ecological, geopolitical, and military dimensions (Erdal & Karakaya, 2012, p. 114)

Energy security, a pivotal component in the implementation of sustainable energy policies, encompasses a broad array of factors: reserves, resource quality, continuity, access, production, transportation, storage, trade, price stability, and infrastructure security. It also involves considerations such as import, conversion, transmission-distribution, and geographical security at national, regional, and global levels. Furthermore, it includes the political regimes of both energy-exporting and importing countries, along with aspects like security and stability, access to information, environmental impact, technology, and efficient energy management. In essence, energy security entails the reliable provision of energy to consumers in a timely, uninterrupted, efficient, high-quality, environmentally sustainable, and cost-effective manner (Ediger, 2008, p. 62). Energy security encompasses both energy supply security for energy-importing countries and energy demand security for energy-exporting countries. Over time, the term 'energy security' has increasingly been employed synonymously with 'energy supply security. (Erdal & Karakaya, 2012, p. 111). As a result, global challenges in the 21st century have brought increased attention to energy security. Events such as the September 11 attacks in 2001, Hurricane Katrina in 2005, and the Russia-Ukraine natural gas dispute in 2005-2006, along with ongoing threats concerning natural gas, have highlighted the vulnerability of energy supply and demand security. Disasters, terrorist or cyber attacks by non-state actors, and natural occurrences all pose risks to both short- and long-term energy supply security (Irie, 2017, pp. 38-39).

Energy security is built upon three pillars: physical, economic, and environmental sustainability. These dimensions provide a framework for understanding energy security. They underscore the complexities encountered in relationships between consumers and producers, particularly when third parties are involved. Any disruption to this tripartite structure poses a risk to energy security, highlighting the importance of addressing potential problems to safeguard energy stability (Asia Pacific Energy Research Centre, 2007, pp. 6-7).

From a political standpoint, energy security represents a critical arena wherein states face risks concerning sustainable development, social welfare, and political stability. Ensuring uninterrupted, affordable, and timely energy delivery is paramount. As such, all interconnected facilities—including power plants, energy transmission lines, LNG facilities, ports, sea routes, pipelines, and pump stations—spanning from production sites to end-users, form the backbone of critical energy infrastructure (Erkal, 2018). When states seek to utilize nuclear facilities in foreign nations for purposes beyond peaceful means, two fundamental elements pose inherent dangers: the human factor and electronic systems. Human intervention can directly lead to issues such as information security breaches, espionage activities, and physical harm. Similarly, electronic systems are susceptible to remote access interventions, which can manipulate software and information systems. Notably, the human factor is central to the creation of every electronic system and software. Consequently, these risks must be considered from the initial installation phase of the facility. In a wartime scenario, adversaries may exploit vulnerabilities through cyber attacks alongside physical assaults, utilizing missile and rocket systems (Gerçeker, 2013, pp. 91-121).

3. THE IMPORTANCE OF CYBER SECURITY IN THE ENERGY SECTOR

Cybersecurity holds a pivotal position within the energy sector, echoing the historical importance of security across human endeavors. Trust, a fundamental concept ingrained in various aspects from shelter to sustenance, is equally critical in the realm of energy resources. Primary and secondary energy resources, essential elements in every facet of basic economic life, significantly shape global politics, underscoring the necessity for their safe production and unhindered supply to consumers. This imperative gives rise to the concept of energy security. The International Energy Agency (IEA) defines energy security as the sustainment of an affordable and unrestricted energy flow for both consumers and producers, devoid of supply constraints (Cherp and Jewell, 2014). Definitions of energy security vary based on observable short and long-term effects. For instance, countries engaged in energy exportation or importation must establish energy security by fostering essential energy infrastructure and

undertaking comprehensive environmental protection planning over extended periods.

