STRATEGIC DIGITALIZATION OF ENERGY INFRASTRUCTURES: CYBER AND GEO-ECONOMIC ISSUES

GIANMARCO GABRIELE MARCHIONNA AND ELIO BRANDO

ABSTRACT

Digitisation is a broad concept that includes implementation approaches such as the Internet of Things (IoT), sectoral application such as Industry 4.0 and systemic abstraction such as the System of Systems (SoS). The implementation of advanced technologies in the digitalization of energy infrastructure is likely to lead to a rapid development of high-tech facilities. However, these advances will also lead to an increase in geo-economic, geopolitical and cyber risks. This paper addresses the importance of new energy infrastructure and technological advances, focusing on the exposure to risks arising from the cyber domain and its geo-economic and digital implications. The paper provides an overview of the geo-economics of energy transition in the context of strategic digitisation, with a governance perspective. Significant features of the energy systems transition are described and a conceptualisation of digital technologies is provided. The state-of-the-art of cybersecurity developments in the context of energy security is assessed, focusing on cyber attacks on energy infrastructure and how to counter them through a security governance framework. Finally, the paper outlines the main risk scenarios for building energy governance, highlighting the challenges and issues in addressing the strategic digitisation of energy systems.

Keywords: *Energy transition; cybersecurity; digitalization; cyber-attack; infrastructure; geopolitics; geoeconomics*

GEOECONOMICS OF ENERGY TRANSITION AND EMERGING TECHNOLOGIES

Geoeconomics does not have a uniform definition and is mistakenly used interchangeably with geopolitics. In fact, they are terms that can be used together to describe the complex interaction between economic and political factors in international relations. In some cases, economic power can be used as a tool of geopolitical strategy, and in others, political power can be used to promote economic interests. According to Wigell (2016: 135), geoeconomics is defined as "the geostrategic use of political power by economic means," while Blackwill and Harris (2016: 9) describe it as "the use of economic instruments to promote and defend national interests, and to produce beneficial geopolitical results; and the effects of other nations' economic actions on a country's geopolitical goals." Geoeconomics involves pursuing influence in the global economy or a given region while also strengthening one's economic resilience. Diesen (2019: 568) furtherly deepens the concept of "asymmetrical dependence," which refers to the ability of a more powerful and less dependent state to set favorable conditions for economic cooperation and to extract political concessions from a more dependent state.

The study of digital energy transition in this context holds significant importance, due to the intricate economic connections formed by global value chains which subsequently influence power dynamics. Within this framework, regions abundant in renewable resources could emerge as desirable destinations for industries aiming to reduce carbon emissions. Moreover, the thesis that dependence on imported hydrocarbons will soon be supplanted by the import of renewable energy, crucial materials such as lithium for batteries, rare earth elements for wind turbines, or sustainable biofuels for transport, paves the way for new strategic alliances.

Despite the more even distribution of renewable energy sources compared to oil and gas, resources will remain essential in a net-zero world. For

example, sites with high renewable energy endowments will be critical for decarbonizing industrial production. Manufacturing clean energy technologies will require increasing volumes of critical minerals, such as lithium, silicon and rare earth elements, whose supply is even more geographically concentrated than that of hydrocarbons. Moreover, natural gas is likely to retain its strategic significance for a considerable period.

Energy infrastructure will also remain essential, including pipelines for transporting clean hydrogen or hydrogen-methane blends, seaports for handling sustainable liquid fuels and hydrogen, and tube trailers for road transportation. With the electrification of new sectors, such as transport and industrial processes, there will be a need for better-quality grid infrastructure and more regional interconnections. Grid infrastructure can also be used as a means of projecting political power and authority beyond territorial space.

Drawing on Diesen and Wigell's theoretical foundations, this paper examines the geoeconomics of energy transition in terms of resources, energy infrastructure, strategic industries and clean energy technologies, and the rules of international economic interaction. Foundational factors such as economic considerations, political will and public perceptions are likely to shape the direction of energy policy and, consequently, the implementation of cybersecurity and digital measures. Addressing the risks' exposure in the context of the digital domain and its implications in geoeconomics, this work focuses on the challenges of energy system digitalization, building on the current composition of energy infrastructure and the role of cybersecurity in this context. Finally, it highlights the resulting governance challenges with a cutting-edge approach.

DIGITALIZATION OF ENERGY SYSTEMS

The advancement of data science and artificial intelligence (AI) has led to digitalization being viewed as a critical solution for addressing sustainability issues in energy systems (Huang et al., 2017; Gouvea et al., 2018). Digitalization provides a new norm for the systemization of knowledge from the physical phenomenon, particularly for energy systems that involve various energy conversion, transmission, and consumption processes, by utilizing improved sensor technology, AI algorithms, cloud computing, remote control, and more .

