Major Cyber Incidents

Polish Energy Infrastructure Attacks, 2025

Other incident names: DynoWiper

By Sebastian Harnisch and Noah Ries

Description

Turla, allegedly acting on behalf of the 16th Centre of Russia's Federal Security Service (FSB), conducted a disruptive sabotage operation against critical energy infrastructure in Poland between 29 and 30 December 2025. The incident was directed against both the information systems (IT) and physical/industrial equipment (OT) of approximately 30 solar and wind farms, as well as two combined heat and power plants (CHP). Reporting to date suggests a sequenced, two-pronged attack pattern. In the first phase, the attackers gained access to the targeted systems as early as March 2025, resulting in long-term infiltration of the infrastructure and the theft of sensitive data. In the second phase, the attackers used their access to deploy wiper malware in late December 2025 [1], [2], [3], [32]. At the same time, the identical wiper malware was used in a second incident which occurred at a manufacturing company; however, the second attack is treated as opportunistic and unrelated to the energy-sector targets. While the disruptive impact of the attacks remained limited, the operation drew strong national and international responses, starting with a detailed report on the attacks against solar and wind farms, as well as a large CHP, by the Polish Cyber Emergency and Response Team (CERT GOV) in January 2026 [4], which was supplemented by EU, UK, German, and French attributions in July 2026. This was joined by a statement by the EU High Representative Kaja Kallas denouncing "the most significant Russian-sponsored cyberattack on critical infrastructure in a NATO/EU country since 2022" [5]. A second Polish CERT report in August 2026 also revealed an attack on a smaller CHP which had been originally assessed as a technical failure by the operator

Timeline
(Suspected) March – December 2025
(Certain) Late 2025 – December 2025

Affected Targets
Russia state-linked Turla

Incident Type
Hijacking without misuses

Affected Targets
Approx. 30 wind and solar farms; 2 combined-heat-and power plants; private manufacturing company (all in Poland)
ss

Impact and significance

The attempted destruction of Polish energy infrastructure, which could have resulted in the loss of access to electricity for 550,000 citizens, is a significant escalation of hybrid warfare operations and tactics by Russian state-affiliated actors against NATO and EU countries supporting Ukraine. Operational details and subsequent national responses, including two detailed investigative reports by the Polish CERT GOV (published on 30 January 2026 and 8 August 2026), inferred that a single attacker group was able to exploit IT-systems and workstations used by engineers to monitor and manage data, which had below-average security protections; the group was also able to infiltrate OT systems, or physical operations control applications. Notably, some of the systems involved were (still) configured with default usernames and passwords, and did not have multi-factor authentication. Therefore, the attackers faced insufficient protections when initially infiltrating the targeted systems and compromising data integrity.

Notably, the attacker used previously unknown TTPs when leveraging a Programmable Logic Controller (PLC) in a private data transmission network (Private APN) to gain access to the OT environment of the smaller CHP, resulting in a temporary shutdown of a steam turbine and water treatment system [33]. While electricity generation continued and the national transmission remained stable in this period, the destructive attack starting in late December 2025 nixed the monitoring and control layer in compromised systems, resulting in a significant loss of operational control. The first CERT report also mentions a private company in the manufacturing sector being targeted simultaneously [4].

Preparatory activities during the initial phase likely provided the attackers with tacit knowledge about the Polish electrical grid and vulnerabilities of decentralised power generation systems, run by various companies through remote terminal units (RTUs) and featuring different software applications. During the disruption phase in December, attackers were able to install wiper malware which disabled monitoring and control functions in the wind and solar network, but failed to destroy data on workstations because the intrusion detection system blocked the full execution of the wipers (see below). Current reporting leaves open whether disruption was planned from the beginning on, or whether that course of action was chosen during the operation.

Interestingly, the potential impact and the sobering details about the attacker's TTPs appear to have triggered a distinct response pattern by the Polish government and its partners: first, senior Polish government officials prominently ascribed responsibility to Russian actors [6], seconded by initial private sector cyber threat intelligence (CTI) reporting. ESET attributed the attack to the threat actor Sandworm, "commonly attributed to Unit 74455 of the Russian Main Intelligence Directorate (GRU)" [7]. With moderate confidence, DRAGOS attributed the attack to ELECTRUM, a group with "technical and operational overlaps with Sandworm" [8]. Subsequently, the Polish CERT issued an unvarnished report which detailed how poor operational security enabled the coordinated attack [4].

Later, a coordinated group of partnered governments (US, UK, Germany, France), as well as the European Union and NATO, supported the Polish CERT's attribution to Turla (aka

Berserk Bear, Dragonfly, etc.), which is associated with the FSB. Like Static Tundra, Turla is considered to be part of the FSB Centre 16 [5], [9], [10]. The European Union then imposed restrictive measures on nine individuals and four entities in a joint sanctions package alongside the UK [5].

The impact and significance of this operation stems less from the material impact of the wiper attacks or the technical sophistication of the operation – except for the leveraging of a private APN at the second CHP. The attack on the grid connection substation resulted in the loss of communication between the solar and wind facilities and distribution system operators (DSOs) because RTU controllers were damaged; however, this did not affect ongoing electricity generation.

Thus, the importance lies with the potential shift in aggressive intentions by Russian state-associated APTs against NATO Member States' critical infrastructure, also signalling a capacity (if not willingness) to preposition destructive assets in civilian critical infrastructure in preparation for a (conventional) conflict in the future.

