applied sciences

MDPI

Review

Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation

Doney Abraham [1,*,†], Siv Hilde Houmb [1,2,†] and Laszlo Erdodi [1,3,†]

[1] Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology, 2815 Gjøvik, Norway; siv.houmb@ntnu.no (S.H.H.); laszlo.erdodi@ntnu.no (L.E.)
[2] Norwegian Defence Cyber Academy, Norwegian Defence University College, 2617 Lillehammmer, Norway
[3] Department of Informatics, The Faculty of Mathematics and Natural Sciences, University of Oslo, 0315 Oslo, Norway
* Correspondence: doney.abraham@ntnu.no; Tel.: +47-95081340
† These authors contributed equally to this work.

Abstract

Advanced Persistent Threats (APT) are stealthy multi-step attacks, often executed over an extensive time period and tailored for a specific attack target. APTs represent a "low and slow" type of cyberattack, meaning that they most often remain undetected until the consequence of the attack becomes evident. Energy infrastructure, including power grids, oil and gas infrastructure, offshore wind installations, etc., form the basis of a modern digital nation. In addition to loss of power, financial systems, banking systems, digital national services, etc., become non-operational without electricity. Loss of power from an APT cyberattack could result in loss of life and the possibility of creating digital chaos. Digital payments becomes unavailable, digital identification is affected, and even POS terminals need to run on emergency power, which is limited in time, resulting in challenges in paying for food and beverages. Examples of Advanced Persistent Threats (APTs) targeting energy infrastructures include Triton, which in 2017 aimed to manipulate the safety systems of a petrochemical plant in Saudi Arabia, potentially leading to catastrophic physical consequences. Another significant incident is the Industroyer2 malware attack in 2022, which targeted a Ukrainian energy provider in an attempt to disrupt operations. The paper combines APT knowledge with energy infrastructure domain expertise, focusing on technical aspects while at the same time providing perspectives on societal consequences that could result from APTs.

Keywords: energy infrastructure; cyber-security; cyberattacks; APT; power grid; smart grid; petroleum; oil and gas; offshore wind; SCADA; ICS; IACS

check for updates

Academic Editors: Jakub Szyguła, Dariusz Marek, Krzysztof Bernacki and Grzegorz Tytko

Received: 10 July 2025
Revised: 7 August 2025
Accepted: 14 August 2025
Published: 22 August 2025

Citation: Abraham, D.; Houmb, S.H.; Erdodi, L. Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation. *Appl. Sci.* **2025**, *15*, 9233. https://doi.org/10.3390/app15179233

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cyber-attacks have increased in both in intensity and in sophistication over the last decades. Additionally, cyberattacks have become targeted, such as the Ukraine power grid attacks in 2015, 2016, and 2017, and in some cases have been used as part of offensive cyberspace operations, e.g., the Russian invasion of Ukraine in 2022. In fact, in the Allied Joint Doctrine for Cyberspace Operations [1] NATO has defined cyberspace as a separate operational domain in addition to maritime, air, space, and land. Cyber threats to the stability and security of the Alliance are complex, destructive, and coercive, and are becoming ever more frequent [2]. Due to the current geo-political situation, the Alliance has decided

to establish the NATO Integrated Cyber Defence Centre (NICC) to enhance the protection of NATO and Allied networks and better coordinate the use of cyberspace as an operational domain. The Center will inform NATO military commanders on possible threats and vulnerabilities in cyberspace, including privately-owned civilian critical infrastructures necessary to support military activities. The Center is one of several measures intended to strengthen the coordination between civilian and military entities as part of the total defense concept.

Modern societies rely on the availability of critical infrastructures to operate efficiently. This is of major concern both for the Alliance as well as for the European Union (EU) and the European Commission (EC). Energy infrastructures is part of those sectors defined as critical infrastructures, in particular national power grids, including transmission, distribution, and production. For Europe this is defined in the EU directives: NIS2 [3], and Critical Entities Resilience Directive—CER [4], as well as in the transposition of these directives into national law. These directives and relevant national laws and best practices are in place to provide better resilience against advanced cyberattacks such as Advanced Persistent Threats (APTs). These advances in cyber resilience are a response to the sabotage of the Nord Stream pipelines in 2022, which demonstrated how energy, digital infrastructure, transportation and space depend on resilient critical infrastructure and how interlinked the external and internal dimensions of a nation's security are. Although most petroleum installations are not covered under the CER directly, some of these are critical assets as well and are critical to the well-being of the EU and its citizens, such as natural gas installations and pipelines.

