Internal Security Review

2025, no. 32, pp. 345–364

https://doi.org/10.4467/20801335PBW.25.017.22183

ARTICLE

Cybersecurity in the offshore and coastal energy sector of the Republic of Poland

DAVID CYBULSKI

Independent author

https://orcid.org/0009-0003-9195-4407

Abstract

The purpose of the article is to discuss the level of cybersecurity of Poland's offshore and coastal energy sector in the context of planned strategic energy projects. The author presented selected cyberattacks on elements of other states' energy sector, he also discussed, among other things, on the basis of *Energy Policy of Poland until 2040*, Poland's planned activities related to energy infrastructure in the Baltic Sea region. He identified threats to Poland's offshore and coastal energy sector, which include: the activities of APT groups and state-sponsored groups, business rivals and hacktivists. He presented the methods used to protect this infrastructure as well as proposals for securing planned investments against ICT attacks.

Keywords

cybersecurity, cyberattacks, APT groups, energetics, energy sector

Introduction

With the ever-increasing digitalisation in society, it is essential to continuously develop existing electricity generation capacity. Decision-makers, aware of the need to modernise the state's existing energy infrastructure, to comply with EU regulations[1] and the expected increase in the country's demand for electricity, took steps to define strategic goals and projects for the energy sector in the long term. This led to the creation of a plan for the development of the Polish state's energy sector, the *Energy Policy of Poland until 2040* (hereinafter: PEP2040).

Offensive actions in the Baltic Sea against projects such as Nord Stream 1 and Nord Stream 2[2], undersea C-Lion 1 telecommunication cable or Estlink 2 power connection show how the security of energy infrastructure is under threat these days[3]. The pursuit of national energy projects in the northern Poland and in its exclusive economic zone increases the degree of computerisation of the energy sector's resources. This enhances the enemy's ability to impact the ICT infrastructure of the Polish energetics. Therefore, it is necessary to review the current state of cybersecurity of Poland's developing offshore and coastal energy sector, as well an answer to the question to what extent it is resilient to threats.

One of the ways in which criminals, including terrorists, and international legal entities (states) exert influence is through their direct or indirect impact on the energy sector of the other party, known as the high-value target. An attack, including ICT, that leads to the cessation of the production and distribution of a specific energy demand may result in the temporary or permanent inability of the state to function. In order to mitigate the risk, the Polish legislator decided, on the basis of Article 3 point 2 letter (a) of the *Act of 26 April 2007 on crisis management*, to classify energy supply systems, energy raw materials and fuels as critical infrastructure (CI). The Act on crisis management imposes certain obligations on CI operators to ensure its proper protection. Additionally, under the *Act of 5 July 2018 on the National Cybersecurity System*[4], CI operators have been

[1] *Polityka energetyczna Polski do 2040 r.* (Eng. Energy Policy of Poland until 2040), Ministry of Climate and Environment, Warszawa 2021, pp. 3–4.

[2] W. Lorenz, S. Zaręba, *Konsekwencje eksplozji rurociągów Nord Stream 1 i 2* (Eng. Consequences of the explosion of the Nord Stream 1 and 2 pipelines), Polski Instytut Spraw Międzynarodowych, 29 IX 2022, https://pism.pl/publikacje/konsekwencje-eksplozji-rurociagow-nord-stream-1-i-2 [accessed: 16 VII 2025].

[3] K. Buchholz, *Baltic Sea Cable Incidents Pile Up*, Statista, 6 II 2025, https://www.statista.com/chart/33892/damage-to-underwater-cables-and-pipelines-in-the-baltic-sea/ [accessed: 16 VII 2025].

[4] An amendment to this act is currently being processed. See: *Draft law amending the Act on the National Cybersecurity System and certain other acts*, no. UC32, https://www.gov.pl/web/premier/

obliged to ensure an adequate level of cybersecurity within their entities in order to minimise the risk of an ICT security incident.

The purpose of this article is to discuss the level of ICT security in the offshore and coastal energy sector of the RP in the context of planned strategic energy projects. It presents selected cyberattacks on elements of the energy sector in other countries and discusses, among other things, on the basis of the *Energy Policy of Poland until 2040*, Poland's planned actions related to energy infrastructure in the Baltic Sea region. The threats to the Polish offshore and maritime energy sector were identified, including the activities of APT groups[5] and state-sponsored groups, business rivals, hacktivists. The methods used to protect this infrastructure as well as proposals for securing planned investments against ICT attacks were also presented.

Examples of cyberattacks targeting the energy sector

The energy infrastructure of the states during the first two decades of the 21st century has been the victim of many successful attacks targeting, among other things, ICT systems and networks. The first well-known cyber offensive of this type was an attack carried out in 2010 against the ICT infrastructure of the uranium enrichment centre in the city of Natanz, Iran, using Stuxnet software. The facility was designed for electricity production and to meet Iran's strategic interests in acquiring its own nuclear deterrent capability. The operation, code-named 'Olimpic Games', was carried out in cooperation by, among others, the United States of America and the State of Israel[6]. Since it was not possible to carry out an attack or sabotage the facility by kinetic means, it was decided to launch a cyberattack instead. Potential weak points in the facility's ICT infrastructure were identified, which, if successfully targeted, would prevent or significantly hinder the continuation of the uranium enrichment process in Natanz. The most destructive method of harming Iran's nuclear strategy was considered to be destruction of the uranium enrichment

projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw3 [accessed: 16 VII 2025].