Secondly, a shift towards more destructive operations by Turla may have occurred, plausibly indicating a more general trend in Russian state-related APT strategy. As stated above, the evidence presented by the Polish CERT in the first report leaves open the question whether this attack was "disruption by design" or "disruption by opportunity." It also remains unclear whether Turla acted alone during both phases of the operation. Given the scope of the operation and the sophistication of the APN penetration at the second CHP, there may have been other actors involved too.

Thirdly, the early and detailed responses by Polish and partner governments suggest that the attack persuaded them to ring alarm bells to forego similar operations against critical infrastructure elsewhere. This way, the attack on Poland, despite substantial efforts by the Polish government to harden digital defenses, convinced both EU and NATO officials to raise the guard because critical infrastructure in key NATO/EU Member States apparently remained vulnerable.

Background

The 2025 Polish energy infrastructure attack should be interpreted in the context of the wider hybrid threat environment. The Republic of Poland has faced an unprecedented number of cyber and hybrid attacks, both before and especially after the start of the Russian full-scale war against Ukraine in 2022; this includes attacks on the water supply and transport system, arson attacks, and various violations of Polish airspace. In a noteworthy development, cyberattacks in Poland reportedly more than doubled in 2025 [11], [12].

Critical infrastructure in Poland, such as water and energy suppliers, as well as the transport sector, have been targeted regularly by Russian actors or their proxies. In May 2025, a cyberattack was launched against a hydropower plant without disrupting the power supply; in August and September 2025, the IT infrastructure of one of Poland's largest energy companies was penetrated. In the first half of 2025, similar attacks were directed against water supply and water sewage infrastructure, with attackers gaining access to operational technology and manipulating the equipment's operation parameters [11, pp. 64–68].

In response to this threat landscape, the Polish government significantly increased defence investment – Poland being now the largest spender on defence within NATO as a percentage of GDP – pursuing a platform-centric and off-the-shelf approach to digital defence modernisation [13]. Notably, the Polish Council of ministers adopted an amendment to the National Cybersecurity System Act (KSC) in late October 2025, transposing the NIS-2 directive into national law. The revelation of the cyber operation against energy infrastructure in January 2026 then hastened the legislative process, leading to an early entry into force of the amendment (April 2026) and a series of ad-hoc recommendations to better protect the energy sector, e.g., by isolating automation systems from the internet.

Turla, a possibly state-integrated cyber threat actor which is often associated with the FSB, obtains considerable technical sophistication and has conducted successful operations, stretching back to the 1990s. Given its purported closeness to the FSB and related entities, such as the Russian IT company CenterInform, its technical, logistic and human capacities are deemed to be substantial. Operational evidence suggests that the group's hijacking of satellite connections (e.g., for Moonlight Maze) required tacit knowledge of related systems which are regularly reserved for state intelligence agencies. The group's criticality and persistence over time further support the argument of extensive (Russian) state backing [14, p. 2].

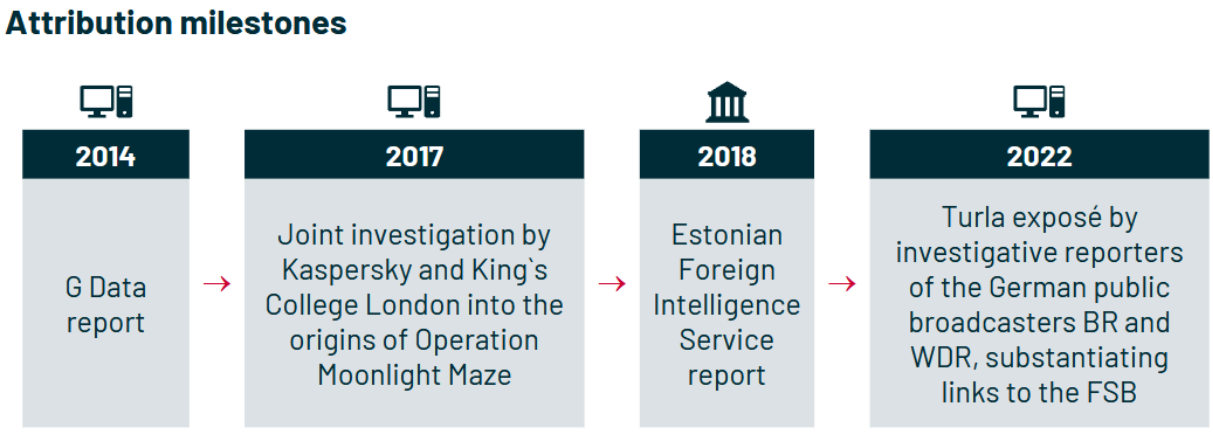


Fig. 1: Attribution Milestones for TURLA operations. Source: [14]

Evidence from the attack against the smaller CHP, reported in August 2026 by the Polish CERT, suggests that the attackers used new sophisticated techniques, acquiring tacit knowledge from persistent reconnaissance operations in mid-December before initiating destructive action on 29 December [32], [33]. Unlike other Russian APTs, Turla had not been associated with destructive operations in the past. Instead, the group reportedly previously focussed on espionage operations in the energy sector and other critical infrastructure targets [15]. However, whether this turn towards disruption was by design or by opportunity remains an open question.

