Cybersecurity – A Permanent Challenge for the Energy Sector

Ioana-Elena ENE, Daniel SAVU
National Institute for Research and Development in Informatics - ICI Bucharest
ioana.ene@ici.ro, daniel.savu@ici.ro

Abstract: Energy security is a primary element in the development of any country. Reliable sources of energy are necessary to sustain industrial activity, power businesses and stimulate economic growth. As the energy sector develops, so does the number of cyber-attacks with significant impact on both energy production and the entire supply chain, which can paralyze the entire economic system, but above all, can destabilize national security. Mitigating all energy sector vulnerabilities is almost impossible. However, in the event of a cybersecurity incident, a series of measures can be implemented with the aim of reducing the risks and ensuring the continuity of operations. This article presents an overview of cyber-threats and vulnerabilities in the energy sector, describes risk management related to cybersecurity, technology solutions and the European Union policy and legislation on cybersecurity in this sector.

Keywords: Cybersecurity, Energy, Smart Grid, Digital Transformation, Smart Energy.

INTRODUCTION

There is no standard, universally accepted, definition of cybersecurity. In general, cybersecurity is defined as the adoption of measures to protect computer systems and their users against unauthorized access. Cybersecurity is ubiquitous especially in the energy field, a priority field for all companies and for all national and international actors, at any level.

Among all businesses, the impact of cyber-attacks in any of the elements of a power and utility plant is extremely dangerous. In the case of a cyber-attack, both related activities, energy supply, as well as public safety and the environment are threatened. Noting that threats and attacks on the energy sector and the number of actors involved have dramatically increased worldwide in recent years, the energy sector and governments have joined forces to take more effective measures to improve security for this sector.

Digitalisation has significantly transformed all areas of life in the 21st century, with the energy sector also benefiting from these changes. However, the new reality, where digital transformation has become such an important variable, brings with it threats related to cyber-attacks. Digital threats can cause various data breaches, which makes adopting cybersecurity measures mandatory. Thus, energy sector organizations need to implement access security precautions to prevent reputational loss and economic damage.

https://doi.org/10.54851/v5i1y202310

The cybersecurity of critical infrastructure, especially in the energy sector, is becoming increasingly important for the safety and security of energy production, distribution, transport and storage, as well as for the stability of the energy market. Information sharing and trust are key elements of cybersecurity.

The increase in cybersecurity incidents across energy systems imposes the need to protect against a variety of threats ranging from cyber-attacks, dynamic and evolving advanced persistent threats and privacy breaches to power disruption and serious human errors caused by lack of relevant training. The diverse threats targeting modern energy systems require new and holistic solutions that use cutting-edge technologies to detect and mitigate threats. Continuous assessment of the dynamic environment of energy systems ensures compliance with the latest cybersecurity standards and enables training of personnel involved in the energy system to respond appropriately to cybersecurity incidents and to mitigate human error.

OVERVIEW OF CYBER-ATTACKS IN THE ENERGY SECTOR

In recent years, cyber-attacks have become a serious threat to the industry, with hackers trying to penetrate energy systems to steal data and paralyze the flow of resources, sometimes to the point of shutting down. In the energy sector the critical infrastructure assets become more and more interconnected and their vulnerability to a cyber-attack increases, with large-scale consequences. The economy as a whole, along with all the other sectors, depends on the energy sector, which is why these attacks are spreading and can disrupt critical infrastructures in today's economies and functioning societies. Some of the main attacks are presented in this chapter.

All started in 2010. Stuxnet was the first virus designed to attack a single, very specific target: the computers that control the nuclear facility in Natanz (Iran). The virus destroyed nuclear centrifuges, spinning them over the allowed speed and temporarily halted the nation's nuclear program, taking it years to recover (Kushner, 2013).

Nowadays, in 2021, **Saudi Aramco**, a petroleum and gas company, faced a ransomware attack by hackers, which involved stolen passwords, wiped data and an attempt to extort a large amount of money ($50 million) from the producer (Ferguson, 2021).

Two major state-owned Brazilian electric utilities companies, **Centrais Eletricas Brasileiras (Eletrobras)** and **Companhia Paranaense de Energia (Copel)**, were hit by the DarkSide ransomware gang, who extracted 1,000 GB of data from COPEL's and Electrobras' systems in February 2021. The result was that both electricity providers were disconnected from National Interconnected System which helps to route electricity throughout the country (Delman, 2021).

The Norwegian energy company **Volue ASA** was the target of Ryuk ransomware in May 2021. Hackers were focused on the encryption of files, databases, and applications, the attack aiming at Volue infrastructure and networks, but no ransom was paid and the cybersecurity task force was able to mitigate any impact (Stupp, 2021).