In today's technological landscape, security systems have evolved, consolidating into electronic infrastructures like automation and software. However, these technological strides have inadvertently opened doors to potential cyber attacks. The threats of data loss, breaches, and various violations stemming from these vulnerabilities have rendered cyber security indispensable (Kron Technology, 2023). Broadly defined, cyber security pertains to the capacity to prevent or defend against cyber attacks and incidents, safeguarding the availability and integrity of networks and infrastructure, alongside maintaining the confidentiality of enclosed information (IEA, 2021). It encompasses existing measures and actions aimed at achieving these objectives. In the contemporary era, cyber security is a ubiquitous presence across numerous sectors due to technological advancements, spanning the defense industry, healthcare, engineering, energy, and beyond. Its significance permeates various domains of operation.

Presently, cyber attacks targeting the energy system frequently involve malware infecting SCADA (Supervisory Control and Data Acquisition) systems, which oversee widely distributed facilities from a central location using devices such as computers, mobile phones, or tablets. These attacks have a historical footprint, dating back to 1982, when a gas pipeline explosion occurred in Siberia due to a cyber attack. Notably, the Stuxnet cyber attack on Iran's nuclear facilities in 2010 marked a significant milestone as the first known autonomous threat to specifically target and sabotage industrial control systems to such an extent. Further instances include the December 23, 2015 cyber attack on the control system of the power grid in three regions of Ukraine, leading to power outages affecting around 225,000 customers for several hours. In 2017, threat actors targeted US government institutions and critical manufacturing sectors, encompassing energy, water, aviation, and nuclear facilities (European Commission, 2019).

Figure 1 shows the trend of major cyber incidents worldwide over the 14-year period. Between 2006 and 2019, cyber incidents worldwide have shown a general increase, notably within the electricity sector. In 2019 alone, 10 out of 97 major cyber attacks were directed at the electricity sector (IEA, 2023a). These attacks persistently impact developed economies, often targeted by cybercriminals seeking profits. For instance, the May 2019 ransomware attack on Baltimore city computers caused approximately $18.2 million in damages, surpassing the requested ransom (Duncan, 2019). High-profile incidents in subsequent years further underscored vulnerabilities within the energy sector. In 2021, Encino Energy, a major US oil company, encountered fuel supply delays due to a cyber attack, leading to a 2-3% surge in oil futures (Russon, 2021). Similarly, in 2022, a cyber attack on a German oil supply firm disrupted the oil supply chain, resulting in Information Communication Technologies (ICT) damage (Pearson, 2022). The X-Force Threat Intelligence Index reported that 10.7% of cyber attacks in 2022 targeted the energy sector, ranking it fourth among targeted sectors (Bonderud, 2023). Recorded major cyber attacks surged by 150% over the previous year, totalling 35 incidents in the span of 5 years (Davis, 2022). At a micro level, public utility practices account for 40% of all incidents, with phishing constituting 20%, ransomware 15%, and data theft 23% in the mentioned sectors. Geographically, North America suffered the highest proportion, accounting for 46% of all attacks, followed by Europe and Latin America at 23%, with Asia, the Middle East, and Africa experiencing just under 5% (Bonderud, 2023).

Electric energy and gas companies face various cyber threats, including billing fraud, data theft, and ransomware. Notably, the energy sector's characteristics heighten cyber threats and risks to the public sector, attributed to an increase in targeted attacks on public companies and the sector's economic disruption and vulnerability due to nation-state actors (Tucker et al., 2020). The absence of centralized cybersecurity leadership in numerous organizations further exacerbates vulnerabilities within energy systems, encompassing both public and private entities involved in electricity generation, transmission, subscribers, and information technology (Akıllı and Özaslan, 2017; Kurnaz and Karatepe, 2019; İşbilen and Konar, 2020).

In table 1, the threat landscape for electrical energy is functionally divided into production, transmission, distribution, and network networks. Attacks on both traditional production systems and modern clean energy infrastructure during the production phase disrupt power plants, leading to service interruptions and ransomware exposure. Intruders gaining access to network control systems during the transmission phase have the potential to execute large-scale power cutoffs affecting customers. Despite a limited firewall in the distribution phase, attacks in this area can result in regional service losses and disruptions in substations. Finally, in the consumption phase, cyber attacks targeting smart meters of electrical energy consumers disrupt services by interrupting smart devices connected to the internet, including electric vehicles.