As the energy system transitions to net-zero and variable renewable energy supply becomes more dominant, the importance of digital technology will become even more significant (Bertoli, 2022). Digitalization implies access to more granular data and advanced analytics capabilities, which allows net-zero emission energy systems to accurately quantify the benefits brought by their operations. Despite the successful digital transformation cases, the design principles and operation regimes of energy systems remain largely unchanged in practice (IEA, 2017). The integration of digital technologies and energy systems is still largely inarticulate. In order to fully unleash the power of numeric modeling and optimization in the energy sector, the digital artifacts of different components of energy systems need to be well linked to each other. The concept and the development of cyber-physical systems for future energy systems have been proposed and intensively investigated in recent years (NIST, 2018). The concept of Cyber-Physical Systems (CPS) is defined as "co-engineered interacting networks of physical and computational components" (NIST, 2018), and it aims to create a virtual representation or digital twin of real entities in physical space and seek optimal solutions to real-world problems by exploring the cyberspace. The digital assistance ability provided by such CPS has largely transformed many traditional industries, but the energy industry has not been sufficiently engaged (Hold et al., 2017). In terms of computational framework, there are three basic elements for such energy system digital assistance: data,

analysis, and connectivity. Information provided by data serves as the basis for digital assistance, while analysis extracts valuable insights from incoming data. Connectivity, on the other hand, helps bridge communication gaps between humans, devices and machines, enabling the efficient collection, analysis and implementation of data and models. These three components, briefly described, explain the high added value of CPS in terms of continuous improvement.

The history of digitalization can be traced back to the 1940s when Norbert Wiener introduced cybernetics as control of any system using technology (Ashby, 1961). Since then, cyberspace has been widely used to describe the artificial world where humans navigate in information-based space (Benedikt, 1991). Digitalization is an inclusive concept that refers to implementation approaches (e.g. IoT), sectoral application (e.g. Industry 4.0), and systematic abstraction (e.g. SoS) (Geisberge and Broy, 2015). The definition of cyber-physical systems (CPS) by NIST (2018), highlights the iterative interaction between physical space and cyberspace rather than pure numerical simulation and optimization. This definition of digitalization aligns with the future trends of the net-zero energy system transition, which will evolve into a decentralized and interconnected network rather than isolated dots: in other words, the way digitalization is defined here fits with the idea that in the future, energy systems will be more connected and decentralized, compared to the current model where energy sources are often located in isolation from one another. Therefore, the interpretation of digitalization from the perspective of interacting networks holds more significance. Other digitalization conceptions that are similar to CPS include the Internet of Things (IoT), Embedded Systems, System of Systems (SoS), Industry 4.0, and Machine-to-Machine (M2M) communication (Törngren et al. 2014; Geisberge, Broy, 2015). All these concepts have in common the coordination of interconnected digital and physical systems, echoing the meaning expressed above by NIST.

The innovation of digitalization depends on various hardware and software technologies. While the German Academy of Science and Engineering (Acatech) lists six aspects, including physical awareness, prediction ability, coordination, human-machine interaction, learning ability, and adaptation flexibility (Geisberge and Broy, 2015), the European Parliamentary Research Service (2021) recognizes the following key enabling technologies: advanced manufacturing, advanced materials and nanomaterials, life-science technologies, micro/nano-electronics and photonics, artificial intelligence, and security and connectivity technologies. Simultaneously, in the context of energy system digitalization, the key enabling technologies include data acquisition, data fusion, data analytics, decision-making, and decision implementation (Cao et al., 2023).

The first step towards future data manipulation in the energy system is 'data acquisition', obtaining state-of-the-art data from different sectors, including generation, storage, transmission, and consumption. However, the high penetration of variable renewable energy has changed the operation regime of the power system, making data acquisition more challenging. Similarly, data from other energy domains, like natural gas networks, is monitored on different time scales and faces new challenges such as increasing variability and regional coordination.

'Data fusion' is the process of merging data from different sources and dealing with possible heterogeneity and inconsistency. Data integration is essential for many digitalization applications, particularly when using cloud computing. For example, district-scale energy systems have control centers where sub-system-level information is exchanged. In such cases, it is essential to have a standard platform to handle heterogeneity from different data sources.

Most literature on energy system digitalization focuses on 'data analytics'. However, most studies on power plant optimization or district-scale

energy system planning use handcrafted data and tailored algorithms, making the solutions less reusable. The challenges for large-scale energy system digitalization require high adaptability to solve the Nth-of-a-kind (NOAK) problem as long as it has already solved the First-of-a-kind (FOAK) problem.

Coordinated 'decision-making' ability is another essential feature of energy system digitalization. Energy systems have physical entities at different levels of detail, and different interacting agents exist in the energy system. Digital assistance should provide a multi-agent simulation platform that can mimic the interactions between various entities in the energy realm. The coordinated problem-solving strategy is crucial for future energy system digitalization, particularly as distributed energy resource utilization becomes a key feature of future energy systems. Digital assistance can integrate external information to improve the entire energy system supply chain, achieving enterprise optimization.

Finally, 'decision implementation': Digitalization can enable closed-loop control of energy systems by coupling cyber and physical spaces, ideally automatically. Successful examples include scheduling appliances in smart homes through embedded optimization algorithms in different appliances. However, fully optimal operations of energy systems enabled by digitalization are limited to specific scenarios and conditions.

All these conceptions share the common feature of linking computers and physical systems horizontally and vertically. There are still several significant gaps in the implementation of solutions that address these needs. However, the goal of cross-sector coordination through the digitalization of energy infrastructure is not that far off with CPS.

The importance of cross-sector collaboration to fully realize the potential of digitalization in the context of energy system digitalization cannot be overstated. The rapid pace of digitalization and its reliance on key enabling technologies make it essential to bridge the significant gaps that exist in the implementation of solutions that address these needs. In this regard, Cyber-Physical Systems (CPS) offer a promising solution by linking computers and physical systems horizontally and vertically. To achieve this goal, stakeholders must collaborate to develop a comprehensive strategy for integrating CPS into energy infrastructure. This will require a deep understanding of the technical aspects of CPS, as well as the economic and regulatory frameworks that govern the energy sector. It is also crucial to prioritize cybersecurity as an integral part of the implementation of CPS to protect against emerging vulnerabilities that can be exploited by malicious actors with different and sophisticated cyber-attacks.