[5] APT (advanced persisted threat) group – a type of advanced cybercriminal group consisting of skilled cybersecurity and ICT specialists who are capable of carrying out advanced ICT attacks on specific entities.

[6] M. Baezner, P. Robin, *Hotspot Analysis: Stuxnet*, Zurych 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf, pp. 7–8 [accessed: 16 VII 2025].

centrifuges[7]. Since the facility did not have direct access to the internet, the attackers decided to infect the internal ICT systems by connecting a USB flash drive with software. The infected centrifuges (more precisely, the programmable logic drivers that controlled them), began to work according to a schedule set by the attackers. Approx. 11–17% of centrifuges at the centre in Natanz were damaged[8], which led to a 15% decrease in nuclear fuel production[9]. In addition, it is suspected that approx. 100 000 other devices were unintentionally infected when the Stuxnet virus unexpectedly began to spread worldwide via the internet[10]. It remains arguably the most well-known case of an attack on ICT system carried out against another country and its energy infrastructure.

Another example of operations in cyberspace targeting elements of a country's energy sector was the 2012 attack on the Kingdom of Saudi Arabia's state-owned company, Saudi Aramco Oil Company (hereinafter: Saudi Aramco), which is the largest resource company in the world. According to calculations by the European Central Bank from 2011, Saudi Arabia was responsible for about 12% of global oil production up to 2009 (with the majority of extraction carried out by Saudi Aramco)[11]. The attack on Saudi Aramco was most likely carried out by cybercriminal group APT33, linked to the Islamic Republic of Iran[12]. The paralysis of the company's ICT systems was carried out using the Shamoon virus. More than 30 000 workstations were infected. This programme spread to other workstations (a behaviour typical of malicious software classified as a worm) and overwrote files in the device's operating system, rendering the infected computer unusable[13].

Ukraine was the victim of another significant attack targeting a country's energy infrastructure. It was carried out on 23 December 2015, against three regional electricity distribution companies: Prykarpattyaoblenergo, Kyivoblenergo and Chernivtsioblenergo. These companies were responsible for the transmission

[7] Ibid., p. 4.

[8] Ibid., p. 9.

[9] T.M. Chen, *Stuxnet, the Real Start of Cyber Warfare?*, "IEEE Network" 2010, vol. 24, no. 6, p. 3. https://doi.org/10.1109/MNET.2010.5634434.

[10] N. Falliere, L.O. Murchu, E. Chien, *W32.Stuxnet Dossier*, Cupertino 2011, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf, p. 5 [accessed: 16 VII 2025].

[11] A. Nakov, G. Nuño, *Saudi Aramco and the Oil Market*, "Working Paper Series" 2011, no. 1354, p. 9.

[12] G. Siboni, S. Kronenfeld, *Iran and Cyberspace Warfare*, "Military and Strategic Affairs" 2012, vol. 4, no. 3, p. 90.

[13] It is worth noting, that since November 2022, the Saudi Aramco (Aramco Overseas Company B.V.) owns 30% stake in Gdańsk Refinery. See: *Saudi Aramco przejmie udziały w gdańskiej rafinerii* (Eng. Saudi Aramco to acquire stake in Gdańsk Refinery), CIRE, 12 I 2022, https://www.cire.pl/artykuly/rynek-paliw/saudi-aramco-przejmie-udzialy-w-gdanskiej-rafinerii [accessed: 14 XII 2024].

of electricity in the Ivano-Frankivsk, Kyiv and Chernivtsi regions, respectively. According to information from the US Cybersecurity and Infrastructure Security Agency (CISA), it is estimated that around 225 000 people were left without electricity for approx. six hours[14]. Moreover, institutions in the government, media, railway transport and mining sectors were also targeted[15]. The attack began (following a phase of open-source reconnaissance of the companies' infrastructure and initial operational preparations) with a phishing campaign distributed to employees of the aforementioned institutions. By opening an attachment in an email, employees unknowingly infected their organisations' networks with a malicious Trojan software[16] called BlackEnergy 3[17]. The malware then connected to C2 servers[18], after which the cybercriminals deployed tools on the infected workstations to extract authentication data and conducted reconnaissance of the attacked companies' internal networks. They gained the ability to log into these systems and networks as well as review the existing ICT infrastructure. After that, they uploaded additional malicious software, called KillDisk, which was to launch upon the operating system restart. The attackers turned off the uninterrupted power supplies (UPS) for selected servers, including those responsible for ICT services, then they activated the power switches. In this way, they disconnected at least 27 electrical substations from the network and cut off electricity supply to aforementioned approx. 225 000 people[19]. Then they uploaded their own patch to the switch management system to stop any further remote control of the switches. After that, the attackers carried out a DoS attack[20] on the call centre of Kyiv's energy distributor. This prevented customers from reporting power outages. The final stage of the operation was the pre-planned shutdown of the UPS devices, which triggered

[14] *Cyber-Attack Against Ukrainian Critical Infrastructure*, CISA, 20 VII 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [accessed: 28 XI 2024].

[15] J. Styczynski, N. Beach-Westmoreland,*When the lights went out: a comprehensive review of the 2015 attacks on Ukrainian critical infrastructure*, [n.p.] 2019, https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf, pp. 5–7, 30–39 [accessed: 16 VII 2025].

[16] Trojan – a type of a computer virus that imitates legitimate programmes and functions.

[17] This is a RAT Trojan (remote access trojan) enabling the attacker to remotely access the victim's workstation.