The focus of such attacks has expanded beyond IT networks. Recently, a government agency issued a warning about ransomware targeting a gas company's visibility into its pipeline operations. This attack resulted in lost productivity and revenue until the ransomware was successfully removed (America's Cyber Defence Agency, 2020).

4. ECONOMIC EFFECTS OF CYBER ATTACKS ON ELECTRICAL ENERGY

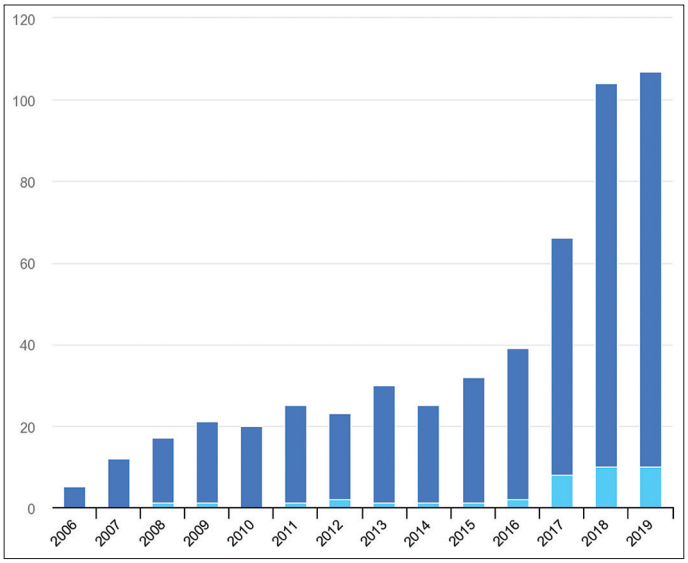
Traditionally designed energy technologies are rapidly integrating with digitalized systems, enabling a smarter energy return and active consumer participation in energy markets, thereby enhancing energy service benefits (European Commission, 2019). This digital evolution is reflected in the global market, with energy consumption surging from 7323 terawatt hours in 1980 to 25,530 terawatt hours in 2022, marking a substantial 349% increase over 42 years (Statista, 2023). Predictions by the IEA indicate that electricity's share in final energy consumption will escalate from 19% to 31% by 2040, primarily driven by burgeoning income levels, industrial growth, and service sector expansion in developing economies. This trajectory forecasts electricity consumption surpassing oil by 2040, accounting for nearly half

Table 1: Effects of potential threat in the electricity sectory

Threat Areas	Production	Transmission	Distribution	Network
Main reason	Legacy production systems and clean energy infrastructure designed without security in minutes	Physical security weaknesses allow access to network control systems	Distributed power systems and limited security built into SCADA systems	Large attack surface of IoT devices, including smart meters and electric vehicles
Results	Service disruption and ransomware attacks on power plants and clean energy generators	Large-scale disruption of customers' electricity through remote interruption of services	Disruption of substations leading to regional loss of service and interruption of service to customers	Theft of customer information, fraud and disruption of services

Source: Tucker et al., 2020

Figure 1: Major cyber incidents worldwide, 2006-2019



Source: IEA, 2023a

of oil consumption. Given electricity's fundamental role in the economy, potential outages trigger a spectrum of events, ranging from disruptions to life-threatening situations (IEA, 2021).

Prolonged power outages pose multifaceted challenges, disrupting traffic flow, posing health and security risks in critical areas such as water treatment and industrial operations involving cooling and heating. Sector-wise, outages curtail workplace productivity and supply chain continuity, complicating operations at sea ports and triggering disruptions in cash distribution and electronic payment systems. Transportation services, including airport operations, face suspension, while indirect sectors like tourism experience reduced attendance and altered travel plans (Lloyd's, 2015). Economic damage due to vulnerabilities in both public and private sector electrical systems is an inevitable consequence.