This paper provides an overview of APTs and other sophisticated cyberattacks on energy infrastructures covering the power grid and petroleum sectors along with an evaluation of the consequence of these cyberattacks on the specific systems being attacked, the sector itself, and the potential wider societal impacts.

This study adopts a targeted literature overview rather than a formal systematic literature review (SLR). The aim was to compile documented successful cyber-attacks on petroleum and power grid infrastructures during the 2010–2023 period and contextualize them using recognized cybersecurity frameworks, such as MITRE ATT&CK for ICS, IEC 62443, and the NIST Cybersecurity Framework. Sources were identified through targeted searches in IEEE Xplore, Web of Science, Scopus, and SpringerLink, as well as authoritative incident reports from government agencies, industry consortia, and security vendors.

From the search results, incidents were included if they met the following criteria:

- Represented a successful, publicly documented cyber-attack on petroleum or power grid sectors.
- Occurred between 2010 and 2023.
- Contained sufficient technical detail to map at least partially to the MITRE ATT&CK for ICS framework.
- Originated from credible, verifiable sources such as peer-reviewed studies or official investigation reports.

This scope ensured that the literature reviewed remained focused on high-impact, verifiable cases relevant to the study objectives.

The main contributions of the paper are as follows:

- Overview of cyberattacks on power grids, especially APTs, including those involved in the war in Ukraine.
- Overview of cyberattacks on petroleum installations, including an evaluation of potential societal impacts based on the current geopolitical situation.
- Discussion of the potential societal impacts of APTs and sophisticated cyberattacks on power grids and petroleum installations.

Recent literature has also examined cyber-threats in emerging smart infrastructure domains that extend beyond traditional ICS and energy sectors. For example, researchers have proposed a hybrid optimization framework for minimizing the age of information in UAV-assisted mobile crowd sensing (MCS), in order to improve real-time data freshness and system resilience [5]. Likewise, federated deep reinforcement learning (FDRL) techniques have been explored to mitigate cyber-threats targeting electric vehicle (EV) charging systems in next-generation wireless power transfer (WPT) environments [6]. Although these areas differ from the operational technology focus of this work, they reflect the growing diversification of critical infrastructure attack surfaces and underscore the importance of cross-domain defense strategies.

The rest of this paper is organized as follows: Section 2 provides background on the power grid and petroleum sectors; Section 3 presents a structured overview of cyberattacks and Advanced Persistent Threats (APTs) targeting the petroleum industry, while Section 4 examines cyberattacks on power grid installations. Section 5 provides an in-depth examination of documented real-world cyberattacks on petroleum and power grid infrastructures, mapping each case to MITRE ATT&CK for ICS tactics and techniques to highlight their evolution in sophistication, objectives, and operational impact. Section 6 introduces a comparative analysis of technical pathways used in cyberattacks on the petroleum and power grid sectors. Section 7 analyzes trends in attack evolution through MITRE ATT&CK for ICS mappings, pattern shifts, and associated mitigation strategies. Section 8 discusses potential societal impacts of these cyberattacks and outlines directions for future work, particularly on enhancing detection capabilities in such installations.

2. Energy Infrastructures and Their Subsystems

2.1. Petroleum Industry

The petroleum industry covers the supply chain involved in exploration, extraction, refining, transportation (often by oil tankers and pipelines), and marketing of petroleum products [7]. This industry is often referred to as Oil and Gas, and its core products are fuel oil, petrol, and gas. The industry spans an upstream, midstream and downstream; upstream includes exploration and extraction of crude oil, midstream encompasses transportation and storage of crude oil, and downstream concerns refining crude oil into various end products.

Industrial Automation and Control Systems (IACS) are used for many purposes in the petroleum industry, such as controlling heavy machinery, e.g., production tanks on offshore production platforms and topdrives on a drilling rig. IACS are also used to manage various processes to ensure that production remains in line with Health, Safety, and Environmental (HSE) regulations. An example of such is the need to manage downhole pressure in order to prevent blowouts, such as the one experienced on the Macondo oil field in the Gulf of Mexico in 2010, when the Deepwater Horizon exploded [8].