On May 7th, 2021, **Colonial Pipeline, U.S.**, faced a ransomware attack by the DarkSide group, who attacked the company's billing system. This pipeline supplied about 45% of the gasoline and jet fuel on the East Coast of the United States. The entire pipeline had to be shut down, affecting the lives of millions of people, airports and airlines, causing shortages at gas stations, raise of gas prices, panic. A $4.4 million ransom was payed to the ransomware gang and partially recovered, but the company's brand image was seriously affected. The attack happened due to a low protection on multi-factor authentication, a basic cybersecurity tool against cyber hackers (Tsvetanov, 2021).

In August 2021, **Port of Houston, U.S.**, the biggest hub of commerce and energy in the Gulf of Mexico, successfully defended itself against an attempted cyber-attack which aimed to break into one of the port's web servers. The leak was a vulnerability in the password management. Had it not been detected in time, the Port's network would have been fully exposed to unrestricted access (Coble, 2021).

All records of cybersecurity incidents targeting oil and energy were beaten in 2022. Thirteen cybersecurity incidents in energy and commodities infrastructure have taken place in 2022 from a total of 45 since 2017, 2022 becoming the top year in terms of cyber-attacks over the last six years.

Due to the war in Ukraine, as the sanctions imposed by the West to Russia become stronger, cyber threats with Russian actors to energy assets increased. About 33% of all attacks since 2017 targeted mainly oil assets and infrastructure. The next vulnerable were electricity networks, with a percent of 25%, followed by gas and shipping with a moderate rate of cyberattacks. Almost 25% of the attacks since 2017 focused on commodities, energy and resources assets (Energy Security Sentinel, 2022).

In January 2022 the Colorado energy company **Delta-Montrose Electric Association (DMEA)** had to shut down 90% of its internal controls due to malicious cyber-ware that wiped 25 years of historical data. Its clients received multiple energy bills (Hope, 2021).

DESFA - the major Greek gas supplier, **Ignitis** - Lithuania's energy group and Energoatom - **Ukraine's** nuclear power company, were also victim companies of cyber-attacks during this period (Goud, 2022).

A cyber-attack targeting **Amsterdam-Rotterdam-Antwerp (ARA)**, the greatest European oil refining hubs, took place in February 2022 and has considerably affected the operations (loading cargoes) in the oil terminals, while the economic impact spread in cascade to all European countries. Eleven German sites were hit by attacks during the same time, leading to interruptions in the petrol supplies in northern Germany and creating a momentary continental energy crisis (World Economic Forum, 2022).

In July 2022, **Creos Luxembourg S.A.**, a company managing electricity and natural gas grids in Luxembourg, was attacked by the BlackCat, a ransomware gang. The group claimed to have stolen 150 GB containing an amount of 180,000 files (email accounts, contracts, agreements etc.) and released an extortion platform where they allowed access to stolen data so that the victims would pay the ransom (Din, 2022).

VMWare Horizon servers were attacked in August 2022 by Lazarus, a North Korean group, author of numerous cyber-attacks and cyber espionage. The hackers' goal was to get access to the networks of energy providers in the U.S., Canada and Japan. The group sent phishing emails to employees by which malware was launched to collect information from Windows systems and allowed the delivery of additional malicious code. Once into the system, the group used a custom malware family (YamaBot, VSingle, MagicRAT) to access and then steal data from devices. In the next step, by social engineering, victims were tricked into downloading infected applications on Windows or macOS operating systems so that the hackers could manage to access computers, propagate malware across their network and steal private keys (Ikeda, 2022).

In September 2022, the ransomware gang **BlackCat attacked Gestore dei Servizi Energetici SpA (GSE)**, an Italian energy provider. The company was forced to shut down all systems and website so that access to data was stopped. Around 700GB of files (contracts, accounting documents, reports, project information etc.) were stolen from the Italian energy agency's servers. In the same month, another security incident took place at **Eni SpA** – the Italian oil supplier (Ehc, 2022).

SMART ENERGY

In order to successfully conduct their operations within the energy system, companies involved in the field must implement the necessary policies, procedures and technologies dedicated to cybersecurity. In the energy operational environment there are five key concepts (Figure 1) that must be fully understood, as cybersecurity is based on these elements.