[18] C2 server (Command & Control) – infrastructure used by the attacker to control and manage systems and devices under his control, including the compromised infrastructure.

[19] SANS ICS, E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid. Defence Use Case*, March 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf, p. 11 [accessed: 6 VIII 2025].

[20] DoS (denial of service) – a type of attack aimed at disrupting the availability of a specific service.

the launch of malicious software called KillDisk upon system reboot. Its purpose was to destroy all data and logs stored on the devices, significantly hindering subsequent analysis that could have identified the causes of the event and possible countermeasures.

It is assumed that the cyberattack on the Ukrainian energy distributors was carried out by at least one cybercriminal state-sponsored group, i.e. APT44, which is linked to the Russian state apparatus[21]. The group is believed to operate under the authority of the Main Intelligence Directorate of the General Staff of the Russian Federation (Russian: Главное управление Генерального штаба Вооруженных Сил Российской Федерации, GRU)[22]. This kind of groups are often a political tool at the disposal of the Russian state.

Another cyberattack targeting various sectors of the Ukrainian state, including the energy sector, took place in 2017. As with the attacks in 2015, these activities were attributed to group APT44[23]. The name of the attack comes from the malicious NotPetya software used in the attack, which was characterised by its ease of lateral movement, disk encryption capabilities and destructive nature. Initially, NotPetya was identified as a type of ransomware[24], however, it did not include any decryption keys that would allow the infected device to be restored to a usable state or its files to remain intact. Such programmes are referred to as wiper. The attack targeted the Ukrainian state and the broadly understood ICT infrastructure located on its territory. However, due to the presence of many branches of foreign companies in Ukraine and the specific nature of the software used (the fastest propagation across the network), the reach of the attack quickly exceeded Ukraine's digital borders and the virus spread globally at a speed not previously observed[25]. In response to cyberattack, the federal government of the United States held six citizens of the Russian Federation criminally accountable – GRU officers[26].

[21] J. Hultquist, *Sandworm Team and the Ukrainian Power Authority Attacks*, Mandiant, 7 I 2016, https://cloud.google.com/blog/topics/threat-intelligence/ukraine-and-sandworm-team [accessed: 15 XII 2024].

[22] G. Roncone et al., *APT44: Unearthing Sandworm*, Mandiant, 17 IV 2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf, p. 2, 7 [accessed: 16 VII 2025].

[23] M. Kerttunen, J. Hemmelskamp, *Major Cyber Incidents: NotPetya*, March 2023, https://eurepoc.eu/wp-content/uploads/2023/05/MACI_NotPetya.pdf, pp. 3–4 [accessed: 16 VII 2025].

[24] Ransomware – a type of malicious software that blocks an access to data on a computer or network and demands a ransom for restoring it.

[25] The ease with which NotPetya software was able to infect subsequent workstations and servers was made possible by combining two tools, i.e. Mimikatz and EternalBlue.

[26] M. Kerttunen, J. Hemmelskamp, *Major Cyber Incidents*…, pp. 3–4.

As mentioned, the attack aimed to infect as many ICT devices in Ukraine as possible and was therefore not directly targeted at the energy sector. However, this sector did not escape the impact of the virus. The victims of the attack included Kyivenergo and Ukrenergo – companies responsible for the distribution of electricity in Ukraine at both the local and national levels[27]. This incident demonstrates that entities in the energy sector must protect themselves not only against targeted threats, but also against general threats faced by other sectors. This significantly broadens the scope of threat monitoring.

In 2023, the Reuters news agency reported that, the Russian Federation made Ukraine's energy sector a priority target of cyberattacks following the invasion[28]. According to reports from this agency, the Security Service of Ukraine (Ukrainian: Служба безпеки України, SBU) determined that, Russia carries out an average of 10 attacks per day. These includes attempts to disable parts of Ukraine's energy infrastructure. This showed that cyberspace functions like a system of interconnected vessels. An example is the attack on a Ukrainian satellite, which resulted in the unavailability of the remote monitoring system for more than 5800 wind turbines in Germany[29].

Since the beginning of the invasion of Ukraine, offensive operations in cyberspace targeting the energy infrastructure of other European countries have been carried out. One of them was a series of attacks conducted in 2023 against Danish CI operators. These attacks were described in a report by SektorCERT – the computer security incident response team responsible for protecting Denmark's CI sector[30]. According to the report, this was the largest and most costly attack ever carried out against this infrastructure. The perpetrators targeted parts of industrial control systems (ICS) in companies and gained access to the ICT infrastructure of 22 entities within the energy sector. All the attacks were carried out simultaneously, they were prepared carefully well in advance and the attackers had knowledge of where to conduct offensive operations[31]. SektorCERT faced the challenge of simultaneously handling incidents affecting 16 attacked institutions, along with additional six

[27] C. Krasznay, *Case Study: The NotPetya Campaign*, in: *Információ-* és *kiberbiztonság*, B. Török (ed.), Budapest 2020, p. 486.

[28] N. Buli, N. Chestney, Ch. Steitz, *Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war*, Reuters, 15 VI 2023, https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/ [accessed: 5 XII 2024].

[29] Ibid.

[30] SektorCERT, *The attack against Danish, critical infrastructure*, November 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [accessed: 5 XII 2024].