DEFENDING THE GRID: CYBER-ATTACKS ON ENERGY INFRASTRUCTURE

In modern times, companies and enterprises providing social or private services in every country have a security team responsible for the physical and cyber safety of their site (Reshmi, 2021). Cyberterrorism is a complex and modern phenomenon that affects all developed countries with access to computers and the Internet (Dargahi et al., 2019). Cyber-attacks pose a direct threat to the security of citizens as well as the functioning of the state, economy, society, science, and education. These attacks can be carried out remotely using simple mechanisms and with minimal economic resources (Yingmo, 2019). Additionally, it is important to examine the types of cyber-attacks, their goals, the associated risks, and the principles and methods of protection. Among others, ransomware, man-in-the-middle (MITM), denial-of-service (DoS), cross-site scripting (XSS), and phishing attacks are common cybersecurity threats that can impact both computer and cyber-physical systems. To understand them better, Chobanov V. and Doychev I. (2022: 1-5) explained ransomware as a cyber-attack where attackers capture files and demand payment in exchange for encrypted data. Attackers can execute these attacks through various

methods such as malicious advertisements, spamming, social engineering, and compromised sites. Ransomware can affect both locally and remotely stored files or memory and cause memory infections that are not detectable by static or dynamic analysis of malware; on the other hand, **Man-in-the-middle (MITM)** attacks aim to steal personal information and login credentials by interfering with user and application communication. MITM attacks are prevalent in both computer systems and cyber-physical systems (CPS). However, MITM attacks are insufficient in CPS since CPS information sources are real-time dynamic systems. To prevent MITM attacks, communication between the user's device and the main server should be encrypted using an SSL service; **Denial-of-service (DoS)** attacks aim to shut down a machine or network by flooding the target with traffic, making it inaccessible to all users. Attackers can execute DoS attacks by sending information that could cause a crash. Linear structured system models for cyber-physical systems (CPSs) can be used to identify the conditions under which attacks may compromise the controllability of the system. During a DoS attack, attackers block access to a subnet, and a load balancer can be used to support the server until there is a large volume of requests that cannot be handled. A distributed denial-of-service (DDoS) attack is an extended form of this attack where many hosts send requests to the target server, with each host sending enough requests to crash the target. Moreover, **cross-site scripting (XSS)** attacks are a common threat that can have catastrophic impacts. Most web applications use JavaScript code to support dynamic client-side behavior. To prevent XSS attacks, it is recommended to develop an application that always checks the values submitted by the user before processing them; **phishing** attacks are a significant security threat that takes place in social engineering. Attackers use fake emails with links that contain false information and keywords similar to the name of the company the employees work for to extract the necessary information, usually credentials. Users must be careful before sending their credentials anywhere.

These types of attacks require, as reported, the use of different methodologies, prior knowledge of the identified targets and, above all, in-depth expertise. This is why stakeholders and all those involved must work together and share knowledge to develop sustainable solutions for energy systems in a context of many different risks. Building a solid foundation and achieving maximum project results in industry and science requires a two-way flow of information and best practices that can only be applied through cooperative best practices.

CRITICAL INFRASTRUCTURE PROTECTION

According to Vevera (2022), infrastructures are socio-technical systems that consist of facilities, distributed technical assets, organizations, and legislative and administrative frameworks for governance. They are critical because their destruction and disruption can result in significant human losses, material damage, and loss of confidence in authorities by citizens, partners, allies, investors, and other stakeholders. Competent authorities identify and designate critical infrastructures based on critical thresholds to concentrate security resources where they are most necessary (Gheorghe et al., 2018). Globalization has led to critical infrastructures aggregating into conglomerations that function at regional and global levels (Helbing, 2013). The digitalization of critical infrastructures has contributed to this trend, introducing new risks related to exposure to an increasingly dangerous cyber environment (Georgescu et al., 2020).

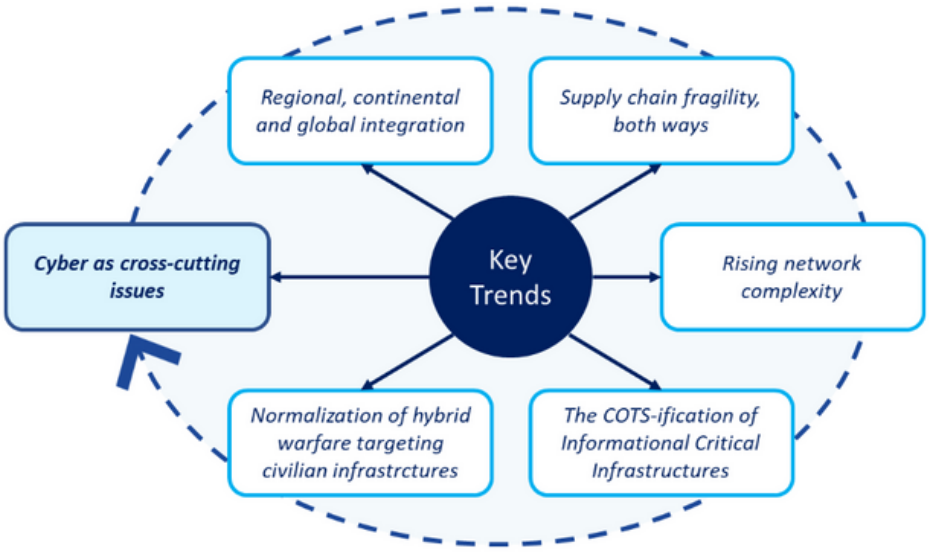

Figure 1. Key trends in the evolution of the Critical Infrastructure system-of-systems. *Source: author's elaboration based on data drawn from Vevera (2022).*