Cyber vulnerabilities within utility systems, whether owned by utilities or connected to public grids, have the potential to threaten their lifespan, company revenue, or public grid wiring. As early as 2010, interference with Puerto Rican utility wireless smart meters resulted in an estimated annual revenue loss of up to $400 million (Krebs, 2012). Although power outages due to cyber attacks up to 2015 were minor compared to those caused by natural disasters or maintenance errors, the 2015 attack on the Western Ukrainian power grid demonstrated the system's susceptibility to cyber threats. The attackers manually shut down 30 substations, leaving 225,000 people without power (E-ISAC, 2016). In the context of the global economy, the United States' largest 25 energy companies manage a network of 121 facilities spanning 94,000 miles (151,278 km) of supply lines (ABB Power Grids, 2020). Recent cyber attacks, such as the 2022 Ukrainian commercial satellite service disruption affecting Central Europe and the ongoing ransomware incidents in Costa Rica, highlight the potential paralysis of critical services, including tax collection, payments, trade, and electricity provision (World Economic Forum, 2022a). The global impact of regional cyber incidents continues to expand, with projected "Energy Information Technologies and Cyber Security Software Services" expenditures rising from $19 billion in 2020 to an estimated $32 billion by 2028 (Business Wire, 2020).

A scenario report has been released detailing the aftermath of cyber attacks that plunged 15 U.S. states into darkness, leaving 93 million people without electricity. The report discusses the economic repercussions, including direct damage to assets and infrastructure, reduced sales revenues for electricity supply companies, business revenue losses, and supply chain disruptions. The estimated impact on the U.S. economy stands at $243 billion, reaching over $1 trillion in the most severe version of the scenario. Additionally, the report analyses the direct and indirect effects on insurance losses, estimating a total compensation payout by the insurance industry ranging from $21.4 billion to $71.1 billion as the scenario escalates (Lloyd's, 2015).

Moreover, the introduction of new technologies like electric vehicle charging stations amplifies risks, showcasing the potential vulnerability of the entire electricity grid to a coordinated attack on these stations (Kenneth, 2017). In our rapidly evolving digital era, with the exponential growth of internet use and technology, the establishment of more robust defence systems, efficient emergency preparedness, and their seamless implementation have become paramount. The prompt detection of attacks, construction of virtual or physical barriers, and the formulation of national and regional cyber security policies are imperative to ensure cyber security in today's landscape (Goodman, 2008).

4.1. Political Effects

Among the foremost cybersecurity threats to the power grid lies the functionality of Industrial Control Systems (ICS), crucial for managing electrical processes and physical operations like circuit breaker control. These systems are progressively integrating with Internet-reliant technologies, enabling remote monitoring and enhancing cost and energy efficiency. However, this integration also widens the attack surface for hackers (Senate Republican Policy Committee, 2021).

The ongoing evolution from traditional energy technologies to modern digital systems is fostering interconnected networks, making energy systems smarter and augmenting consumer benefits. Yet, this digital transformation exposes vulnerabilities to potential cyber attacks, highlighting the criticality of robust cybersecurity policies. Threats to energy supply security pose significant risks (European Commission, 2023). While energy companies swiftly respond upon detecting cyber threats, sudden halts in their operations raise concerns about potential energy shortages. The efficacy of defence mechanisms within the energy sector remains unclear amid these challenges.

Organizations attacked by cyber threats often remain silent about ransom payments as a solution, temporarily quieting the threats. Initiatives like the Cybersecurity Risk Information Sharing Program (CRISP), funded partially by the Department of Energy (DOE) and managed by the Electric Information Sharing and Analysis Centre (E-ISAC), aim to foster threat data sharing, enhancing industry protection and resilience. However, despite increased awareness, cybersecurity personnel and managerial positions are not yet universally prevalent, and proactive efforts often lag in effectiveness (Bonderud, 2023). Recruitment and retention challenges in the cybersecurity sector, including a global shortage of skilled professionals, comparatively lower salaries offered by energy companies, and the lack of security expertise tailored to operational activities, pose substantial obstacles. The heightened degree of digitalization necessitates specialized cybersecurity skills. A recent survey revealed that 62% of respondents in public services acknowledged their organizations lacking the necessary tools and skills to counter cyber threats (IEA, 2023b). Training and retaining personnel capable of managing security systems remain a key challenge in addressing cyber attacks' causes and consequences within international energy supply security.