[31] Ibid., p. 10.

that were targeted during a second wave of attacks. SektorCERT attributed these subsequent attacks to another, as yet unidentified, cybercriminal group, which was employing new attack tools, including numerous 0-day vulnerabilities[32]. This indicates a high level of skills in discovering such vulnerabilities or financial resources to purchase information about security flaws from other cybercriminal groups[33]. It is suspected that group APT44[34] was behind the attacks (or at least some of them). Notably, SektorCERT determined that the sources of the attacks at their peak originated from IP addresses that, according to geolocation data, pointed to Poland and Ukraine[35].

Identification of energy sector resources in the maritime area of the RP

In PEP2040, a significant emphasis has been placed on the country's offshore and coastal energy subsector. This is demonstrated by the following actions listed in this document:

- establishment of offshore wind farms in Poland's exclusive economic zone, which are expected to reach capacity to generate electricity of approx. 11 GW by 2040,
- creation of main installation terminal (port) specialising in servicing the supply chain for offshore wind farms,
- expansion of the transmission network in the northern and north-western parts of Poland in order to adapt the Polish power system for receiving and transmitting energy generated, among other sources, by offshore wind power plants,
- import of natural gas via the Baltic Pipe since 2022. Possible import of 10 billion m^3 of natural gas and an export – 3 billion m^3,
- increase of the regasification capacity of the LNG terminal in Świnoujście to 8.3 billion m^3 of natural gas,

[32] 0-day vulnerability – a vulnerability that has not been publicly acknowledged by the vendor and for which no official software update exists to mitigate the vulnerability.

[33] *Behind the Rise of the Million Dollar Zero-Day Market*, SIRP, https://sirp.io/behind-the-rise-of-the-million-dollar-zero-day-market/ [accessed: 14 XII 2024].

[34] *The attack against Danish, critical infrastructure*…, pp. 14–16.

[35] Ibid., p. 26.

- construction of a natural gas regasification terminal in the Gulf of Gdańsk (FSRU terminal[36]) with a nominal capacity of 4.5 billion m^3 of gas,
- expansion of gas pipelines in the northern and central parts of Poland to enable the transport of gas from the FSRU terminal further inland,
- possible expansion of the Kosakowo Underground Gas Storage Facility in Dębogórze,
- increasing the crude oil storage capacity at the oil terminal and the PERN base in Gdańsk to approx. 1.9 billion m^3,
- construction of a second line of the Pomeranian Pipeline to optimise the transport of crude oil from the Naftoport in Gdańsk further inland,
- increasing the production capacity of the Gdańsk Refinery in the area of petrochemicals,
- extraction of crude oil from deposits located in the Baltic Sea and on the Norwegian continental shelf,
- identification of new crude oil and natural gas deposits in the Baltic Sea and on the Norwegian continental shelf,
- enabling LNG bunkering in Poland's four largest ports: Gdańsk, Gdynia, Szczecin and Świnoujście,
- establishment of a submarine direct current connection between Poland and Lithuania (and more broadly, the Baltic States) with a planned capacity of 700 MW (220 kV),
- potential use of hydropower resources.

This list could be supplemented with existing energy infrastructure that is not mentioned in PEP2040 but is, to some extent, concentrated around the country's offshore or coastal energy sector – such as the submarine interconnection between Sweden and Poland via the SwePol Link cable line with a capacity of 600 MW (450 kV) as well as crude oil and liquid fuel storage facilities: Dębogórze, Świnoujście, Trzebież, Szczecin, Koszalin, Ugoszcz, Gdańsk. It is likely that almost all of Poland's demand for natural gas will be covered by supplies from the direction of the Baltic Sea, primarily through the Baltic Pipe. Offshore wind farms are expected to become one of the three main pillars of Poland's future energy mix, meeting approx. 18% of the country's energy demand[37]. In addition, the electricity generated by the planned nuclear power plant, which is to be located in the Pomeranian Voivodeship, should also be taken into account, as the power system (mainly the transmission

[36] FSRU (floating storage regasification unit) – a floating unit used for regasification of natural gas.

[37] *Morskie farmy wiatrowe najważniejsze w transformacji energetycznej Polski* (Eng. Offshore wind farms key to Poland's energy transition), Polityka, 2023, https://polityka.co.pl/morskie-farmy-wiatrowe-najwazniejsze-w-transformacji-energetycznej-polski-3060556.html [accessed: 15 XII 2024].

infrastructure) being developed in the northern part of Poland will be expanded and adapted to share transmission infrastructure with this nuclear power plant as well as, among others, offshore wind farms located in at least two shoals: the Middle Bank (Ławica Środkowa) and the Słupsk Bank (Ławica Słupska). This means that any cybersecurity threats related to the distribution of electricity from the planned offshore wind farms and the nuclear power plant will have a significant impact on both projects, considerably hindering their operation.

As part of the identification of energy sector resources in the maritime area of the RP and the related threats, additional entities that influence the shape of Poland's energy sector in the context of offshore and coastal energy have been taken into account, namely: the maritime offices in Gdynia and Szczecin, as well as the Ministry of Climate and Environment (as the office serving the minister responsible for the 'energy' area of public administration)[38].

Types of potential adversaries for the ICT resources of companies in the Polish energy sector

It can be anticipated that the investments undertaken in the Polish energy sector will generate relatively high profits, particularly for companies that form the backbone of this sector. This may encourage cybercriminals to carry out offensive actions against these entities. However, such actions do not necessarily have to be motivated by financial gain alone. Significant threats may also come from APT groups, state-sponsored or state-linked cybercriminal groups, business rivals and hacktivists.