The Critical Infrastructure Protection (CIP) framework provides two concepts to understand how disruptions occur and spread through geographical space and sectoral boundaries. Firstly, the **interdependencies**, where infrastructures have bi-directional interrelationships that facilitate the transmission of a change in the state of one infrastructure to another. These interrelationships can lead to common-cause failures, escalating failures, and cascading disruptions. Secondly, **cascading disruptions**, where the fortuitous alignment of breakages can ensure the rapid transmission of disruptions throughout an entire system-of-systems, prolonging a crisis and amplifying damages beyond what could be predicted by decision-makers (Vevera, 2022).

The complexity of infrastructure systems leads to emergent behaviors and uncertainty in ascertaining system reactions to decisions and events. Vevera (2022) titles as parts of the "*Critical Infrastructure Protection Diplomacy*" *(CIPD)* system, practitioners who utilize specialized knowledge and engage in specific activities to counter the risks, vulnerabilities, and threats posed by the complex and emergent behaviors of the critical infrastructure (CI) system-of-systems. Sousa-Poza et al. (2008) describe this system as operating in a dynamic and challenging security environment, highlighting in Figure 1 (below) the main key trends on a systemic level.

As explained by Vevera (2022), the shown key trends represent the likely future evolution of critical infrastructures. **Ongoing regional, continental, and global integration** has resulted in the transborder interconnection of critical infrastructures, driven by the desire for greater efficiency and economies of scale. However, not all infrastructures are interconnected equally or at the same rate due to various factors such as differences in technology, regulation, or investment priorities. For example, regions may have varying levels of interconnectivity in their energy systems, with some having more developed transmission networks for efficient transfer of electricity across long distances, while others rely more on local generation. Additionally, differences in renewable energy infrastructure, such as wind or solar power, require more sophisticated energy storage and management systems. Recent events, such as the pandemic and the Ukraine crisis, have underscored the **fragility of supply chains** and how easily they can be destabilized by demand and supply

shocks. Moreover, **infrastructure networks are becoming more complex** due to the exponential increase in the number of possible interactions, which leads to the emergence of new behaviors, system ambiguity, and uncertainty. The trend of using "commercial off-the-shelf" hardware and software in critical infrastructure systems - the so-called **COTS-ification of informational critical infrastructures** by Georgescu (2018) - has resulted in an increased surface area of contact with the cyber environment, which poses significant challenges and threats. At the same time, civilian infrastructures have become principal targets of **hybrid warfare**, as they are critical to the functioning of society. Cyber-attacks, coupled with attribution issues and the importance of critical infrastructures, have led to the normalization of hybrid attacks against them, with multiple potential purposes. The ongoing digitalization of critical infrastructures has interconnected them across sectors and geographical regions through the **cyber domain**, exposing them to the global cyber environment.

These trends indicate an increase in exposure to various deliberate risks, including: the rise of hybrid warfare and the advantages of cyber-attacks; the effects of transnational organized crime, which can undermining public institutions and support terrorist groups, state proxies, or even state actors (Georgescu, 2018); the increasing presence of cyber in every critical infrastructure system, as evidenced by the convergence of European regulatory frameworks (Georgescu, 2018); the commodification of malware, which allows inexperienced attackers to cause significant damage to an unprepared victim organization; the innovative and dangerous rise of off-the-shelf commercial system components; the blurring of boundaries between physical and virtual infrastructure; the proliferation and diversification of threats, which surpass improvements in security culture and regulatory frameworks; the proliferation of cyber weapons and the competence of non-state actors in employing them for strategic, financial, or ideological reasons; the initial application of new technologies, such as blockchain and AI, which create new advantages but also risks; the divide between territorialized state agencies and institutions and cyberspace, which has no boundaries except for the physical infrastructure that supports it. The increasing exposure to deliberate cyber risks requires a cross-dimensional and multi-dimensional approach to cyber security, which goes beyond mere regulatory compliance and includes understanding the specific risks that organisations and institutions may face. Furthermore, it is important for organisations and institutions to invest in training and awareness-raising of their employees on cyber security so that everyone can contribute to mitigating the risks. Finally, organisations and institutions need to collaborate nationally and internationally to share information and best practices on cyber security and develop new solutions to protect their critical infrastructure from evolving cyber threats.

RISKS AND IMPLICATIONS

The energy sector is a critical infrastructure that relies heavily on information systems and technology to ensure efficient and reliable operations. However, this dependence also exposes the sector to various potential cybersecurity risks that could have severe consequences, including cyber, physical, geo-economic, and geopolitical risks.

Cybersecurity risk is a critical concern for the energy sector, particularly the renewable energy systems branch, which depends heavily on information systems and technology for efficient and reliable operations. Nonetheless, relying on this interdependence also makes the industry vulnerable to numerous cybersecurity threats that may have significant ramifications. These risks may include non-compliance with cybersecurity regulations, which could lead to legal liabilities and

financial losses. Security threats to employees and assets could result in physical safety risks and equipment damage. The actors involved in these risks could range from insiders to activists/hacktivists, criminal organizations, and hackers, who may execute cyber attacks to compromise the confidentiality, integrity, and availability of information systems. In the renewable energy systems branch, cyber risks may involve attacks targeting the control systems of wind turbines, solar panels, and other renewable energy devices, leading to disruptions in energy production or equipment damage. The energy sector's increasing reliance on digital technologies and interconnected systems has heightened the risk of cybersecurity breaches. The impacts are likely to be significant due to damage to critical infrastructures, resulting in risks to national cyber security, economic fallout, reputational damage, and significant disruptions to the functioning of the sector.