National governments worldwide are placing significant emphasis on legal frameworks to address cybersecurity concerns in critical sectors. The introduction of the Protecting Power Grid Resources with Cybersecurity Technology Act by US senators in April 2021 exemplifies efforts to develop laws, regulations, and decrees in the energy sector (Senate Republican Policy Committee, 2021). Despite ongoing programs globally, there remains no universally accepted global framework or standard. The European Union focuses on addressing critical differences between stakeholders and the potential burden on smaller or emerging organizations in cybersecurity policy designs for the electricity sector (European Court of Auditors, 2019). However, the current cybersecurity structure remains primarily a set of recommendations. Moreover, attacks threatening electrical energy, originating from sectors like oil and gas, are witnessing a paradigm shift. For instance, a scenario designed for the US portrays cyber hackers targeting a hydroelectric power plant by manipulating dam gates, potentially causing devastating floods (Honea et al., 2018). Such scenarios not only pose threats to human lives but also result in severe financial sanctions due to flood damages and the destruction of nearby settlements. Negative scenarios underscore the urgent need for international cooperation in the energy sector. In this context, a 2019 survey revealed that 86% of EU citizens advocate increased cooperation for ensuring secure energy access (European Commission, 2023).

Government agencies, non-profit organizations, global conglomerates, and small-to-medium-sized enterprises all rely on each other, necessitating the overcoming of information asymmetry collectively (World Economic Forum, 2022b). The convergence of various national and international policies supporting businesses, public institutions, and countries' infrastructures is increasingly driven by cyber events. Foreseeing the prominence of cybersecurity policies in the near future, countries may experience increased national or international energy costs. The demand for a qualified workforce to maintain electrical systems on a national scale may rise, potentially impacting the overall cost of electricity.

The impending energy transition poses new challenges; fossil fuel-exporting countries might face instability without reinventing themselves for a new energy era. Additionally, a rapid shift from fossil fuels could have significant global economic consequences, affecting workers, communities, cybersecurity, and dependencies on specific minerals (International Renewable Energy Agency [IRENA], 2019). Despite being the world's most advanced economy, the United States remains vulnerable to cyberattacks disrupting power grids, capable of impacting global adversaries' critical infrastructure. Government reports highlight challenges in recruiting a skilled workforce, limited confidential threat information sharing between public and private sectors, resource constraints, dependence on vulnerable critical infrastructure, and uncertainties in implementing cybersecurity standards (Senate Republican Policy Committee, 2021). Most organizations struggle to map their assets or identify key risk points within their networks, making cyber evaluation complex and hindering precise resource allocation for mitigation (World Economic Forum, 2022a).

5. CONCLUSION

The global energy sector is progressively transitioning from fossil fuels to electrical energy, becoming an essential resource for industries and an attractive target for cyber attacks. As such, cybersecurity policies are a top priority for developed economies like the US and Europe. Cyber resilience is particularly crucial for the electricity ecosystem due to its pivotal role as a societal backbone. Mass electricity outages not only instigate political and sociological unrest but also pose psychological implications, impacting a country's reputation on the global stage.

However, deficiencies exist in the electricity sector's cybersecurity policies, notably the shortage of trained personnel specialized in preventing energy-specific cyber attacks. Even with available expertise, setting wages below market rates diminishes the industry's attractiveness for cybersecurity professionals. Bridging the cyber talent gap within the electricity industry is essential to avoid exacerbating global/national distributor companies' macro and microeconomic losses.

To mitigate risks, it's crucial for governments, global and national energy organizations to proactively devise cyber risk action plans, including scenario-based strategies to combat cyber attacks. Collaborative efforts among countries are imperative to identify and address risks within the electricity sector. Governments

should play a primary role in protecting against cyber attacks through legislative measures, necessitating common international legislation that integrates cybersecurity policies within the next decade.