Against this backdrop, we argue that Turla may have expanded its operational profile with this operation, thereby moving closer to the attack profiles of other Russian state-affiliated APTs such as Sandworm. The potential shift in Turla's operational profile has left some analysts guessing whether bureaucratic politics, the jockeying for the Kremlin's favour, or the growing success of Poland's assistance to Ukraine has resulted in a notable conversion of Russia's state-affiliated activities towards a more aggressive and destructive attack pattern [16].

Both the unique sequence and duration of the attribution campaign in the aftermath of the 2025 Polish energy infrastructure campaign indicate that Poland's policymakers aimed to showcase their decisiveness toward countering Russia's hybrid threats. As EuRepoC data on public political attributions illustrates, most cyber attribution campaigns since 2000 have started with technical reports. In contrast, the said attribution campaign started with prompt political statements by senior Polish government officials. In the first phase of the attribution campaign, the Polish Minister of Digitalisation, Krzysztof Gawkowski, and the Minister of Energy, Milosz Motyka, disclosed the attack on 13 January 2026, describing it as the most severe attack on energy infrastructure in recent history [18]. Shortly thereafter, Polish Prime Minister Donald Tusk took center stage and declared on 15 January 2026 that "everything indicates that these attacks were prepared by groups directly linked to the Russian services" [6].

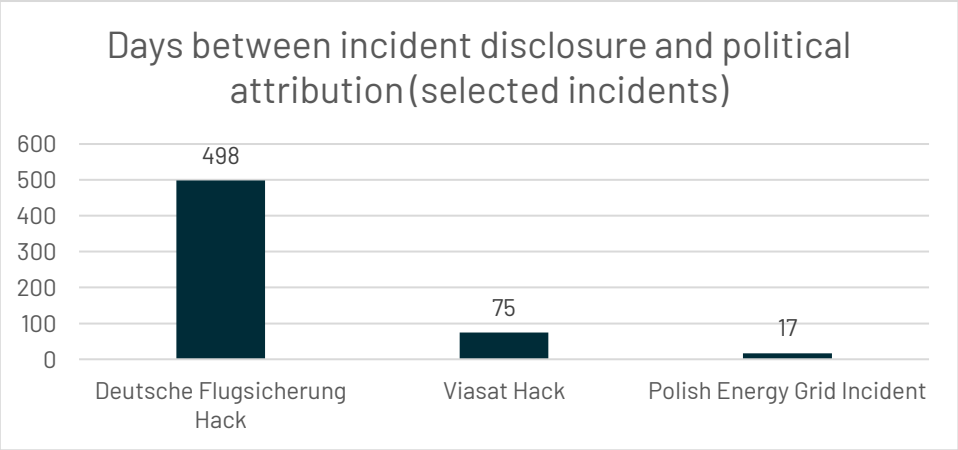


Fig. 2. Authors' illustration of data from source [17].

Additionally, the timeframe between incident detection and political attribution was notably short in comparison to previous incidents. Fig. 2 shows the duration of other attributions to Russian cyberattacks on critical infrastructure targets.

In the second phase, private CTI companies initiated the public technical attribution process. ESET attributed the attack to Sandworm with medium confidence on 23 January 2026 [7], while Dragos attributed it to a group with "overlapping technical capabilities" to ELECTRUM (aka Sandworm) with moderate confidence a few days later [8]. In contrast, the Polish CERT noted in a substantial technical report on 30 January that, while the malware contained similarities to Sandworm tools, the level of similarity was too low for definitive attribution. In turn, the agency determined in its 46-page report [4] that the technical evidence retrieved pointed more convincingly to an "activity cluster known publicly as 'Static Tundra' (Cisco), 'Berserk Bear' (CrowdStrike), 'Ghost Blizzard' (Microsoft), 'Dragon Fly' (Symantec)" [4, p. 36].

The prompt collusion of early political attributions by senior Polish government officials and the subsequent technical reports of major CTI companies were also highlighted by two separate (but coordinated) cybersecurity alerts from the US Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Center (NCSC) [19], [20].