Geo-economic risks in the energy sector are significant and multifaceted, with potential implications for State, non-state actors, and private companies. State actors can engage in cyber activities to promote their national interests and gain a competitive advantage in the energy sector. For example, state-sponsored cyber attacks could affect critical infrastructure, such as oil refineries, gas pipelines, and power grids, to disrupt operations, and cause physical damage or steal sensitive data. Such attacks could have serious consequences for the companies concerned, with repercussions for the entire energy sector and the national economy. Non-state actors, such as hacktivists, could also pose a significant threat to the energy sector. They can target the sector to expose vulnerabilities or promote a particular agenda, as mentioned in relation to the Russian-Ukrainian conflict. These attacks could impact energy operations, cause significant damage to reputation, and even cause physical and economic damage. In addition, one of the most pressing risks is cybersecurity breaches, which could cause reputational damage, loss of consumer confidence, and possible impacts on industry financial performance and future investments. Private companies in the energy sector are particularly vulnerable to cyber risks and any cyber security breach could cause significant economic and reputational impacts, especially in the long run.

The potential for economic espionage, theft of intellectual property, and other cyber-related activities could contribute to international competition in the energy sector, with Geopolitical risks playing a significant role. Major geopolitical threats in the energy sector concern the potential impact of trade tensions, sanctions, and conflicts among different countries or regions. For instance, changes in trade policies, such as the imposition of tariffs on energy imports or exports, could impact the demand and supply of energy resources, leading to significant fluctuations in prices. Similarly, sanctions imposed by one country or group of countries on another may affect the energy sector by limiting access to key resources like oil or gas. In this context, it is very important for the private sector to consider cyber risk as part of geopolitical and geo-economic ones. This is the case of investments and capital allocation strategies in countries such as China, the United States of America, or - as demonstrated in current events - Russia, where the digital infrastructure of the financial sector has approached the splinternet phenomenon (or internet balkanization) following the removal of some Russian banking assets from the SWIFT system as part of Western war sanctions. Moreover, political instability or conflicts in energy-rich regions could also impact the supply and demand of energy resources, leading to price fluctuations, supply disruptions, and the weaponization of global supply chains. In support of these goals, cyber attacks often serve as a 'battle ram' for kinetic attacks, significantly weakening target infrastructures and facilitating the perpetuation of physical damage with regional conflict implications and geopolitical tensions.

Finally, physical risks in the energy sector encompass a range of potential threats to the physical safety of personnel and critical infrastructure, and there is a growing concern that cyber attacks could support or precede physical attacks. These risks could include physical attacks on critical infrastructure, insider threats, and external security events such as natural disasters or terrorist attacks. Physical attacks on critical infrastructure could involve the use of explosives, sabotage, or other destructive means to damage or destroy facilities, equipment, or systems. Such attacks could be supported by cyber-attacks that compromise the security of critical systems or provide reconnaissance information to attackers. Insider threats could include intentional acts of sabotage or negligence by employees or contractors, which could lead to the compromise of critical systems or data. Cyber-attacks may also support insider threats by providing access to sensitive data or compromising authentication mechanisms.

Considering these prospects, it is crucial for energy sector stakeholders to develop a comprehensive understanding of the challenges facing the sector and take proactive measures to mitigate them. This includes investing in cybersecurity measures to protect against potential cyber threats, diversifying energy sources and markets to reduce the impact of supply disruptions, and building resilient supply chains that are less vulnerable to geopolitical and cyber threats. Thus, constructing a comprehensive governance framework will require a joint effort to develop policies and regulation, aimed at a stable and secure energy market.

ENERGY GOVERNANCE CHALLENGES

As countries continue to develop new sources of energy and establish more extensive regional energy transport channels, new interdependence, and trade patterns are likely to emerge. However, the cybersecurity issue related to infrastructure has become a frontier issue in geopolitical research on energy transition. Studies by Qi et al. (2017), Dignum (2018), and Handke (2018) have shown that cybersecurity risks in energy infrastructure have attracted significant research attention.

Miao et al. (2020) have pointed out that the energy geopolitical game still exists in the new energy era, but its focus has shifted to the field of Global Energy Internet closely related to power use. The innovative application of information technologies, such as smart grids, energy storage technologies, and ultra-high-voltage electricity transmission, can effectively meet the demand for new energy power transmission flexibility, making it more intelligent, efficient, interconnected, and sustainable. However, this also makes the new energy grid more vulnerable to network attacks. Network attackers may try to disrupt the management and power distribution of the power grid, and interrupt and destroy industrial infrastructure.

On the other hand, in the absence of international norms, the development of digital technology in the energy field may bring security concerns. Most new energy equipment and power grid systems rely heavily on computers to manage the production, distribution, and output of new energy, prompting high requirements for cybersecurity. Facilities highly dependent on complex and large-scale power grids have high cybersecurity vulnerability risks and may suffer serious security impacts due to network attacks. The global energy network transmission will produce a short-board effect where countries with the weakest cybersecurity construction will easily become the target of attacks, which may even destroy the energy supply of all countries connected over the internet and thereby seriously aggravate geopolitical risks.