International electrical energy security necessitates a proactive public-private partnership. Large public and private organizations are likely to establish new units at senior management levels dedicated to cybersecurity within the coming years. Identified deficiencies in the study include the insufficient proliferation of cybersecurity culture in the electrical energy sector and the absence of established new cybersecurity models. Furthermore, the lack of an international organization specifically focused on cybersecurity in the energy sector poses challenges. Additionally, the unsuitability of electrical energy for local, regional, or national storage systems reduces the ecosystem's resistance, limiting feasible precautionary measures in this area.

REFERENCES

ABB Power Grids. (2020), Data ABB. Available from: https://library.e.abb.com/public/2a4edd749ba54d9cb83050d2e145a9c3/velocity-suite-brochure-9akk106930a8237-a4-web.pdf?x-sign=ampb4fy2xwiwtxhlqunhxzr84p4oiwyti8cxkkof8nxax3hdlq5m3omm8r5hhoqw [Last accessed on 2023 Apr 28].

Akıllı, H., Özaslan R. (2017), Su kayıplarının önlenmesinde teknoloji kullanımı: Büyükşehir belediyelerinde SCADA uygulaması. Suleyman Demirel University Journal of Faculty of Economics and Administrative Sciences, 22, 1599-1618.

America's Cyber Defence Agency. (2020), Ransomware Impacting Pipeline Operations, Washington. Available from: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-049a [Last accessed on 2023 Mar 06].

Bonderud, D. (2023), 2022 Industry Threat Recap: Energy; Security Intelligence. Portsmouth: Security Intelligence. Available from: https://securityintelligence.com/articles/2022-industry-threat-recap-energy [Last accessed on 2023 Nov 09].

Business Wire. (2020), Navigant Research Report Finds Global Annual Market for Energy IT and Cybersecurity for Software and Services is Expected to Reach $32 Billion by 2028. Available from: https://www.businesswire.com/news/home/20200211005108/en/navigant-research-report-finds-global-annual-market [Last accessed on 2023 Feb 11].

Cherp, A., Jewell, J. (2014), The concept of energy security: Beyond the four as. Energy Policy, 75, 415-421.

Davis, D. (2022), 5 Big Cyberattacks in Oil and Gas. Available from: https://www.oilandgasiq.com/digital-transformation/articles/5-big-cyber-security-attacks-in-oil-and-gas [Last accessed on 2023 Jun 20].

Duncan, I. (2019), Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts. Maryland, U.S: Baltimore Sun. Available from: https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html [Last accessed on 2023 Nov 01].

Electric Information Sharing and Analysis Centre. (2016), Analysis of the Cyber Attack on the Ukrainian Power Grid. Available from: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/e-isac_sans_ukraine_DUC_5.pdf [Last accessed on 2023 May 04].

European Commission. (2019), Commission Recommendation Cybersecurity in the Energy Sector. Available from: https://energy.ec.europa.eu/system/files/2019-04/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final_0.pdf [Last accessed on 2023 Jun 17].

European Commission. (2023), Critical Infrastructure and Cybersecurity. Available from: https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en [Last accessed on 2023 Dec 11].

European Court of Auditors. (2019), Challenges to Effective EU Cybersecurity Policy. European Union. Available from: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf [Last accessed on 2023 May 01].

Goodman, S.E. (2008), Critical information infrastructure protection. In: Responses to Cyber Terrorism NATO Science for Piece and Security. Ankara: IOS Press, Centre of Excellence Defence against Terrorism.

Honea, M., Yamamoto, Y., Laux, J., Guiliano, C., Hart, D.M. (2018), Hydropower Facilities: Vulnerability to Cyber Attacks. Water Power and DAM Construction. Available from: https://www.waterpowermagazine.com/features/featureunder-cyber-attack-7051600 [Last accessed on 2023 Mar 14].