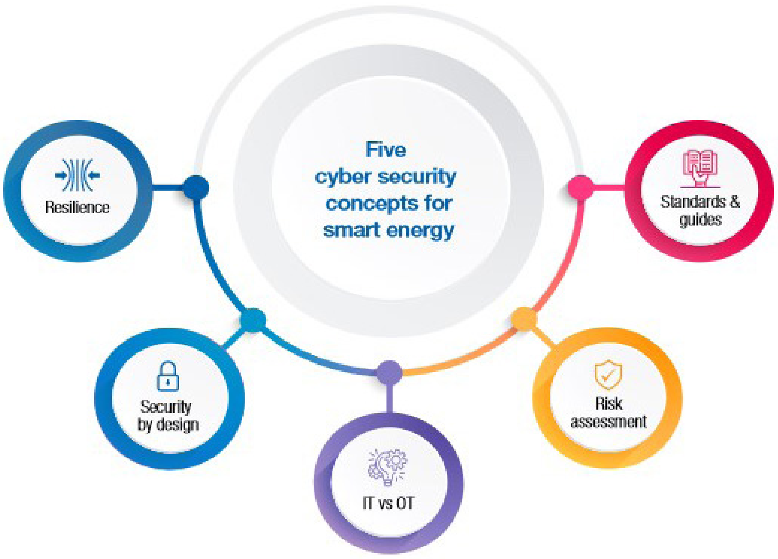

Figure 1. *Five cybersecurity concepts for smart energy (Source: IEC Technology Report 2022)*

The five key concepts are as follows (IEC, 2019):

- **Resilience.** The resilience of an organization can be defined as its ability to quickly recover or adapt to adverse situations or changes. Resilience must be the basis of the overall strategy to ensure the continuity of a business. To ensure resilience, organizations must focus on the safety, security and reliability of processes and service delivery. Necessary security measures must be implemented to mitigate impacts before incidents occur (identification and prevention), during incidents (detection and response) and after the incidents have been resolved (recovery).
- **Security by design.** It is an approach to software and hardware development that seeks to eliminate system vulnerabilities so that they become impervious to attack through measures such as continuous testing, authentication and compliance to best programming practices. Security is vital to all critical infrastructure and needs to be implemented into systems and operations from the outset. However, with legacy systems there may be security implementation issues, requiring the inclusion of security controls in all subsequent stages of system upgrades.
- **IT vs. OT.** There are both similarities and differences between information technology (IT) and operational technology (OT). Technologies in operational environments include a number of different security constraints and requirements than those in information technology environments. The main reason is that energy systems are cyber-physical systems and security incidents can cause both physical security incidents and power loss. Consequently, availability, authentication, authorization and data integrity in operational environments are typically more critical requirements than privacy. In terms of similarities, both IT and OT environments are increasingly relying on IoT technologies.
- **Risk assessment**. Assessing and mitigating risks and continuously updating processes are fundamental to improving security. Any organization must determine, based on business requirements, what security risks it is exposed to (human safety, physical, functional, environmental, financial, societal and reputational). Risk assessment allows the identification of vulnerabilities within systems and processes in the face of threats of any

type, estimates the probability of an incident and determines its potential impact. Organizations can take several approaches to assess risks - quantitative, qualitative, semi-quantitative, asset-based, vulnerability-based, or threat-based.

- **Standards & guides.** Cyber security standards and best practice guidelines for energy OT environments should be used to support the risk management process and establish security programs and policies. There is no need to rethink new ways of cybersecurity because there are already key cybersecurity standards and best practice guidelines for different areas and security purposes.

Cybersecurity planning must build on these standards and guidelines to improve resilience, security and interoperability within the energy system.

CYBERSECURITY VULNERABILITIES WITHIN THE ENERGY INDUSTRY

The energy sector is a preferential target both for the enemies of the states and for hackers looking for profit. According to the Cybersecurity Guide there are three basic characteristics that make energy companies vulnerable targets to cyber-attacks (Bowcut, 2021):

- utilities are usually dispersed on large areas, with large distances between geographic locations, which leads to a huge and almost impossible to control attack surface;
- there are complex relationships between utilities and third-party supply chains;
- in the companies in the energy sector (mainly the electric-power and gas ones) there are multiple connections between physical and cyber infrastructure; the result is the vulnerability to attack of the OT infrastructure and IT networks.

The energy sector consists of diverse and geographically-dispersed critical assets and systems. It is divided in four subsectors: electricity, oil and gas, including the generation, refining, storage and distribution of oil, gas and electric power, nuclear energy and alternative fuels. Geographically dispersed targets represent a multi-threat environment as they are difficult to protect.