However, some scholars have pointed out that decentralized small-scale power generation can reduce cybersecurity risks. Studies by Liu *et al.* (2012) and Månsson (2015) have supported this claim. Scholten D. and Bosman R. (2016: 273-283)

have introduced the concept of "power grid community" believing that the grid can ensure community energy security and lay a foundation for regional peace and stability.

For decades, digital technologies have been contributing to the improvement of energy systems (IEA, 2017). Since the 1970s, the adoption of large IT systems to facilitate the management and operation of the grid has made energy companies true pioneers of digitalization. Today, electricity markets are monitored and controlled in real-time across vast geographical areas to offer services to a wide range of users. The astonishing progress in digitalization and its rapid spread throughout the energy sector raises the fundamental question of a new digital energy era, starting with applications already widely used in upstream activities. Technically recoverable oil and gas resources could be increased, thus increasing profits. In the total energy sector, the IEA (2017) estimates that digitalization could save around USD 80 billion per year, or about 5% of the total annual energy production costs, through monitoring and reducing unplanned interruptions, downtime, and prolonging the operational life of resources.

Furthermore, it is relevant to observe how digital systems can radically transform electricity markets. The greatest potential for transformation through digitalization is its ability to break down boundaries between energy sectors, increasing flexibility and enabling integration across entire systems. Electricity is at the center of this transformation, where digitalization is blurring the distinction between generation and consumption, and offering four interconnected opportunities (IEA, 2017):

- **"Smart demand response"**, increasing system flexibility, saving resources invested in new electrical infrastructure. In the residential sector alone, households and appliances could "plug in" to an interconnected electrical system, allowing devices to change the time they draw electricity from the grid, thus improving consumption efficiency and reducing costs for families.

- Integration of renewable energy into the grid, addressing demand fluctuations due to adverse weather conditions by the use of demand response programs and energy storage technologies. These can be used to store energy produced from renewable sources during peak production periods and then deploy it when energy demand is high.;

- Introduction of intelligent charging technologies for electric vehicles that would shift charging to periods when electricity demand is low and supply is abundant, providing further flexibility to the grid and saving on additional infrastructure costs; and finally,

- Development of distributed energy resources, such as home photovoltaic solar panels and storage, creating better incentives for producers, facilitating storage and sale of excess electricity on the grid: new tools such as blockchain could support the trade of electricity within local energy communities.

In the long term, this overview projects direct energy use for digital devices into a battle between growing data demand and continuous efficiency improvement (IEA, 2017). The use of digitally interconnected systems brings several benefits to the energy system, but also makes it more vulnerable to possible cyberattacks. If interruptions caused to energy systems by this threat were quite limited in the past, today attacks are increasingly frequent because they are cheap and easy to organize. Thus, the collaboration between public institutional actors and private actors, such as companies, corporations, and research centers, becomes a fundamental step in the energy governance framework.

The so-called "resilience" capacity at the systemic level depends precisely on the awareness that public and private actors have of vulnerabilities and related cyber risks. For this reason, international efforts in defense policies for energy infrastructure can help or support governments, companies, and organizations to build a margin of digital resilience (IEA, 2017), improving customary practices for reacting and preventing attacks, defense plans, and digital integration policies in the energy agenda.

At the same time, governance must also deal with privacy and data ownership, fundamental especially for consumers from whom this data is collected in detail. Intelligent devices, such as those mentioned earlier, can collect and aggregate data on family habits based on home energy demand, by time slot in relation to different devices. Despite the risk, monitoring aggregated and anonymized data allows for a better understanding of energy systems. The greatest benefit is in reducing costs for individual consumers. Together with concerns about privacy, digitalization also impacts employment models. In other words, the application of such technologies requires a variety of skills that inevitably translates into an increase in jobs in some sectors of the energy industry and a reduction in others.

Governance is therefore called upon to try to balance the mitigation of the negative impacts just described, as well as to promote innovation in response to the operational needs of public services. Similarly, if policy and market design are vital for a less risky digital transition, it is also true that the same transition is essential in response to the need for an energy transition. Digital technologies play a pivotal role in bolstering the sustainability agenda by facilitating the monitoring of greenhouse gas emissions and tracking instances of environmental pollution globally, regionally, and even locally. In addition, such technologies support decision-making processes by providing, for example, a detailed overview of consumption through online records, thus ensuring quick, targeted, and responsive responses even at the political level beyond the operational.

CONCLUSION

The strategic digitalization of energy systems plays an important role in the geoeconomics of energy transition, as stated by Diesen (2019) and Wigell (2016). This paper studied the geoeconomic and digital implications of new energy infrastructures and emerging technologies, paying attention to the advancement of energy systems digitalization. Additionally, this work addressed the state-of-the-art of cybersecurity evolution in the context of energy security, as well as geo-economic and digital risks in relation to the renewed attention to this issue.

The war in Ukraine and the rise in energy prices have led to a rethinking of national and international energy strategies and how to cope with a more fragmented global supply chain. The development of new technologies and infrastructures, such as the ones mentioned above, could involve security and cyber risks not to be underestimated. Moreover, the geopolitical and geoeconomic scenario requires a reflection on the development of globalization and the relationship between the digital transition and the social system. To fully understand how these interconnected forces shape our societies, economies, and global dynamics, we must undertake a deeper exploration of their implications and potential consequences. This calls for a comprehensive approach that takes into account the complex and multifaceted nature of these phenomena. Moving forward, it will be crucial to develop a comprehensive governance framework that can provide and maintain energy supplies while also safeguarding strategic interests from cyberattacks. This will require the construction of a robust capacity

framework that can ensure the security and reliability of energy infrastructure. At the same time, it will be necessary to build a cybersecurity perimeter that can protect against emerging threats and vulnerabilities.