2.2. Power Grid

The power grid covers the production, transmission, distribution and consumption of electrical power [9]. Production sites include hydropower, wind power, solar, nuclear, etc. Production sites connect to the transmission network, which is comprised of a network of high voltage (125 kV and higher) power lines. Within Europe, there are more than 40 transmission operators; and these are organized into the European Network of Transmission System Operators (ENTSO-E) to support the need for coordination across the European power grid. Distribution lines are regional power line networks that are in charge of stepping down voltage levels to enable safe delivery into manufacturing sites, office buildings, households, etc. In cases where consumers are also producing electricity that is provided to the distribution grid, these consumers are called prosumers. The power grid is supported

by substations that are capable of stepping down or stepping up the voltage depending on the location and purpose of the substation. Substations are equipped with primary and secondary systems to connect power lines together and to manage the grid. Primary systems include circuit breakers, power meters, busbars, etc., while secondary systems include protection relays, remote terminal units, gateways, IEDs, etc. Primary systems are managed by the secondary system, also known as the substation control system. This management was earlier performed using peer-to-peer proprietary communication over copper cables; today digital substations makes use of fiber cables and modern international communication protocols, such as IEC 61850 [10].

3. Overview of Cyberattacks on the Petroleum Industry

The petroleum industry's role in ensuring energy supply to various sectors makes it a prime target for cyberattacks. As oil and gas operations become increasingly dependent on interconnected systems, adversaries have exploited vulnerabilities in these networks by targeting critical components and processes throughout the supply chain.

The oil and gas sector has traditionally been characterized by isolated Operational Technology (OT) systems. However, with the onset of Industry 4.0, these systems are becoming increasingly integrated with Information Technology (IT), enhancing efficiency and control but also expanding the attack surface [11]. This increase in interconnected devices and systems, including Supervisory Control and Data Acquisition (SCADA) systems and Internet of Things (IoT) devices, creates new vectors for cyberattacks. A notable example is the 2020 ransomware attack on a natural gas compression facility, which disrupted the control and communication assets of the facility's OT network [11,12]. This attack demonstrated how the convergence of IT and OT systems can lead to significant operational disruptions when targeted by malicious actors. In this incident, the attackers exploited vulnerabilities in the facility's OT systems, underscoring the pressing need for enhanced security protocols across both IT and OT environments.

Types of CyberAttacks Targeting Oil and Gas Systems

Cyberattacks on the petroleum industry range from ransomware and malware to Advanced Persistent Threats (APTs) [11]. Each attack type leverages different vulnerabilities, and the effects can range from data theft to full-scale operational disruptions.

- **Ransomware:** Ransomware attacks, such as the 2020 attack targeting a natural gas compression facility, are designed to encrypt critical systems and demand payment in exchange for decryption. These attacks are often indiscriminate, i.e., not explicitly designed to affect oil and gas systems, but can have profound consequences for operational continuity.
- **Malware and Phishing Attacks:** Malware and phishing attacks are often the entry points for more sophisticated breaches. Attackers may infiltrate networks via malicious emails or websites, using malware to move laterally through the system and target ICS environments. Phishing attacks, particularly those targeting employees with access to sensitive OT systems, remain among the most common methods adversaries use to gain initial access.
- **Advanced Persistent Threats (APTs):** APTs, typically associated with nation-state actors, are highly targeted and designed to remain undetected within the system for extended periods. These attacks focus on gathering intelligence, manipulating processes, or degrading the functionality of critical systems over time. APTs are particularly dangerous because they can be used to launch more devastating attacks at crucial moments, such as during geopolitical tension or economic crises.

Attackers often exploit insecure remote access, phishing, outdated firmware, and poor segmentation between IT and OT networks. The documented attacks in Table 1 exemplify how adversaries leverage such vulnerabilities.

Although the petroleum sector has experienced attack types similar to those in other critical infrastructure—such as APT campaigns (e.g., Havex), ransomware, and supply chain compromises—their execution and impact are shaped by the industry's unique operational landscape. Offshore platforms, subsea production systems, and integrated drilling automation create long and complex supply chains with multiple vendor dependencies. Threat actors often focus on disrupting production schedules, interfering with safety instrumented systems, or gaining persistent access to logistics and exploration data rather than causing immediate grid-wide physical effects. The sector's dependence on remote monitoring and vendor-managed systems increase its exposure to supply chain intrusions and remote service exploitation. As such, mitigation strategies prioritize vendor access governance, offshore-specific incident response planning, and redundant control pathways to maintain production continuity even during a cyber disruption.