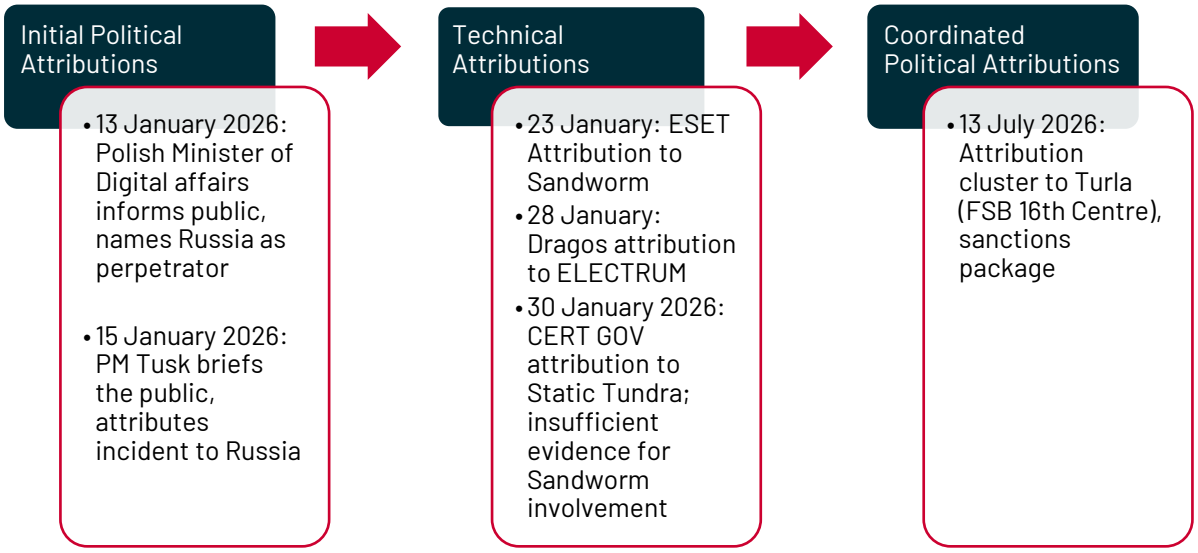


Fig. 3: Three stages of attribution. Authors' conceptualisation.

In the third wave of attributive actions, a cluster of countries issued coordinated responses. On the one hand, the European Union and the United Kingdom launched their first joint cyber sanctions package, which is said to be aimed at "the Russian state's persistent and increasingly reckless attempts to sow chaos and division across Europe." Notably, the package officially attributes the Polish energy infrastructure attack to the FSB Centre 16 (aka Turla), with the EU sanctioning nine individuals and four entities. Moreover, several EU partners and candidate countries (Albania, Bosnia and Herzegovina, Iceland, Moldova, Montenegro, North Macedonia, Norway, and Ukraine) aligned themselves with the EU's statement [5], [21]. While invoking Turla slightly deviates from the original attribution by the Polish CERT to Berserk Bear (aka Static Tundra), the latter is also considered to be part of the FSB Centre 16 [10].

Individual states, among them Germany and France, summoned their respective Russian ambassadors to protest Russian behaviour diplomatically [22]. In a related move, the Russian Foreign Ministry denied all allegations of involvement, with spokeswoman Maria Zhakharova stating that no evidence was given to back up these claims [23]. Moreover, several Russian diplomats insisted that Russia had always advocated the peaceful use of cyberspace [24].

In a related fourth move, the Polish CERT issued a second technical report on 8 August 2026, detailing a sophisticated attack targeting a second, smaller CHP. The attack happened in sync with the overall operation, but maintenance staff first deemed the turbine and water treatment shutdown as technical failures, reporting them informally as such. The Polish CERT, already aware of the other attacks, then started an investigation, which, after several months of intense scrutiny, led to the second technical report. While the report itself did not attribute this second CHP attack to Turla,

it presented circumstantial evidence to suggest that this attack was conducted in coordination with the attacks on the 30 solar and windfarms and the first CHP [32].

Technical details

The first report by the Polish CERT and subsequent technical analysis provide substantial evidence of the three related attacks, their access modes, sequencing, TTPs, and subsequent identification [4]. The forensics retrieved suggest (so far) that one single actor, Turla, assaulted three different systems: a collection of wind and solar farms, a private manufacturing company, and a combined heat and power plant for destructive purposes on 29/30 December, following an initial phase of reconnaissance and espionage starting in March 2025 [4, p. 12].

In the case of the wind and solar farms, a grid connection point (GCP) was compromised (where voltage transformation takes place and where the distribution system operator [DSO] monitors and controls operations). The attack vector comprised of FortiGate devices in each of the approximately 30 solar and wind facilities, serving as VPN concentrators and firewalls, all of which were exposed to the internet and lacked proper two-factor authentication. The analysis showed that some of these FortiGate devices had been vulnerable for longer time periods and that some of these devices, apparently belonging to the same operating company, used similar account names and passwords [4, pp. 5–7].