Not only that the targets are dispersed, but the energy industry includes mixed (private and public) entities and vendor relationships with other companies which many times exceed the borders of a region, country or even continent. There is no organization (either private or governmental) able to protect all of the entities that form the energy sector.

The third layer of cybersecurity issues for the energy sector addresses the multiple connections between many of the components, which is specific to this industry. For example, a power failure or outage in one region can cause relative chaos if the availability of electricity in another part of the country is compromised. Also, a shortage in gas supply can cause an explosion in the gas prices nationwide.

Another deficiency in the fight against cyber-attacks is the lack of skilled cybersecurity workers. All energy companies and the government need well-trained cybersecurity professionals for the protection of critical infrastructure assets. Even if in 2022 4.7 million people worked as professionals in cybersecurity, there is still room for 3.4 million (Cybersecurity Workforce Study, 2022).

A WORD ABOUT CYBER VULNERABILITY OF NUCLEAR POWER PLANTS

Cybersecurity of nuclear energy is essential to national security. A cyber-attack on a nuclear power plant might endanger national security and have major risks which include political damage, loss of public confidence, coercion of interests, environmental and economic damage and casualties. Therefore, it is essential that nuclear facilities improve their digital infrastructure to prevent these damaging impacts.

The threat of cyber-attacks grows as global nuclear energy grows. In power plants, digital systems replaced early analogue systems which led to the evolution of process control systems. Standardized hardware and software in Supervisory Control and Data Acquisition (SCADA) systems took the place of highly specialized hardware and software systems. But everything comes with a price. The transition to digital systems adds new risks and vulnerability to new interconnects of system components, potential operational issues and vulnerabilities from cyber-attack that must be assessed and addressed.

In order to assess system vulnerabilities, four main categories of digital computer and communication systems must be considered (Pickering & Davies, 2021):

- safety-related and important-to-safety functions;
- security functions;
- emergency preparedness functions;
- support systems and equipment important to safety and security.

Together, these four elements provide a framework for designing and implementing cybersecurity plans for nuclear power plants.

TYPES OF ATTACKS IN THE ENERGY SECTOR

Threat categories in the energy sector are presented below (Blueprint Energy Solutions GmbH, 2019):

- **Malware** (malicious software) refers to any type of software designed specifically to affect a computer, being installed on it without the consent of the computer's owner. Malware can steal personal information, slow down the computer, steal passwords, stop a computer from working and even send fake emails. There are many types of malware such as computer viruses, Trojan horses etc.
- **Web Based Attacks / Web application attacks** are any threats that use the Web to facilitate cybercrime. Web applications can be vulnerable to attacks, which can allow cyber criminals to gain access to data and other sensitive information, helping infected PCs to be absorbed into botnets or to gain access to internal systems through web interface. According to Verizon's Data Breach Investigations Report (DBIR), elaborated in 2022, over 60% of the 18,000 security incidents reported to the team were associated with hacks of basic web applications.
- **Social engineering / Phishing / Spam** **Social engineering**, in the context of information security, is a form of psychological manipulation of people in which attackers impersonate a trusted source in order to convince them to perform certain tasks, such as granting access to a computer or account or revealing confidential information. Phishing and spam are the threat tools most often used in such schemes.
- **Denial of Service (DoS)** attack is a cyber-attack meant to temporarily or indefinitely shut down a machine or network, making it inaccessible to its intended users. Attackers flood the victim's system with requests for services or traffic to overload the network /computer and hinder or even stop the network/computer's ability to handle legitimate requests. The DoS attack results in the target's website being inaccessible or in poor network performance.
- **Insider Threat** represents a threat to an organization that originates from individuals within the organization, such as current or former employees, contractors, or business associates, who have inside information about the organization's security practices, data and IT systems. The threat can materialize through fraud, theft of confidential or commercially valuable information, theft of intellectual property or sabotage of IT systems. These people can be:
  - malicious insiders (insiders who take advantage of their access rights to harm their organization);
  - careless insiders (people who make mistakes or ignore company policies putting the company at risk);
  - infiltrators (external actors who obtain legitimate access credentials without, however, having the necessary authorization).
- **Cyber Espionage** or **Cyberwar** is the act or practice by which an unauthorized

user steals data and information from individuals or entities, for personal, economic, political or military advantage, using individual networks / computers and Internet. For this purpose, attackers can use a lot of techniques including malware dissemination, social engineering, phishing, Trojan horses, spyware.