Table 1. Summary of Documented Cyberattacks on Energy Infrastructures (2010–2023)

Attack Name/ Incident	Year	Targeted Infrastructure	Attack Methodology	Root Cause	Impact	Mitigation Measures	Lessons Learned
Stuxnet [13]	2010	Iranian Nuclear Facility	Malware (Worm)	Exploited zero-day vulnerabilities in Siemens PLCs	Physical damage to centrifuges, disrupting uranium enrichment	Regularly update and patch systems; implement network segmentation	Importance of securing industrial control systems (ICS) against sophisticated malware
Havex [14]	2013	Energy sector ICS (EU, US)	Remote Access Trojan via software supply chain	Compromised ICS software installers	Unauthorized access to ICS networks; potential data exfiltration	Verify integrity of software updates; monitor network traffic for anomalies	Vigilance in supply chain security; importance of monitoring ICS networks
Operation Cleaver [15]	2014	Global Energy Infrastructure	Advanced Persistent Threats	Exploited vulnerabilities in critical infrastructure systems	Unauthorized access to sensitive systems; potential for sabotage	Implement advanced threat detection; enhance system hardening	Importance of monitoring for APTs and securing critical infrastructure
Dragonfly (Energetic Bear) [16]	2014	Energy Sector (EU, US)	Malware (Havex RAT) via phishing and watering hole attacks	Compromised ICS software and websites	Unauthorized access to energy sector networks; potential data exfiltration	Regularly update and patch systems; monitor network traffic for anomalies	Vigilance in supply chain security; importance of monitoring ICS networks
BlackEnergy [17]	2015	Power Grid (Ukraine)	Malware (Trojan) delivered via phishing emails	Lack of employee cybersecurity training; inadequate email filtering	Power outage affecting 225,000 customers for several hours	Employee cybersecurity training; implement advanced email filtering	Need for comprehensive cybersecurity training and robust email security
Industroyer (CrashOverride) [18]	2016	Transmission Substations (Ukraine)	Malware targeting industrial communication protocols	Exploited specific ICS protocol vulnerabilities	Power outage in Kyiv for about an hour	Regularly update ICS protocols; implement intrusion detection systems	Importance of securing ICS protocols and continuous monitoring

Table 1. *Cont.*

Attack Name/ Incident	Year	Targeted Infrastructure	Attack Methodology	Root Cause	Impact	Mitigation Measures	Lessons Learned
Triton (Trisis) [19]	2017	Saudi Petrochemical Plant	Malware targeting safety instrumented systems (SIS)	Inadequate segmentation between IT and OT networks	Potential physical damage; plant shutdown	Network segmentation; monitor SIS for unauthorized changes	Criticality of securing SIS and enforcing strict network segmentation
Colonial Pipeline [20]	2021	U.S. Fuel Pipeline	Ransomware via compromised password	Use of a single-factor VPN password; lack of multifactor authentication	Pipeline shutdown causing fuel shortages in the Eastern U.S.	Implement multifactor authentication; regular password audits	Necessity of multifactor authentication and regular security assessments
Oldsmar Water Plant [21]	2021	Water treatment OT system	Remote access tool exploitation	Poor password security; lack of network segmentation	Attempted alteration of water chemical levels; thwarted by operator	Implement strong password policies; restrict remote access; monitor system activity	Criticality of securing remote access and monitoring ICS environments
Industroyer2 [22]	2022	Transmission Substations (Ukraine)	Malware targeting power substations with IEC 60870-5-104 protocol commands	Having access to the controlling station computer	Opening circuit breakers to cut the power	Prevent access to the controlling station and its network, prevent information disclosure regarding protocol level details (Information Object Addresses) and network level details (IP addresses)	IEC104 protocol is an easy target if the attacker has access to one of the endpoints. Network level information (IP addresses) and Protocol level information (Information Object Addresses) should have been better protected
FrostyGoop [23]	2023	Urban Heating Infrastructure (Ukraine)	Modbus-based device command manipulation	Unpatched MikroTik routers; exposed Modbus access	Disruption of heating services to 600 buildings for 48 h	Regularly update and patch network devices; monitor for unauthorized access	Regularly update and patch network devices; monitor for unauthorized access