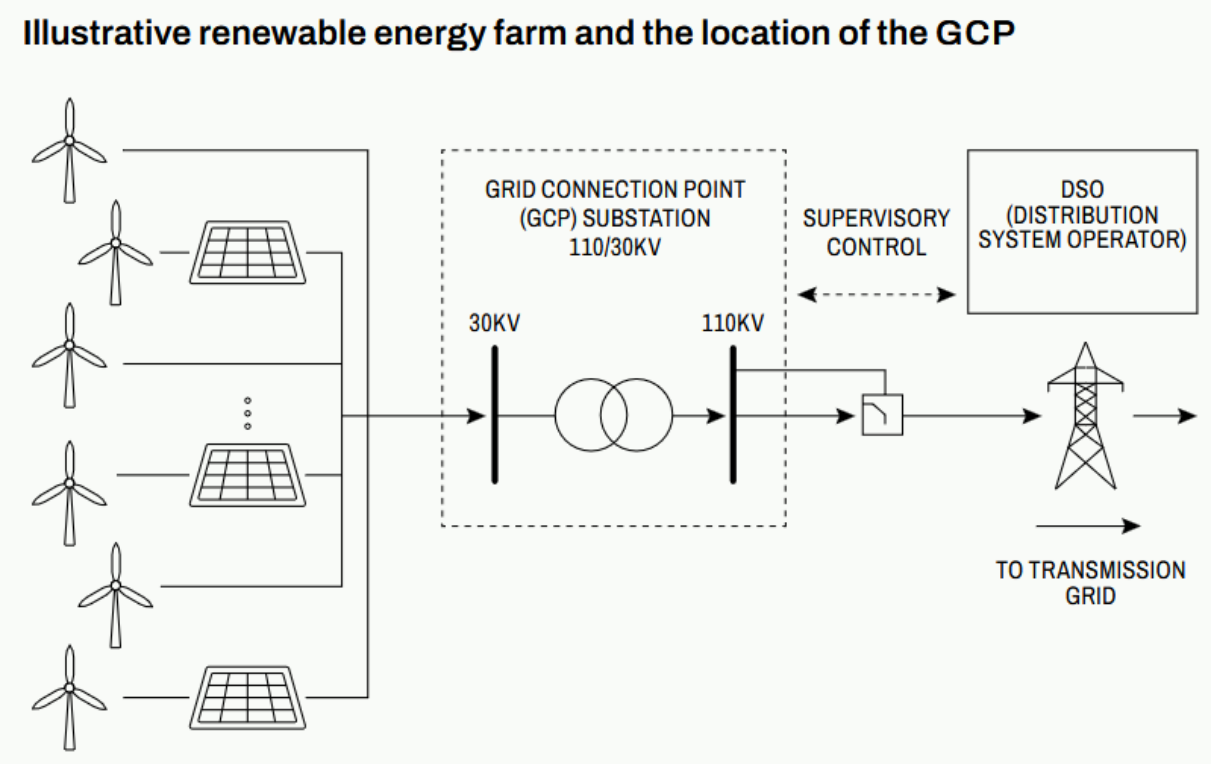


Fig. 4: Taken from [4, p. 6]

Destructive action, then, proceeded through remote terminal units (RTUs) of different firms (Hitachi, Mikronika), using modified firmware to introduce invalid instructions, thereby sending the devices into a reboot loop. At two facilities, the attacker also disabled protection and control relays by deleting essential files for operation [4, pp. 8–9].

At the first CHP, access to privileged accounts in the Active Directory domain was gained to distribute wiper malware through group policy objects (GPOs), but the endpoint detection response (EDR) solution installed by the CHP company recognised suspicious activities and blocked them [4, p. 20].

In a related move, a manufacturing sector company was targeted on 29 December, using similar TTPs. A Fortinet perimeter device was penetrated and two scripts were introduced for credential exfiltration and the modification of security settings. These were used to establish an SSL-VPN tunnel to distribute wiper malware dubbed "LazyWiper" through a GPO solution. The attacker also used the obtained credentials to access cloud services to retrieve files and email messages on OT work modernisation, SCADA system configuration and operation, and other technical operational data [4, pp. 24–26].

Interestingly, two types of wiper malware were used in these attacks which could not be attributed to any previously-known malware family. Detailed technical analysis of the malware suggests significant sophistication, e.g., the corruption of small portions of data to maximise speed or the skipping of certain system directories to keep the system stable while corrupting data for eventual rebooting in order to maximise impact [25].

The second report by the Polish CERT describes a sophisticated attack against a second, smaller CHP on 29 December, which caused a temporary shutdown of a steam turbine and the water treatment system, even if heat and electricity supply remained unhampered [32].

Assuming a common perpetrator, this additional operational route is important for several reasons. First, the delayed reporting on the disruption and the subsequent incident identification has important regulatory implications. Originally, responsible CHP operators believed that the incident was caused by a technical malfunction due to an error made by contracted engineers, rather than the result of malicious activities by third party actor(s). Subsequent CHP reporting on the unexplained failure then led to a comprehensive investigation by the Polish CERT uncovering the nexus to the related attacks [33]. Thus, statements by Polish authorities stressed the importance of reporting unexplained failures and operational disruptions, even if more circumscribed reporting requirements set out by the European Union's NIS2 law suggest otherwise [33].

Second, the disruption at the second CHP further substantiates the technical sophistication of the operation. While gaining initial access through traditional means (a perimeter device at a wind farm), the attacker then leveraged a Teltonika RUTX50 cellular router creatively to use a SHH service as a tunnel to communicate with an APN network to attack a WAGO PFC 200 controller. This move, in turn, enabled access the OT system of the CHP plant in mid-December 2025 [32: p.8-13]. Private APNs are often used as

proprietary mobile networks in industrial control systems or in large machine fleets to enable machines to communicate with each other. APNs are considered a secure alternative — for example, compared to VPN solutions — because data traffic is isolated from the public internet.

TTPs during the destruction phase at the second CHP involved access to Siemens PLCs and Moxa device servers and to network switches on 29 December: the attacker connected to Siemens PLCs, turned them to “stop” mode, and reset a password to prevent operators from changing the controllers’ operating state(s) and control logic(s), causing the shutdown of steam turbine and water treatment systems. The CERT report foregrounds that, like at the other renewable energy facilities involved, the restoration of factory settings and subsequent changes in login and IP addresses strengthened the assumption of responsibility to the same perpetrator [32], [34].