- **Botnet** is a network of computers or Internet-connected devices running bots under someone's control. Each of these devices has been infected with malware that allows the attacker to control them remotely. Thus, botnets can be used to perform distributed denial-of-service attacks (DDoS attacks), steal data, and send spam messages, allowing the attacker to access the device and its connection.
- **Ransomware** is a type of malware that threatens a victim, destroying or blocking their access to critical data or systems until a ransom is paid. It spreads through email attachments, infected programs and compromised websites. Ransomware is usually delivered via phishing emails or drive-by downloads, tricking the victim into clicking on a malicious link or opening an attachment. Thus, without the consent of the users and without them being informed, a drive-by download type program will be automatically downloaded from the Internet. Once downloaded it will run malicious code without any user interaction. After the malicious code is executed, the user's computer is infected with ransomware.

RISK MANAGEMENT RELATED TO CYBERSECURITY: SOLUTIONS

In the past few years, the companies in the energy sector were victims of numerous cyber-attacks that could be avoided if dedicated measures would have been taken. The most frequent five cyber threats were the following (Avertium, 2022):

- supply chain attacks;
- poor and not highly secured integration of systems;
- ransomware and incident response;
- Identity and Access Management (IAM) inefficiencies;
- mobile device phishing.

Threats targeting ICS (Industrial Control Systems) and third-party facilities are some of the most significant cybersecurity threats in the energy sector. Any losses and blockages can cause huge damage to whole communities and even at the national level. For cyber-attacks to be successfully countered, cybersecurity best practices must be implemented within the energy sector (Hetz, 2021):

- **Securing the stages of the supply chain.** The existence of a large number of vendors offering a multitude of products can be a problem because attackers can always speculate on the smallest weakness in a product that can cause a security breach. Thus, in a report published in mid-2021 by The Cybersecurity and Infrastructure Security Agency, more than 600 flaws were identified in the industrial control systems (ICS) offered by 76 vendors, compared to only 449 identified in the second half of the year 2020.
- **Cyber risk assessment at every level.** The implementation of effective ways to ensure cybersecurity is a factor of protection, training and allows risk assessment. Since trusted employees and suppliers can be the target of cyber-attacks, they must be effectively trained to prevent these attacks. The processes by which companies are interconnected must be reviewed in order to detect flaws that can affect systems and expose them to security hazards.
- **Providing awareness training on the need to ensure cybersecurity and risk reporting.** Because of its importance, cybersecurity in the energy sector is a responsibility for everyone involved, not just security teams. A first step is the awareness of the effects and implications of the successful operation of cybersecurity systems within the sector, especially by employees in high-risk fields (IT and OT).

- **Deploy cybersecurity risks monitoring solution.** Ensuring cybersecurity in the energy sector requires the implementation of monitoring solutions that work around the clock to provide real-time alerts of incidents or failures. Early detection helps reduce the negative effects on the functionality of operations within the sector, reduce financial losses and ensures the rapid restart of operations. An example is that of AmeriGas, which, using continuous monitoring, was able to detect and block a recent data breach attempt in a record time of only eight seconds.
- **Protection of operational technology networks.** As energy sector cybersecurity is an intersection between IT and OT, effective prevention methods must be implemented that span both. Thus, a series of measures are needed to ensure the separation of high-risk processes from the usual ones, the updating of IT systems, the monitoring of security fixes and the creation of redundant systems that allow rapid recovery. In addition, in the event that one of the business partners is the victim of a cyber-attack, alternative suppliers must be identified so that the supply chain is not interrupted.

CYBERSECURITY TECHNOLOGY SOLUTIONS FOR THE ENERGY INDUSTRY

The modern energy industry can face a multitude of security issues stemming from the critical nature of networks, systems and equipment. As a result, well-developed strategies are needed to underpin the use of high-performance cybersecurity solutions. Some of these solutions are presented below (Bowcut, 2021).

Virtual Dispersive Networking (VDN) is a technology which divides a message into several parts that will be encrypted separately and then routed to multiple servers, computers and even smartphones, thus avoiding potential bottlenecks. Data packets are sent along different routes by means of protocols. Transmitting data via different routes minimizes the effects of a Man-in-the-Middle attack, as hackers can only obtain an insignificant part of the transmitted data. Thus, the data is almost impossible to decrypt and only makes sense to its recipient.

Hardware authentication refers to a security system that uses a hardware device to grant access to users. Hardware authentication is particularly useful in geographically dispersed OT (operational technology) networks. Based on this strategy, access to computer resources is achieved through a dedicated physical device, for example a token, and a primary password held by an authorized user.

User-behaviour analytics (UBA) is a cybersecurity process through which the users of a system are tracked for the purpose of detecting threats, targeted attacks and financial fraud. Thus, information is collected about network events typically generated by network users. In other words, UBA examines the activities of a user, thus allowing the identification of any unacceptable or potentially dangerous behavior. Using machine learning techniques, UBA can gradually increase its accuracy as it better understands the intentions behind a user's behaviour.