Furthermore, the definition of digitalization cited above aligns with the future trends of net-zero energy system transition, which will evolve into a decentralized and interconnected network rather than isolated dots. Therefore, the interpretation of digitalization from the perspective of "interacting networks" holds more significance. Although digital development is taking place at exponential speed, the cyber strategy on energy infrastructures continues to cover little of the current developments in this field. In particular, the growth of renewable energy is happening simultaneously with the development of digitalization, which can help in balancing power grids, as renewable energy producers increase their activity and lower production based on weather conditions. Nevertheless, while some concerns might be exaggerated, there exist legitimate apprehensions regarding the vulnerability of utilities and grids to cyberattacks, orchestrated by terrorists or hostile nations. The notable case of a successful cyberattack on energy distribution companies in Ukraine back in 2015 serves as a poignant reminder, prompting the potential for such attacks to inflict significant damage on energy systems at a large scale.

The increased utilization of renewable energy and the resulting decentralization of energy systems have significant implications for cybersecurity. While decentralization can make the system more resilient to cyberattacks, it also presents new challenges and vulnerabilities that must be addressed. To address these challenges, it is crucial to implement a comprehensive cybersecurity governance framework for these new renewable energy plants, which is still an underdeveloped area. To ensure the security and reliability of energy infrastructure, it is crucial to establish a comprehensive cybersecurity governance framework. This framework should include several key aspects that work together to make the organization more resilient. One vital aspect is the development of strong governance structures that promote accountability, transparency, and effective decision-making. This involves clearly defining roles and responsibilities for cybersecurity management and regularly assessing cyber risks and vulnerabilities. Another critical aspect is the implementation of robust cybersecurity measures that are capable of protecting against emerging threats and vulnerabilities. This includes developing effective incident response plans and leveraging advanced technologies, such as artificial intelligence and machine learning to detect and respond to cyber threats. Moreover, it is essential to fully integrate the cybersecurity governance framework into the overall business strategy. By doing so, senior management can prioritize cybersecurity as a strategic imperative and allocate the necessary resources and capabilities to ensure long-term survival and growth, even in the face of adversity. Lastly, building a culture of cybersecurity awareness and training among all employees is crucial. This helps mitigate the risk of human error and ensures that staff are equipped with the necessary skills and knowledge to identify and respond to cyber threats. Discussions about the development of renewable energy and cybersecurity together can lead to important policy recommendations that consider the interdependencies between these two areas. However, it is important to recognize that predictions about the future energy system may be influenced by the social context in which they are made. Factors such as public perception, political will, and economic considerations can all play a role in shaping the direction of energy policy and the implementation of cybersecurity measures.

BIBLIOGRAPHY

Ashby, W. R. (1961). *An introduction to cybernetics*. Chapman & Hall Ltd, London.

Benedikt, M. (1991). *Cyberspace: first steps*. MIT Press, Cambridge.

Bertoli, E. (2022). *The potential of digital business models in the new energy economy*. https://www.iea.org/articles/the-potential-of-digitalbusiness-models-in-the-new-energy-economy. Accessed March 28, 2023.

Blackwill, D., & Harris, J. (2016). .*War by Other Means: Geoeconomics and Statecraft*. Cambridge, MA: Belknap Press.

Cao, L., Hu, P., Li, X. et al. (2023). 'Digital technologies for net-zero energy transition: a preliminary study'. *Carb Neutrality* 2, 7. https://doi.org/10.1007/s43979-023-00047-7

Chobanov V., Doychev, I. (2022). 'Cyber Security impact on energy systems'. 2022 *International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Ankara, Turkey, 2022: 1-5, doi: 10.1109/HORA55278.2022.9800102.

Dargahi, T., Dehghantanha, A., Bahrami, P.N. et al. (2019). 'A Cyber-Kill-Chain based taxonomy of crypto-ransomware features'. *J Comput Virol Hack Tech* 15, 277–305. https://doi.org/10.1007/s11416-019-00338-7

Diesen, G. (2019) 'The geoeconomics of Russia's greater Eurasia initiative'. *Asian Polit Policy* 11(4), 566–585. https://doi.org/10.1111/aspp.12497

Dignum, M. (2018). 'Connecting visions of a future renewable energy grid'. In: Scholten D eds. *The Geopolitics of Renewables, Lecture Notes in Energy*, Vol 61. Springer, Cham. https://doi.org/10.1007/978-3-319-67855-9_10

European Parliamentary Research Service. (2021). 'Key enabling technologies for Europe's technological sovereignty'. STUDY, Panel for the Future of Science and Technology. *EPRS | Scientific Foresight Unit (STOA)*. PE 697.184. ISBN 978-92-846-8666-7| doi: 10.2861/24482 | QA-01-21-349-EN-N. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697184/EPRS_STU(2021)697184_EN.pdf. Accessed March 17, 2023.

Geisberge, E., Broy, M. (2015). *Living in a networked world: Integrated research agenda Cyber- Physical Systems (agendaCPS)*. Herbert Utz Verlag GmbH, München

Georgescu, A. (2018). 'Pandora's Botnet – Cybercrime as a Persistent Systemic Threat. Future of Europe: Security and Privacy in Cyberspace'. *The VISIO Journal* 3, 1-8.