Timeline

March – May 2025	Initial Access & Espionage
July 2025	Lateral expansion & gaining tacit knowledge
Late 2025	Reconnaissance, credential theft & data access
8 December 2025	Expansion of access: gaining of administrative shares
18 December 2025	Access to second CHP plant gained, access expanded
21-22 December 2025	Further reconnaissance activity
25 December 2025	Network scanning and login attempts at all facilities with Mikronika RTUs in use
29 December 2025	Wipers employed: disruption attempt at both CHPs
13 January 2026	Minister of Digital Affairs informs public about the incident, names Russia as culprit
15 January 2026	PM Tusk briefs the public, attributes to Russia
23 January 2026	ESET analysis of DynoWiper: attribution to GRU-linked Sandworm
28 January 2026	Dragos intel brief: attribution to ELECTRUM with moderate confidence
30 January 2026	Polish CERT: attribution to FSB 16th Centre-linked Static Tundra; insufficient evidence for Sandworm involvement
06 February 2026	Elastic Security Labs analysis
10 February 2026	CISA Alert
13 July 2026	EU, UK & Allies: attribution cluster to Turla (FSB 16th Centre), sanctions package
08 August 2026	Follow-up analysis on second CHP by CERT-PL

Sources: [4], [5], [6], [7], [8], [18], [19], [25]

Enablers

In this case, there is substantial public evidence indicating that recurring vulnerabilities and risk drivers were present in the systems attacked.

First, key enablers were internet-exposed remote access and weak authentication which significantly increased the probability of initial access [4, p. 7], [19]. Secondly, evidence from attacks on solar and wind facilities suggests that password reuse and weak account management (i.e., reuse of default credentials) across different facilities of the same company created significantly expanded exposure. Thirdly, OT and IT systems featured both weak configuration governance and default accounts. These security lapses enabled destructive actions against remote terminal units, relays, etc., and related grid-connection components [4]. Fourth, to degrade forensic capacity and premediated recovery time, attackers tampered with factory-reset perimeter devices. Finally, the attackers often moved laterally at will because inadequate network zoning and limited containment boundaries between IT and OT broadened the exposure once perimeter access had been achieved [8].

In the case of the second, smaller CHP, the intrusion started on a Fortinet VPN and an internet-connected firewall device located at a wind farm. The attackers then identified a Teltonika cellular router on the same network and accessed its admin interface. An SSH service running on that device was then used to establish a tunnel that enabled communication to a private APN network managed by the distribution system operator (DSO). The attacker scanned the private APN network and identified a Wago programmable logic controller running at a CHP plant. An SSH service enabled on this controller gave the attackers access to the plant's operational technology networks. This way, the intruders were able (presumably for the first time) to leverage an APN network, previously believed to be a secure alternative to VPNs, as they are separate from the public internet [32], [35].

The second CERT report thus concludes that "execution was made possible, among other factors, by a misconfiguration that allowed connections to be established between arbitrary devices within the private APN network." Offering a stern warning, it adds: "Based on surveys conducted with multiple entities using this type of solution, it was determined that such a configuration was commonly encountered in Poland at the time the surveys were carried out. To the best of our knowledge, similar configurations are also widely deployed in other countries around the world" [32, p. 16].

Private Sector Engagement

- ESET: attribution and reporting
- DRAGOS: attribution and reporting
- Elastic Security Labs: Reporting

Legal Assessment

On 26 May, Poland's Permanent Representative to the UN stated in a Security Council debate that Poland had been a victim "of violations of the Charter and of fundamental principles of international law," citing (not further specified) hybrid and cyberattacks by Russia [28]. In addition, on 13 July 2026, Poland's Ministry of Foreign Affairs referred to Russia's cyber activities when giving reason for imposing sanctions against "malicious actions violating international law as well as established norms of responsible state behaviour" [29]. However, neither the Polish statements nor the respective EU, NATO, UK, or US announcements offered detailed legal assessments.

Several governments, as well as EU and NATO institutions, have subsequently commented on the Polish energy infrastructure incident, which had been singled out earlier by senior Polish officials as a "substantial escalation" of hybrid warfare practices against Poland. In July 2026, nearly 40 countries, including EU and NATO Member States, attributed the responsibility for the attack to Russian actors [5], [9].

While no other country identified spillover effects from the attack, the respective EU and NATO statements called upon the Russian government to stop its "disregard of agreed international norms of responsible state behavior in cyberspace" by leveraging its cyber ecosystem to target NATO and EU members. The EU statement specifically mentioned previous malicious behaviour by the Russian FSB and the military intelligence service (GRU), including through proxies such as Turla, against EU Member States and Ukraine, while justifying restrictive measures against nine individuals and four institutions. Notably, and in a related responding move, the EU and UK, after formally starting the EU-UK Cyber Dialogue in 2023, agreed upon their first joint cyber sanctions package against Russian threat actors [21], [27]. The UK's statement spoke of "reckless behaviour" and stated that "Britain will continue to call out this behaviour, bolster our resilience and respond to the hybrid threat posed by the Russian state. This will not deter us from supporting Ukraine" [21].

Restrictive measures against individuals and organisations that are held responsible for malicious cyber behaviour, e.g., in the form of economic sanctions, are deemed legitimate and necessary in both the European Union and the United Kingdom. However, the respective willingness and capacity to impose costs on state and non-state actors, such as Sandworm, Turla, or the Russian government itself, varies considerably [27].

In the post-Brexit UK, cyber-related economic sanctions have been imposed on more than 100 individuals and 20 entities since the establishment of the cyber sanctions regime, focussing on targeting the enabling digital ecosystem, such as protected hosting or cloud services [21], [27]. In the UK, the Foreign, Commonwealth and Development Office (FCDO) holds respective attribution and sanction competences, facilitating faster and more forceful implementation of asset freezes and other financial sanctions.