Smart Grid (SG) is a combination of a power grid and a communication network; security attacks may take place in both the physical space, as in the conventional power grid and cyber space as in any communication network. The most commonly occurring attacks in SG are false data injection, denial of service, distributed denial of service and global positioning system spoofing attacks (Mazhar et. al., 2023).

In modern SGs ruled by advanced computing and networking technologies, Artificial Intelligence (AI) has the potential to influence the future design and implementation of cybersecurity systems for the power grid (Macwan & King, 2021). These systems may enhance the overall operation of the power system by leveraging and making sense of massive amounts of data.

Machine Learning (ML) is one of the leading artificial intelligence technologies capable of detecting, identifying, and responding by mitigating adversary attacks in SGs (Berghout et al., 2022). Because the conventional computational techniques do not have the sufficient ability to process the vast amount of data introduced by smart grid systems, AI techniques have received much attention. Many of the research efforts were put into studying these AI techniques to address the challenges, because they use large-scale data to further improve smart grid performance.

The AI techniques in the smart grid can generally be classified into the following areas (Omitaomu & Niu, 2021):

- expert systems: a human expert in loop technique used for certain problems;
- supervised learning: an AI paradigm in which the mapping of inputs and outputs has been studied to predict the outputs of new inputs;
- unsupervised learning: a machine learning (ML) class in which the unlabelled data are used to capture the similarity and difference in the data;
- reinforcement learning (RL): differs from supervised and unsupervised learning due to its intelligent agents' strategy, which aims to maximize the notion of cumulative reward;
- ensemble methods: combine the results from several AI algorithms to overcome the limitations of one algorithm with better overall performance.

The main Artificial Intelligence techniques in SGs are (Omitaomu & Niu, 2021):

- Research Methodology;
- Load Forecasting;
- Power Grid Stability Assessment (Transient Stability Assessment, Frequency Stability Assessment, Small Signal Stability Assessment, Voltage Stability Assessment);
- Faults Detection;
- Smart Grid Security.

EUROPEAN UNION POLICY AND LEGISLATION ON CYBERSECURITY IN THE POWER SECTOR

- **European Programme for Critical Infrastructure Protection - EPCIP (2006).** EPCIP was adopted by the European Commission in response to the request of the European Council to develop a comprehensive strategy and action plan to improve the protection of critical infrastructure of all EU member states as well as important economic sectors. Threats addressed include terrorism, criminal activities and natural disasters.
- **Council Directive 2008/114 - Identification and designation of European critical infrastructures and the assessment of the need to improve their protection.** While embracing an all-hazards approach, its scope is limited to the sectors energy and transport. Owners or operators of critical infrastructure are required to prepare advanced business continuity plans and appoint Security Liaison Officers who will act as points of contact with the national authority responsible for the protection of critical infrastructure. In February 2013, the Commission issued a cybersecurity strategy that outlined the EU's vision for building cybersecurity capabilities. In June 2019, the Commission published an evaluation of the Critical Infrastructure Directive (2008) which found that, given the new challenges related to technological, economic, social, political and environmental developments, the directive is no longer sufficiently relevant. It was concluded that the directive was only partially effective, failing to establish a common approach to the assessment of critical infrastructure protection measures. Options identified for a future revision of the directive include a more systems-focused approach and better alignment with relevant EU legislation.