The greatest threat that should be considered when assessing the resilience of one's own ICT systems and networks currently comes from APT groups. The aim of their precise attacks are usually the most critical companies and institutions. These operations can last for many months or even years, involving careful reconnaissance of the target, preparation of dedicated tools tailored to the victim's identified weaknesses, maintaining gained access to the systems and evading detection.

Another type of threat comes from cybercriminal groups that are state-sponsored or state-affiliated. They often operate (like APT groups) on a contractual basis, including selling their services to other actors. The aim of state-sponsored actors, which are not a part of APT groups, is more likely to involve short-term

[38] § 1(2) point 1 of the *Regulation of the Prime Minister of 19 December 2023 on the detailed scope of activities of the Minister of Climate and Environment.*

and/or medium-term activities focused, for example, on disrupting the operations of an organisation or conducting propaganda.

Business rivals may pose a threat in the context of stealing or otherwise attempting to obtain information about the status of ongoing projects and the companies carrying them out. This constitutes unfair competition: based on data theft, a business rival may attempt to harm the planned investment, the company executing it or adjust their own investment plans in response to the adversary's actions. Such harmful activities can be carried out directly by the business rival alone, but it is much more common practice to outsource this to an external actor (cybercriminal group) with no formal connection to the client.

The last group mentioned are hacktivists, who carry out their activities in cyberspace for ideological reasons. Their motivation to take action usually stems from political events. Hacktivists can attack both government institutions in the heat of the moment (e.g. after a decision by the authorities that they did not accept) or targeting companies whose business, environmental, pricing or public relations policies provokes their opposition.

The actors described above may attempt sabotage, infiltration or destruction of ICT infrastructure supporting energy projects. Therefore, it is essential that the entities responsible for these projects and decision-makers conduct risk analyses and develop security plans, so that the threat of a cyberattack can be reduced to an acceptable level.

Moreover, it is also worth noting that the presence of companies with foreign capital in the Polish energy market may encourage adversaries to carry out offensive actions targeting the capital invested in energy projects in Poland. One example is the Gdańsk Refinery, in which a significant stake is owned by a subsidiary of the Saudi Aramco capital group. Such activities may be of particular interest to hacktivists and business rivals.

ICT resources in the offshore energy sector enterprises and types of attacks against them

The resources that an organisation in the energy sector, including offshore energy, must protect to prevent a cybersecurity incident can be divided into two groups of the so-called ICT infrastructure environments. These are corporate environments and industrial control system environments.

Different systems and devices, due to the nature of their functions, may be used for office tasks and for activities that ensure the operation of industrial machinery necessary for the production or distribution of electricity. Although in theory it is possible to completely separate these two environments, in practice they are often interdependent. An example of this is the need for authorised user from the corporate network or a user from external company providing machine maintenance services to take corrective actions in the industrial control system environment through remote access.

In a mature organisation, the corporate environment typically uses such systems and devices as: its own domain, domain controller, web servers, email servers, database servers, business applications and endpoints (workstations, printers) etc. Regardless of the specifics of the corporate environment, it should be adequately protected due to the risks to the continuity of business operations, its impact on the industrial control systems and its dependence on them.

In the industrial control system environment of a large enterprise, which includes entities responsible for the production and distribution of electric energy, there should be systems and devices such as: remote terminal units (RTU), HMI interfaces[39], SCADA system[40], controllers, PLCs[41], signal converters, optical diodes, as well as sensors and detectors. These, in turn, should be protected by systems and devices similar to those used in corporate environments or specialised for industrial control system environments, depending on specific needs. The examples presented are not exhaustive due to the varying nature of environments in different enterprises, which may adopt diverse approaches to the design and maintenance of their ICT infrastructure, depending on available financial and human resources.

Common problems occurring in both environments include: outdated software versions that are vulnerable to attacks[42], a lack of user awareness about threats as well as the failure to apply good practices and standards in the field of ICT and cybersecurity. For example, in an attack using malware WannaCry, outdated software in the form of the SMBv1 protocol was used[43].

A relatively common type of attack targeting industrial control system environments is a supply chain attack. Attackers take such actions when are unable to gain direct access – that is, a point of entry – to the target infrastructure.

[39] HMI (human-machine interface) – interface between the machine and its operator, most often in the form of a graphical representation of the process.

[40] SCADA (supervisory control and data acquisition) – ICT system supervising the course of the production process.

[41] PLC (programmable logic controller) – used to control the operation of a machine.

[42] *Outdated Software*, Plurilock, https://plurilock.com/deep-dive/outdated-software/ [accessed: 15 XII 2024].

[43] M. Akbanov, V.G. Vassilakis, M.D. Logothetis, *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, "Journal of Telecommunications and Information Technology" 2019, vol. 75, no. 1, pp. 114–115. https://doi.org/10.26636/jtit.2019.130218.

Smaller subcontractors, who usually have proportionally lower investments in their company's security, are an easier target. Such an attack can occur, for example, when the supplier, under an agreement with the organisation, has remote access to its industrial ICT infrastructure. In this way, attackers can obtain authentication data for service accounts within the organisation's industrial control system and conduct further offensive operations directly there.

Protective mechanisms for the ICT resources of Polish energy sector

Ways to secure ICT resources of Polish energy sector, including the offshore and coastal energy sector, can be divided into individual and state-level security measures related to the activities of specific services and institutions.