In the EU, in turn, the competence for legal attribution still lies with Member States, even though the EU High Representative (now) regularly makes (political) attribution statements, which may then be backed up by the EU's cyber sanctions regime under the EU Cyber Diplomacy Toolbox [30]. This split of competencies, in conjunction with other

factors, such as lacking technical capacity, the hesitancy to share sensitive intelligence, or the political considerations concerning perpetrators, have hampered the EU's ability to respond more frequently (and more robustly) against cyberattacks [31].

Domestically, the Polish legal response primarily comprised of preventative (NIS 2 directive transposition) and administrative measures (ad-hoc technical guidelines and recommendations), yet no public information regarding potential criminal investigations has been published. Internationally, Poland's legal action was multilateral and European, rather than unilateral and on a national level.

Sources

[1] É. Marzolf, A. Roussi, J. Loesel, and S. Clark, "EU sanctions Russian cyber spies for years-long hacking," POLITICO, Jul. 13, 2026. Accessed: Aug. 11, 2026. [Online]. Available: https://www.politico.eu/article/eu-sanctions-russian-cyber-spies-for-years-long-hacking/

[2] "Incident details: Russia's FSB 16th Centre aka Turla Carried Out Sabotage Operations Against Polish Energy Infrastructure on 29 and 30 December 2025," EuRepoC: European Repository of Cyber Incidents. Accessed: Aug. 11, 2026. [Online]. Available: https://eurepoc.eu/table-view/

[3] "2025 Poland Wiper Attacks, 2025 Poland Wiper Campaign, Campaign C0063," MITRE ATT&CK. Accessed: Aug. 11, 2026. [Online]. Available: https://attack.mitre.org/campaigns/C0063/

[4] CERT Polska, "Energy Sector Incident Report – 29 December," Ministry of Digital Affairs of the Republic of Poland, Jan. 2026. [Online]. Available: https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf

[5] "Cyber / Russia: Statement by the High Representative on behalf of the European Union denouncing Russia's malicious cyber ecosystem targeting the EU, its member states and international partners," Consilium. Accessed: Jul. 19, 2026. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/

[6] "Poland Stops Cyberattacks on Energy Infrastructure - The Chancellery of the Prime Minister - Gov.pl website," The Chancellery of the Prime Minister. Accessed: Jul. 23, 2026. [Online]. Available: https://www.gov.pl/web/primeminister/poland-stops-cyberattacks-on-energy-infrastructure

[7] "ESET Research: Sandworm behind cyberattack on Poland's power grid in late 2025," welivesecurity. Accessed: Jul. 23, 2026. [Online]. Available: https://www.welivesecurity.com/en/eset-research/eset-research-sandworm-cyberattack-poland-power-grid-late-2025/

[8] D. Gauthier, "Poland Power Grid Attack Targets Distributed Energy Facilities," Dragos. Accessed: Aug. 11, 2026. [Online]. Available: https://www.dragos.com/blog/poland-power-grid-attack-electrum-targets-distributed-energy-2025

[9] "Statement of condemnation by the North Atlantic Council of Russia's malicious cyber activities," Official texts and resources | NATO. Accessed: Aug. 11, 2026. [Online]. Available: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/13/statement-of-condemnation-by-the-north-atlantic-council-of-russias-malicious-cyber-activities

[10] "Russia's FSB malign activity: factsheet," Foreign, Commonwealth & Development Office. Accessed: Aug. 11, 2026. [Online]. Available: https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

[11] A. Olech, J. Smoleń, and A. Wojciechowska, "Poland as a target of Russian hybrid attacks," Defence24. Accessed: Aug. 11, 2026. [Online]. Available: https://defence24.com/geopolitics/report-poland-as-a-target-of-russian-hybrid-attacks

[12] C. Ciobanu, "Poland faced surge in cyberattacks in 2025 including energy sector assault," AP News, Mar. 24, 2026. Accessed: Aug. 11, 2026. [Online]. Available: https://apnews.com/article/poland-cyberattacks-2025-energy-system-russia-57ebc6e1c67654586c21f0936faa47d1

[13] J. Huismans, R. Lucas, O. Palicka, S. Winder, and E. Silfversten, "Poland's Digital Defence Landscape: Lessons from Polish investment in digital capabilities for defence," Rand Corp, Jan. 2026. Accessed: Aug. 11, 2026. [Online]. Available: https://www.rand.org/pubs/research_reports/RRA3831-6.html