International Energy Agency. (2021), Enhancing Cyber Resilience in Electricity Systems. Available from: https://iea.blob.core.windows.net/assets/0ddf8935-be23-4d5f-b798-3aad1f32432f/enhancing_cyber_resilience_in_electricity_systems.pdf [Last accessed on 2023 May 29].

International Energy Agency. (2023a), Significant Cyber Incidents Worldwide, 2006-2019. Available from: https://www.iea.org/data-and-statistics/charts/significant-cyber-incidents-worldwide-2006-2019 [Last accessed on 2023 Dec 29].

International Energy Agency. (2023b), Cybersecurity-is the Power System Lagging Behind? Available from: https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind [Last accessed on 2023 Nov 13].

International Renewable Energy Agency. (2019), A New World: The Geopolitics of the Energy Transformation. Available from: https://www.irena.org/-/media/files/irena/agency/publication/2019/jan/global_commission_geopolitics_new_world_2019.pdf [Last accessed on 2023 May 24].

İşbilen, F., Konar, M. (2020), Uçak sistemlerinin SCADA ile modellenmesi. Avrupa Bilim ve Teknoloji Dergisi, 18, 338-346.

Kenneth, R. (2017). Electric Vehicle Cyber Research, presentation slides for SANS Automotive Cybersecurity Workshop. https://www.sans.org/summit-archives/file/summit-archive-1493817272.pdf [Last accessed on 2023 Nov 14].

Krebs, B. (2012), FBI: Smart Meter Hacks Likely to Spread. Krebs on Security. Available from: https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread [Last accessed on 2023 Jan 10].

Kron Technology. (2023), Enerji Sektöründe Siber Güvenlik. Available from: https://kron.com.tr/enerji-sektorunde-siber-guvenlik [Last accessed on 2023 Apr 04].

Kurnaz, S., Karatepe, S. (2019), Kamusal Kritik Tesislerin Güvenliği Kapsamında Türkiye'Deki Hava Alanlarının Siber Güvenliği. 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı. p119-129.

Lloyd's. (2015), The Insurance Implications of a Cyber Attack on the US Power Grid. Available from: https://assets.lloyds.com/assets/pdf-business-blackout-business-blackout20150708/1/pdf-business-blackout-business-blackout20150708.pdf [Last accessed on 2023 Mar 18].

Pearson, J. (2022), Shell Re-Routes Oil Supplies after Cyberattack on German Firm. United Kingdom: Reuters. Available from: https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01 [Last accessed on 2023 Aug 20].

Russon, A. (2021), ABD'de Siber Saldırı: Bilgisayar Korsanları Ülkenin en Büyük Boru Hattını Devre Dışı Bıraktı, Akaryakıt Karayoluyla Taşınacak. BBC News. Available from: https://www.bbc.com/turkce/haberler-dunya-57056048 [Last accessed on 2023 Apr 04].

Senate Republican Policy Committee. (2021), Infrastructure Cybersecurity: The U.S. Electric, Grid. Available from: https://www.rpc.senate.gov/policy-papers/infrastructure-cybersecurity-the-us-electric-grid [Last accessed on 2023 Nov 19].

Statista. (2023), Net Electricity Consumption Worldwide in Select Years from 1980 to 2022. Available from: https://www.statista.com/statistics/280704/world-power-consumption/#:~:text=the%20world's%20electricity%20consumption%20has,25%2c500%20terawatt%2dhours%20in%202022 [Last accessed on 2023 Sep 19].

Tucker, B., Maruyama, A., Wallance, D. (2020), The Energy-Sector Threat: How to Address Cybersecurity Vulnerabilities. New York City: Mc Kinsey and Company. p1-12.

World Economic Forum. (2022a), Systemic Cybersecurity Risk and Role of the Global Community: Managing the Unmanageable. Available from: https://www3.weforum.org/docs/wef_gfc_cybersecurity_2022.pdf [Last accessed on 2023 Sep 10].

World Economic Forum. (2022b), Cyber Energy Sector Trust Value Chain. Available from: https://www.weforum.org/agenda/2022/11/cybersecurity-energy-sector-trust-value-chain [Last accessed on 2023 Nov 19].