Georgescu, A., Vevera, V. & Cirnu, C. E. (2020). 'The Diplomacy of Systemic Governance in Cyberspace'. *International Journal of Cyber Diplomacy* 1(1), 79-88.

Goldthau, A., & Westphal, K. (2019). 'Why the Global Energy Transition Does Not Mean the End of the Petrostate'. *Global Policy* 10(2): 279-283. doi:10.1111/1758-5899.1264.

Gouvea, R., Kapelianis, D., Kassicieh, S. (2018). 'Assessing the nexus of sustainability and information & communications technology'. *Technol Forecast Soc Change* 130, 39–44. https://doi.org/10.1016/j.techfore.2017.07.023

Handke, S. (2018). *Renewables and the core of the energy union: How the pentalateral forum facilitates the energy transition in Western Europe. Lecture Notes in Energy*. Cham: Springer International Publishing.

Helbing, D. (2013). 'Globally networked risks and how to respond'. *Nature* 497, 51–59. DOI: 10.1038/nature12047

Hielscher, S., Sovacool, B.K. (2018). 'Contested smart and low-carbon energy futures: media discourses of smart meters in the United Kingdom'. *J. Cleaner Prod* 195, 978–990.

Hold, P., Erol, S., Reisinger, G. et al. (2017). 'Planning and evaluation of digital assistance systems'. *Procedia Manuf* 9, 143–150. https://doi.org/10.1016/j.promfg.2017.04.024.

Huang, Z., Hang, Y., Peng, Z. et al. (2017). 'Planning community energy system in the industry 4.0 era: achievements, challenges and a potential solution'. *Renewable Sustainable Energy Rev* 78, 710–721. https://doi.org/10.1016/j.rser.2017.04.004

International Energy Agency. (2017). *Digitalisation and Energy*, IEA, Paris.

Keating, C. B. & Katina, P. F. (2016). 'Complex system governance development: a first generation methodology' *International Journal of System of Systems Engineering* 7, 43–74.

Liu, J., Xiao, Y., Li, S. et al. (2012). 'Cyber security and privacy issues in smart grids'. *IEEE Communications Surveys & Tutorials* 14(4), 981–997.

Månsson, A. (2015). 'A resource curse for renewables? Conflict and cooperation in the renewable energy sector'. *Energy Research & Social Science* 10, 1–9.

Miao, Z. Q., Mao, J. K. (2020). 'A study on the geopolitics of energy in the era of electric power'. J*ournal of Global Energy Interconnection* 3(5), 518–525. (in Chinese).

National Institute of Science and Technology. (2018). 'Cyber-physical systems'. https://www.nist.gov/el/cyber-physical-system. Accessed May 28, 2023.

Qi, J., Hahn, A., Lu, X. et al. (2017). 'Cybersecurity for distributed energy resources and smart inverters'. *IET Cyber-Physical Systems: Theory & Applications*, 1(1), 28–39.

Reshmi, T. R. (2021). 'Information security breaches due to ransomware attacks – a systematic literature review'. *International Journal of Information Management Data Insights* 1(2), November 2021, 100013. https://doi.org/10.1016/j.jjimei.2021.100013

Scholl, E., Westphal, K., Yafimava, I. (2016). 'Overland, Energy security and the OSCE: the case for energy risk mitigation and connectivity' *SWP Berlin*, 2016. https://www.swp-berlin.org/fileadmin/contents/products/comments/2016C26_wep_et_al.pdf.

Scholten, D., Bosman, R. (2016). 'The geopolitics of renewables; exploring the political implications of renewable energy systems'. *Technological Forecasting and Social Change, Elsevier* 103(C), 273-283.

Sousa-Poza, A., Kovacic, S. & Keating, C. B. (2008). 'System of systems engineering: An emerging multidiscipline'. *International Journal of System-of-Systems Engineering* 1(1/2), 1–17.

Törngren, M., Bensalem, S., Cengarle, M.V. (2014). 'Cyber-physical European roadmap and strategy d5.1'. *CyPhERS project*. http://www.cyphers.eu/sites/default/files/D5.1.pdf. Accessed March 18, 2023.

Valeriano, B., Maness, R. C. (2018). 'How we stopped worrying about cyber doom and started collecting data'. *Politics Governance 6(2): Global Cybersecurity: New Directions in Theory and Methods* 6-49, https://doi.org/10.17645/pag.v6i2.1368.

Van de Graaf, T., Colgan, J.D. (2017). 'Russian gas games or well-oiled conflict? Energy security and the 2014 Ukraine crisis'. *Energy Res. Soc. Sci.* 24, 59–64. https://doi.org/10.1016/j.erss.2016.12.018.

Vevera, V. (2022). 'Critical Infrastructure Diplomacy – Tracing the Contours of a New Practice.' *International Journal of Cyber Diplomacy* 3: 41-49. https://doi.org/10.54852/ijcd.v3y202205.

Wigell, M. (2016) 'Conceptualizing regional powers' geoeconomic strategies: neo-imperialism, neo-mercantilism, hegemony and liberal institutionalism'. *Asia Eur J* 14, 135-151.

Yingmo, J., Kim-Kwang, R., Chooc, M., Liad, L., Chenab, C. (2019). 'Tradeoff gain and loss optimization against man-in-the-middle attacks based on game theoretic model'. *Future Generation Computer Systems* 101, 169-179. https://doi.org/10.1016/j.future.2019.05.078

Zetter, K. (2016). 'Inside the cunning, unprecedented hack of Ukraine's Power Grid'. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukrainespower-grid/. Accessed May 18, 2023.