[14] K. Zettl-Schabath, T. Gschwend, and C. Borrett, "Advanced Persistent Threat Profile: Turla." EuRepoC, Heidelberg, Dec. 2022. [Online]. Available: https://eurepoc.eu/wp-content/uploads/2023/07/Turla-EN.pdf
[15] S. Sharma, "Examining the Activities of the Turla APT Group," Trend Micro. Accessed: Aug. 11, 2026. [Online]. Available: https://www.trendmicro.com/en_gb/research/23/i/examining-the-activities-of-the-turla-group.html
[16] A. Petriczko, "Who Was Behind the Largest Cyberattack on Polish Energy Infrastructure in Years?," Balkan Insight. Accessed: Jul. 21, 2026. [Online]. Available: https://balkaninsight.com/2026/02/26/who-was-behind-the-largest-cyberattack-on-polish-energy-infrastructure-in-years/rd/
[17] K. Zettl-Schabath et al., "Global Dataset of Cyber Incidents." European Repository of Cyber Incidents, Mar. 04, 2025. doi: 10.5281/ZENODO.14965395.
[18] E. Kliszcz, "Russian cyberattacks tried to cause blackout in Poland, minister says," TVP World. Accessed: Aug. 11, 2026. [Online]. Available: https://tvpworld.com/91021372/polish-minister-russia-behind-massive-energy-cyberattacks
[19] "Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps," CISA. Accessed: Aug. 11, 2026. [Online]. Available: https://www.cisa.gov/news-events/alerts/2026/02/10/poland-energy-sector-cyber-incident-highlights-ot-and-ics-security-gaps
[20] J. Ellison, "Cyber attacks disrupt critical infrastructure: UK operators must act now." Accessed: Aug. 11, 2026. [Online]. Available: https://www.linkedin.com/posts/jonathon-ellison-obe_how-to-prepare-for-and-plan-your-organisations-activity-7426569749402132480-XG1v/
[21] Y. Cooper, "UK and EU strike Russian cyber networks with new sanctions," GOV.UK. Accessed: Jul. 23, 2026. [Online]. Available: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions
[22] "EU, UK slap sanctions on Russian spies and hackers over cyberattacks," France 24. Accessed: Aug. 11, 2026. [Online]. Available: https://www.france24.com/en/europe/20260713-eu-and-uk-slap-sanctions-on-russian-spies-and-hackers-over-cyberattacks
[23] "Europe groundlessly accuses Russia of 'malicious activity' in cyberspace — diplomat," TASS. Accessed: Jul. 23, 2026. [Online]. Available: https://tass.com/politics/2161727
[24] "Russian permanent mission accuses EU of making unfounded public accusations against Moscow," TASS. Accessed: Jul. 23, 2026. [Online]. Available: https://tass.com/politics/2160231
[25] "DYNOWIPER: Destructive Malware Targeting Poland's Energy Sector," Elastic Security Labs. Accessed: Aug. 11, 2026. [Online]. Available: https://www.elastic.co/security-labs/dynowiper
[26] "Poland Energy Sector Incident (Dec 2025)| OT/ICS Attack Analysis & Controls," DENEXUS. Accessed: Aug. 11, 2026. [Online]. Available: https://www.denexus.io/poland-energy-sector-incident-december-2025
[27] P. Lausberg, "Cyber sanctions: Strengthening EU-UK responses to escalating threats." EPC, Mar. 17, 2026. [Online]. Available: https://d1xp398qalq39s.cloudfront.net/uploads/ckeditor/2026/03/19/eu-uk-cybersanctions-pb-v3.pdf
[28] K. Szczerski, "Poland participates in the UN Security Council briefing on multilateralism," Poland in the UN. Accessed: Aug. 11, 2026. [Online]. Available: https://www.gov.pl/web/un/poland-participates-in-the-un-security-council-briefing-on-multilateralism
[29] "Statement on Russian malicious activities in cyberspace," Ministry of Foreign Affairs. Accessed: Aug. 11, 2026. [Online]. Available: https://www.gov.pl/web/diplomacy/statement-on-russian-malicious-activities-in-cyberspace

[30] Y. Miadzvetskaya, "EU sanctions in response to cyber-attacks as crime-based emergency measures," Comput. Law Secur. Rev., vol. 54, p. 106010, Sep. 2024, doi: 10.1016/j.clsr.2024.106010.
[31] K. Zettl-Schabath, B. Ibralic, S. Drick, I. Villalva Gándara, and M. Parer, "More Thoughts, More Words, Different Actions?: The EU's Application of the Cyber Diplomacy Toolbox, Part II." EuRepoC, Heidelberg, May 2025.
[32] CERT Polska, "Follow-up Analysis of the 29 December 2025 Energy Sector Incident," Ministry of Digital Affairs of the Republic of Poland, August 2026. [Online]. Available: https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Follow_up_Report_2025.pdf
[33] Alexander Martin, "Poland Uncovers second heat plant cyberattack that went hidden for moths, August 10, 2026, https://therecord.media/poland-uncovers-critical-infrastructure-attack-hidden?mkt_tok=Njc4LUZITC03MTAAAAGjjm73nqH_YInUK_aY4-HJBR8qZC0VSlQhr58OysOmPPFnZKKr6cSgPk7WV38iSV8jCG_eOMxHcNdsRGpElFhDM4NS017aE0gCgigPV54
[34] Bill Toulas, "Hackers breached a small Polish energy plant via private APN last year", August 10, 2026, https://www.bleepingcomputer.com/news/security/hackers-breached-a-small-polish-energy-plant-via-private-apn-last-year/
[35] Swati Khandelwal , „Hackers Breach Polish Power Plant Controls via Private Cellular Network and Shut Turbine", August 11th, 2026, https://thehackernews.com/2026/08/hackers-breach-polish-power-plant.html
[36] Ministerstwo Cyfryzacji, Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa zaczyna obowiązywać, 02.04.2026, https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-zaczyna-obowiazywac

Table of Technical terms

RTU / Remote Terminal Unit	An **RTU** is a computer with radio interfacing used in remote situations. Typically collects measurement data and controls remote plant components.
PLC / Programmable Logic Controller	A **PLC** executes automated control logic.
Protection relay	A **protection relay** responds to electrical fault conditions and can shut down equipment.
GCP / Grid Connection Point	A **GCP** refers to a physical or logical interface between a generation facility and the power grid.
DSO / Distribution System Operator	A **DSO** monitors and controls distribution networks.