Individual security measures of CI operator

Important ways to counteract the effects of a potential attack include, among others, the use of firewall devices, network segmentation allowing potentially compromised devices to be isolated, and strict control of user account privileges (identity and access management / privileged access management, IAM/PAM) in line with best practices of industry environment[44]. It happens that control panels for industrial control system infrastructure are accessible from the internet, sometimes even without requiring user authentication, which poses a serious risk to such a system[45].

Due to the possibility of mutual interaction between corporate environments and industrial control system environments, they should be secured in a consistent manner that does not treat either area as a less important dimension of security. Both environments usually utilise shared elements of the enterprise's ICT infrastructure, such as the same domain. Therefore, both can become victims of an attack if not properly secured. These solutions should be protected by, among other things, devices and systems such as firewalls, multi-factor authentication (MFA), sytems: Anti-DDoS; security information and event management (SIEM); security orchestration, automation and response (SOAR); intrusion detection system (IDS); intrusion prevention system (IPS); data loss prevention (DLP); endpoint detection and response (EDR); antivirus software, as well as IAM/PAM solutions, servers with backup copies (backup), email filters and UPS.

[44] *Security and Privacy Controls For Information Systems and Organizations*, NIST, September 2020, pp. 19–20. https://doi.org/10.6028/NIST.SP.800-53r5.

[45] *Raport roczny z działalności CERT POLSKA 2023* (Eng. CERT Polska Annual Report for 2023), https://cert.pl/uploads/docs/Raport_CP_2023.pdf, pp. 57–58 [accessed: 16 VII 2025].

Importantly, according to the draft law amending the Act on crisis management and certain other acts currently under consideration, it is planned, among other things, to impose minimum cybersecurity standards on CI operators[46]. This may result in improved ICT security for institutions that are crucial from the state's perspective. These requirements will be based on the results of a risk assessment of organisational and technical solutions carried out by the given entity. This is a new approach that takes into account the evolution of threats and the time-based depreciation of implemented safeguards, in order to ensure the continuity of security measures.

Furthermore, under the draft law amending the Act on the National Cybersecurity System[47], it is planned to conduct risk assessments related to the supply chain, including suppliers and business customers with whom the entity intends to cooperate. Such an assessment will aim to ensure the security of the entrepreneur's networks and ICT systems against potential supply chain attacks. The proposed amendment may still change in scope regarding risk assessment, especially the provisions concerning entities designated as high-risk suppliers. Changes may be dictated by, among other things, public concerns related to submitted proposals, including arbitrary and politically motivated decisions that could result in an entity being classified as a high-risk supplier[48].

State-level security measures for CI operator

Despite the growing threat of attacks on the country's CI, it is not the role of an entrepreneur to allocate all company revenues to making the enterprise resilient to a given type of threat. It is the state that should protect its interests, including by ensuring the continuity of its functioning through the security of electricity generation and distribution processes within its territory. These tasks are carried out, among others, by the Armed Forces of the RP under Article 26 of the *Constitution of the Republic of Poland of 2 April 1997* and subordinate legislation, the Internal Security Agency and the Foreign Intelligence Agency based on Articles 5 and 6 of the *Act of 24 May 2002 on the Internal Security Agency and*

[46] *Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw* (Eng. Draft law amending the Act on the crisis management and certain other acts), no. UC47, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-zarzadzaniu-kryzysowym-oraz-niektorych-innych-ustaw5 [accessed: 16 VII 2025].

[47] *Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa…*

[48] M. Fraser, *Organizacje przedsiębiorców krytycznie o nowelizacji KSC. Dostawcy wysokiego ryzyka do poprawki* (Eng. Business groups criticise the National Cybersecurity System amendment. High-risk suppliers to be reconsidered), CyberDefence24, 9 XI 2021, https://cyberdefence24.pl/polityka-i-prawo/organizacje-przedsiebiorcow-krytycznie-o-nowelizacji-ksc-dostawcy-wysokiego-ryzyka-do-poprawki [accessed: 18 VII 2025].

the Foreign Intelligence Agency as well as the Police based on Article 1(2) points 2–4 of the *Act of 6 April 1990 on the Police*. The role of these institutions is to identify threats to national security and to respond accordingly.

Activities related to the protection of the interests of Poland's offshore and coastal energy sector are carried out by, among others:

- the Polish Navy – as the branch of the armed forces responsible for ensuring the country's maritime security,
- the Maritime Border Guard Unit – which provides ongoing supervision and control of maritime areas,
- Special Forces in the form of military units GROM and Formoza – which enable a rapid response to asymmetric kinetic operations,
- the Internal Security Agency – carrying out preventive tasks related to national security, CI and economic interests of the RP,
- the Foreign Intelligence Agency – carrying out tasks to counter external threats to the RP and its interests and property,
- the Police – as an authority tasked with safeguarding national security and public order,
- CSIRT GOV – responsible for protecting the state's CI in the context of cybersecurity threats.

Most of the listed institutions carry out protective tasks, mainly related to kinetic threats, both symmetric and asymmetric. In turn, CSIRT GOV, which stands for the Computer Security Incident Response Team, operating within the framework of the Internal Security Agency, carries out its activities on the basis of Article 26 points 3 and 7 as well as Article 27 point 1 of the Act on the National Cybersecurity System and protects, among others, CI operators in the state's digital sphere. This enables assistance to be provided to these operators in the event of attacks by, among others, APT and state-sponsored groups.