- **Directive (Eu) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.** The directive sets out the rules that form the basis of the current EU cybersecurity regime. Thus, a unitary system for increasing the security level of networks and IT systems that support the provision of essential services and digital services of the greatest importance has been established throughout the European Union. The directive required the designation of competent national authorities, the creation of IT security incident response teams and the adoption of national cybersecurity strategies. Essential service providers and digital service providers were required to adopt appropriate security measures and notify relevant national authorities of serious incidents.
- **The European Cybersecurity Act (Regulation (EU) 2019/881) became active in June 2019.** The regulation aims to strengthen the EU's response to cyber-attacks, improve cyber-resilience and increase trust in the digital single market. The Act addresses the issue of legacy infrastructure, older technology with a lifespan of 30-60 years, designed before cybersecurity concerns existed. The regulation has two functions:
- granting a permanent mandate to ENISA (the European Union Agency for Cybersecurity);
- setting out a framework for European Cybersecurity Certificates; ICT products, services and processes are certified according to various criteria, with predefined security levels being ‚low', ‚medium' and ‚high'.
- **Commission Recommendation on energy cybersecurity - Recommendation (EU) 2019/553**, promulgated by the Commission in April 2019, contains guidelines that Member States and key stakeholders (especially energy network operators) must take them into account when making infrastructure decisions. Guidance is provided on how to address challenges specific to the energy sector, identifying the main actions needed to defend cybersecurity. Measures include the analysis and identification of security risks, particularly with respect to legacy systems, updating software and hardware, and establishing a capability to automatically monitor security events.
- **Security of Gas Supply Regulation - Regulation (EU) 2017/1938** on measures to safeguard security of gas supply serves to strengthen the internal market for natural gas and to provide measures for the event of a supply crisis. It defines the responsibilities and duties of companies, national authorities and the EU Commission. The regulation considers interruptions in natural gas supplies caused by a number of risk factors, including cyber-attacks, war, acts of terrorism and sabotage. The regulation establishes rules for regional risk assessment and emergency planning and introduces a mechanism for mutual assistance in the event of a severe gas supply crisis, based on the principle of solidarity.
- **Electricity Risk Preparedness Regulation: Regulation (EU) 2019/941** specifically addresses the prevention and management of crises in the electricity sector. The development of common methods and rules for assessing risks to the security of electricity supply, including those related to cyber-attacks and crisis management, as well as the creation of a common framework for improving the assessment and monitoring of the security of electricity supply are envisaged. As an ongoing development, the **Network code on cybersecurity** aims to establish a European standard on the cybersecurity of cross-border electricity flows. It includes rules on cyber risk assessment, common minimum requirements, cybersecurity certification of products and services, monitoring, reporting and crisis

management. The code provides a clear definition of the roles and responsibilities of the various stakeholders (ENTSO-E and DSO Entity, 2022).

MAJOR TRENDS

Due to the fact that attack surfaces are continuously growing, offensive cyber capabilities have increased and there are deficiencies in international cooperation, protection against these cyber threats is increasingly difficult.

The following trends can be observed (Wilson & all., 2021):

- the expansion of the landscape of digital threats due to the convergence between IT and OT requires increasing the connectivity of critical infrastructure and the rapid adoption of emerging technologies that allow accelerating the transformation of the business model;
- attacks on the supply chain are more and more numerous and sophisticated, which requires the need to increase the security level of the interactions between the operating environment in the energy sector and the external environments of partners and suppliers;
- the increase in the number of cyber-attacks in the industry represents a disruptive factor not only for business operations, but also for public safety in general.

The power industry should act now to ensure that the disruptive effects of future cyber-attacks will be as reduced as possible. Consequently, five technical priorities for the power sector security should be considered:

- strong power sector migration to the cloud;
- merging of data protection, governance and privacy;
- better collaboration to secure Operational Technologies (OT);
- access management (IAM/PAM) success factors;
- evolving requirements for Managed Security Services.

CONCLUSIONS

The energy sector cyberthreats landscape evolves and expands rapidly, the attacks becoming more frequent, the actors more varied and the tools increasingly sophisticated especially since digitalisation era started. The vulnerabilities of the power sector – dispersed geographic locations, complex relationships between utilities and third-party supply chains, specific multiple connections between physical and cyber infrastructure – make power companies some of the most frequently attacked targets, increasingly by nation-state actors aiming for disruption and even destruction.

The first step companies can take to address cyber risk is to identify and map critical assets across the extended enterprise and building a secure, vigilant and resilient framework. The second step consists in collaboration with peers, governments, suppliers and other sectors in order to share intelligence, develop new standards and adopt new technologies. Augmented reality, artificial intelligence, drones and others increase in their utility through technological advances. Using modern tools, companies have the capability to monitor networks in real time, discover threats and address them rapidly, significantly reducing risk both for them and for the society in general.

REFERENCE LIST

Avertium. (2022) *The top 5 cyber threats in the energy sector.* Available at: https://www.avertium.com/resources/threat-reports/top-5-cyber-threats-in-energy-sector [Accessed 15 February 2023].

Berghout, T., Benbouzid, M., & Muyeen, S.M. (2022) Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. I*nternational Journal of Critical Infrastructure Protection.* 38: 100547. doi: 10.1016/j.ijcip.2022.100547.

Blueprint Energy Solutions GmbH. (2019) *Final Report - Study on cybersecurity in the energy sector of the Energy Community.* Document no.: FINR-CS-EC-121019.

Bowcut, S. (2021) Cybersecurity in the energy industry. *Cybersecurity Guide*. Available at: https://cybersecurityguide.org/industries/energy/ [Accessed 24 February 2023].