It is worth noting that Poland recognises threats to its interests in the Baltic Sea region and pursues a policy aimed at securing them. For instance, a new combat team within the Formoza Military Unit was formed, which is intended to enable more effective counteraction against kinetic threats of an asymmetric nature in the Baltic Sea area[49].

[49] *Powstaje kolejny zespół bojowy w Formozie. To odpowiedź na współczesne zagrożenia militarne i niemilitarne związane z funkcjonowaniem infrastruktury krytycznej* (Eng. Another combat team is being formed in Formoza. It is a response to contemporary military and non-military threats to the operation of critical infrastructure), Ministerstwo Obrony Narodowej, 22 VIII 2023, https://www.gov.pl/web/obrona-narodowa/powstaje-kolejny-zespol-bojowy-w-formozie-to-odpowiedz-na-wspolczesne-zagrozenia-militarne-i-niemilitarne-zwiazane-z-funkcjonowaniem-infrastruktury-krytycznej [accessed: 10 XII 2024].

It should be noted that probably not all of energy facilities and investments mentioned in the article will be included in the CI, based on the criteria specified in classified Annex No. 2 to the National Critical Infrastructure Protection Program[50]. This may result from the fact that these facilities, still under development, may not yet have undergone the procedure for selecting CI objects from among the state's overall infrastructure. Due to the unique nature of investments such as offshore wind farms, one could consider whether Poland should act proactively and designate these facilities, their installations or parts thereof, as CI even before their completion. This would enable the state to protect the infrastructure as soon as it is built or modernised. Such an approach would constitute a comprehensive strategy for safeguarding the state's energy interests.

Summary

Due to threats posed primarily by APT groups and state-sponsored groups to current and planned investments in offshore and coastal energy infrastructure, it is necessary for the Polish state to provide support to ensure a predefined level of security for exposed organisations and their ICT infrastructure, including security in cyberspace. For strategic projects implemented under PEP2040, ICT infrastructure should be secured from the very beginning of its development, in line with *security by design* approach. This infrastructure should be created in accordance with industry best practices in the cybersecurity industry, in order to minimise the risk of effective attack.

Based on the presented materials, it can be inferred that the Polish state is currently only basically prepared to ensure cybersecurity for the offshore and coastal energy sector. In the era of ruthless competition in cyberspace, this may prove insufficient, especially considering the threats that may emerge in the future and the available ways to mitigate them. There is a lack of proactive measures to ensure that energy projects of strategic importance to national security are secured from the very beginning of their development cycle (planning and conceptual phases). Furthermore, as indicated, a threat may materialise not only through a direct cyberattack on an organisation but also – which is becoming increasingly common – through an attack on the supply chain. The subcontractor may turn out to be a convenient entry point to the target organisation's infrastructure. Without expansion of security measures by both the CI operators and the state, the security

[50] *Narodowy Program Ochrony Infrastruktury Krytycznej* (Eng. National Critical Infrastructure Protection Program), Rządowe Centrum Bezpieczeństwa, Warszawa 2023.

may prove ineffective and inadequate in the face of evolving realities. It may be necessary to assess the impact of new regulations, such as amendments to the Act on crisis management and the Act on National Cybersecurity System, to evaluate their effectiveness in addressing current and future cybersecurity challenges. This could enable a more comprehensive approach to the issue.

Bibliography

Akbanov M., Vassilakis V.G., Logothetis M.D., *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, "Journal of Telecommunications and Information Technology" 2019, vol. 75, no. 1, pp. 113–124. https://doi.org/10.26636/jtit.2019.130218.

Chen T.M., *Stuxnet, the Real Start of Cyber Warfare?*, "IEEE Network" 2010, vol. 24, no. 6, pp. 2–3. https://doi.org/10.1109/MNET.2010.5634434.

Krasznay C., *Case Study: The NotPetya Campaign*, in: *Információ-* és *kiberbiztonság*, B. Török (ed.), Budapest 2020.

Nakov A., Nuño G., *Saudi Aramco and the Oil Market*, "Working Paper Series" 2011, no. 1354.

Security and Privacy Controls For Information Systems and Organizations, NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

Siboni G., Kronenfeld S., *Iran and Cyberspace Warfare*, "Military and Strategic Affairs" 2012, vol. 4, no. 3, pp. 77–99.

Internet sources

Baezner M., Robin P., *Hotspot Analysis: Stuxnet*, Zürich 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf [accessed: 16 VII 2025].

Behind the Rise of the Million Dollar Zero-Day Market, SIRP, https://sirp.io/behind-the-rise-of-the-million-dollar-zero-day-market/ [accessed: 14 XII 2024].

Buchholz K., *Baltic Sea Cable Incidents Pile Up*, Statista, 6 II 2025, https://www.statista.com/chart/33892/damage-to-underwater-cables-and-pipelines-in-the-baltic-sea/ [accessed: 16 VII 2025].

Buli N., Chestney N., Steitz Ch., *Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war*, Reuters, 15 VI 2023, https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/ [accessed: 5 XII 2024].

Cyber-Attack Against Ukrainian Critical Infrastructure, CISA, 20 VII 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [accessed: 28 XI 2024].

Falliere N., Murchu L.O., Chien E., *W32.Stuxnet Dossier*, Cupertino 2011, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf [accessed: 16 VII 2025].

Fraser M., *Organizacje przedsiębiorców krytycznie o nowelizacji KSC. Dostawcy wysokiego ryzyka do poprawki* (Eng. Business groups criticise the National Cybersecurity System amendment. High-risk suppliers to be reconsidered), CyberDefence24, 9 XI 2021, https://cyberdefence24.pl/polityka-i-prawo/organizacje-przedsiebiorcow-krytycznie-o-nowelizacji-ksc-dostawcy-wysokiego-ryzyka-do-poprawki [accessed: 18 VII 2025].

Hultquist J., *Sandworm Team and the Ukrainian Power Authority Attacks*, Mandiant, 7 I 2016, https://cloud.google.com/blog/topics/threat-intelligence/ukraine-and-sandworm-team [accessed: 15 XII 2024].

Kerttunen M., Hemmelskamp J., *Major Cyber Incidents: NotPetya*, March 2023, https://eurepoc.eu/wp-content/uploads/2023/05/MACI_NotPetya.pdf [accessed: 16 VII 2025].

Lorenz W., Zaręba S., *Konsekwencje eksplozji rurociągów Nord Stream 1 i 2* (Eng. Consequences of the explosion of the Nord Stream 1 and 2 pipelines), Polski Instytut Spraw Międzynarodowych, 29 IX 2022, https://pism.pl/publikacje/konsekwencje-eksplozji-rurociagow-nord-stream-1-i-2 [accessed: 16 VII 2025].

Morskie farmy wiatrowe najważniejsze w transformacji energetycznej Polski (Eng. Offshore wind farms key to Poland's energy transition), Polityka, 2023, https://polityka.co.pl/morskie-farmy-wiatrowe-najwazniejsze-w-transformacji-energetycznej-polski-3060556.html [accessed: 15 XII 2024].

Outdated Software, Plurilock, https://plurilock.com/deep-dive/outdated-software/ [accessed: 15 XII 2024].

Powstaje kolejny zespół bojowy w Formozie. To odpowiedź na współczesne zagrożenia militarne i niemilitarne związane z funkcjonowaniem infrastruktury krytycznej (Eng. Another combat team is being formed in Formoza. It is a response to contemporary military and non-military threats to the operation of critical infrastructure), Ministerstwo Obrony Narodowej, 22 VIII 2023, https://www.gov.pl/web/obrona-narodowa/powstaje-kolejny-zespol-bojowy-w-formozie-to-odpowiedz-na-wspolczesne-zagrozenia-militarne-i-niemilitarne-zwiazane-z-funkcjonowaniem-infrastruktury-krytycznej [accessed: 10 XII 2024].

Roncone G., Black D., Wolfram J., McLellan T., Simonian N., Hall R., Prokopenkov A., Perez D., Aytes L., Wahlstrom A., *APT44: Unearthing Sandworm*, 2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf [accessed: 16 VII 2025].

SANS ICS, E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid. Defence Use Case*, March 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS--and-Electricity-Information-Sharing-and.pdf [accessed: 6 VIII 2025].

Saudi Aramco przejmie udziały w gdańskiej rafinerii (Eng. Saudi Aramco to acquire stake in Gdańsk refinery), CIRE, 12 I 2022, https://www.cire.pl/artykuly/rynek-paliw/saudi-aramco-przejmie-udzialy-w-gdanskiej-rafinerii [accessed: 14 XII 2024].

SektorCERT, *The attack against Danish, critical infrastructure*, November 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [accessed: 5 XII 2024].

Styczynski J., Beach-Westmoreland N., *When the lights went out: a comprehensive review of the 2015 attacks on Ukrainian critical infrastructure*, [n.p.] 2019, https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf [accessed: 16 VII 2025].

Legal acts

Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997, no. 78, item 483, as amended).

Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws of 2024, item 1077, as amended).

Act of 26 April 2007 on crisis management (consolidated text, Journal of Laws of 2023, item 122, as amended).

Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency (consolidated text, Journal of Laws of 2025, item 902).

Act of 6 April 1990 on the Police (consolidated text, Journal of Laws of 2025, item 636, as amended).

Regulation of the Prime Minister of 19 December 2023 on the detailed scope of activities of the Minister of Climate and Environment (Journal of Laws of 2023, item 2726).

Other documents

Narodowy Program Ochrony Infrastruktury Krytycznej (Eng. National Critical Infrastructure Protection Program), Rządowe Centrum Bezpieczeństwa, Warszawa 2023.

Polityka energetyczna Polski do 2040 r. (Eng. Energy Policy of Poland until 2040), Ministry of Climate and Environment, Warszawa 2021.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Eng. Draft law amending the Act on the National Cybersecurity System and certain other acts), no. UC32, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw3 [accessed: 16 VII 2025].

Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (Eng. Draft law amending the Act on the crisis management and certain other acts), no. UC47, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-zarzadzaniu-kryzysowym-oraz-niektorych-innych-ustaw5 [accessed: 16 VII 2025].

Raport roczny z działalności CERT POLSKA 2023 (Eng. CERT Polska Annual Report for 2023), https://cert.pl/uploads/docs/Raport_CP_2023.pdf [accessed: 16 VII 2025].

David Cybulski

Specialist in the field of cybersecurity. He gained professional experience in the private sector and in state administration. Passionate about innovative cybersecurity solutions and new techniques used in cyberattacks by APT groups, with particular emphasis on social engineering attacks. His scientific interests include the protection of critical infrastructure, the activity of selected APT groups, the security aspects of Shadow IT and Cyber Threat Intelligence / Threat Hunting activities towards selected cybercriminal groups.

Contact: dcybulski@proton.me