Coble, S. (2021) Port of Houston Quells Cyber-Attack. *Infosecurity Magazine*.

Cybersecurity Workforce Study. (2022) Available at: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx. [Accessed 3 March 2023].

Delman, M. (2021) Microsoft Patches Windows Zero-Day; Brazilian utilities hit by ransomware. *Morphisec*.

Din, A. (2022) BlackCat Ransomware Says It's Behind the Attack on Creos Luxembourg S.A. Available at: https://heimdalsecurity.com/blog/blackcat-ransomware-says-its-behind-the-attack-on-creos-luxembourg-s-a/ [Accessed 7 March 2023].

EC. (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union L 345/75.*

EU. (2006) Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection (COM (2006) 786 final). *Official Journal of the European Union C 126.*

EU. (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union L 194/1.*

EU. (2017) Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010. *Official Journal of the European Union L 280/1.*

EU. (2019a) Commission Recommendation (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector (notified under document C (2019) 2400). *Official Journal of the European Union L 96/50.*

EU. (2019b) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union L 151/15.*

EU. (2019c) Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC. *Official Journal of the European Union L 158/1.*

Ehc, T. (2022) BlackCat ransomware: We attacked Gestore dei Servizi Energetici SpA, *SecNews.* https://en.secnews.gr/418897/blackcat-ransomware-epitethikame-stin-gestore-dei-servizi-energetici-spa/ [Accessed 3 March 2023].

Energy Security Sentinel. (2022) *An interactive study of geopolitical risk and energy prices.* https://www.spglobal.com/commodityinsights/PlattsContent/_assets/_files/en/specialreports/oil/oil-security-sentinel.html [Accessed 10 March 2023].

Ferguson, S. (2021) *Saudi Aramco Traces Data Leak to Attack on Supplier.* https://www.bankinfosecurity.com/saudi-aramco-says-supplier-leaked-company-data-a-17130 [Accessed 11 March 2023].

Goud, N. (2022) Russia launched DDoS attack on Ukraine Nuclear Plant. *Cybersecurity Insiders.*

Hetz, M. (2021) *Managing cybersecurity risks in the power sector.* https://www.ge.com/gas-power/resources/articles/2021/managing-cybersecurity-risks-in-power-sector [Accessed 17 February 2023].

Hope, A. (2021) Colorado Energy Company Suffered a Cyber Attack Destroying 25 Years of Data and Shut Down Internal Controls. *CPO Magazine.*

IEC. (2019) Technology Report: Cybersecurity and resilience guidelines for the smart energy operational environment, *IEC - International Electrotechnical Commission.* https://www.iec.ch/basecamp/cyber-security-and-resilience-guidelines-smart-energy-operational-environment [Accessed 28 February 2023].

Ikeda, S. (2022) Lazarus Hackers for Cyber Espionage; Targets Are Energy Companies Running VMware Horizon Servers, *CPO Magazine.*

Kushner, D. (2013) The real story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program. *IEEE Spectrum.*

Macwan, R., & King, R. (2021) Artificial Intelligence for Energy Systems Cybersecurity. *Conference: Artificial Intelligence for Energy Systems Cybersecurity.*

Mazhar, T., Irfan, H., M., Khan, S., Haq, I., Ullah, I., Iqbal, M.& Hamam, H. (2023) Analysis of Cybersecurity Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods. *Future Internet.* 15.

Omitaomu, O., A. & Niu, H. (2021) Artificial Intelligence Techniques in Smart Grid: A Survey. *Smart Cities.* 4(2), 548-568.

Pickering, S., Y. & Davies, P., B. (2021) Cybersecurity of Nuclear Power Plants: US and Global Perspectives. *Georgetown Journal of International Affairs.*

Stupp, C. (2021) Energy Tech Firm Hit in Ransomware Attack. *World Street Journal Pro Cybersecurity.*

Tsvetanov, T. (2021) The effect of the Colonial Pipeline shutdown on gasoline prices, Elsevier. *Economic Letters.* 209.

Wilson, R. van Tiel, B., Knott, J., & van Hoof, J. (2021) *PwC power sector cybersecurity trends and insights for 2021.* https://www.pwc.com/gx/en/issues/cybersecurity/power-sector-cybersecurity.pdf. [Accessed 17 February 2023].

World Economic Forum. (2022) *Why the energy sector's latest cyberattack in Europe matters.* https://www.weforum.org/agenda/2022/02/cyberattack-amsterdam-rotterdam-antwerp-energy-sector/ [Accessed 10 March 2023].