4. Overview of Cyberattacks on the Power Grids Industry

Over the last decade, power grid systems have transferred into what today is known as the smart grid, with the consequence of legacy grid components being connected to networked smart grid components and consequently exposed to cyberattacks. This means that the island or isolation assumption breaks down and that legacy power grid components need to be patched and hardened in the same manner as new smart grid components. However, these legacy systems are designed to be dependable, and not necessarily to be cybersecure. It is sometimes not even possible to patch and update them; therefore, dated vulnerabilities may offer an opportunity for the attackers to pivot into and successfully execute a cyberattack, even if the system has been hardened in order to make it more complex to attack. Additionally, even if patches for dated vulnerabilities are available, the dependable nature of these systems is often such that they cannot endure volatility and frequent system changes. These heterogeneous system environments have already been exploited in multiple attacks.

The Stuxnet worm in 2010 is well known as the first Advanced Persistent Threat (APT) attack targeting Cyber–Physical Systems (CPS). Stuxnet targeted the Natanz nuclear facility [24], impacting almost one-fifth of Iran's nuclear centrifuges [25]. Another aspect of the Stuxnet attack was that it demonstrated the role of domain knowledge in ICS attacks. This means that motivated and capable adversaries can tailor and empower malware based on domain knowledge, allowing them exploit capabilities native to the system. The incident also opened up a geopolitical aspect to such attacks.

In 2011, the Laboratory of Cryptography and System Security (CrySyS) discovered the "Duqu" malware [26]. Duqu had similarities to Stuxnet, but had no payload and was not self-replicating. However, it utilized many of the same techniques as Stuxnet. Analysis has shown that Duqu's primary purpose was reconnaissance.

After the Russian annexation of the Crimean peninsula in 2014, there have been multiple cyberattacks on power grid installations in Ukraine, affecting grid operations of at least 30 substations [27,28]. The first cyberattack in December 2015 targeted the distribution level in the Kyiv area, affecting 225,000+ customers [29]. This attack made use of the BlackEnergy3 malware [30]. The attack used native power grid communication protocols such as IEC 104 as well as domain knowledge to take control over breaker operations while denying operators the ability to interact with the SCADA system [31]. Furthermore, the attackers demonstrated an understanding of operational procedures and were able to force the substation into shutdown. The second cyberattack was carried out on 17 December 2016. This time, a transmission-level substation in Kyiv was the target. The attack used the CrashOverride/Industroyer malware [32]. CrashOverride/Industroyer malware employs a similar approach to what was seen in the Stuxnet and Ukraine 2015 attacks by understanding and codifying domain knowledge of the industrial process to disrupt grid operation. According to [33], the CrashOverride/Industroyer malware is not unique to any ICS configuration or vendor, but leverages network communication and grid operation knowledge. For this reason, it represents a threat to power grid installations outside of the targeted substations.

A new variant of Industroyer appeared in February 2022, a few weeks prior to the Russian invasion of Ukraine. This malware very likely used the source code of the original Industroyer from 2016. Although the first version of Industroyer had a modular approach with modules for the different protocols (IEC 60870-104, OPC DA, etc.), the new version was purpose-built for the IEC60870-104 protocol, which is used to access power substations from the dispatch centers. Based on the available analyses, the malware was most likely created in a rush without including anti-reverse engineering techniques. Another important characteristic of this malware is its hardcoded network and OT parameters, such as IP addresses and Information Object Addresses (IOAs). The malware was created in different versions for the different targets, with each version only containing the necessary parameters for its target. These IP addresses and IOA addresses were most likely obtained in a previous phase of the attack based on prior network reconnaissance or insider provided information. Although the new variant included only the IEC60870-104 module, this module was seriously updated since 2016. The malware had general persistency and command and control techniques, but focused on interfering with and stopping the running of IEC104-related processes on the target computer. The purpose of these actions was to rebuild and control the IEC104 TCP connection and to change the state of the Information Object Addresses responsible for opening circuit breakers. As a result, the attackers were able to cause a temporary blackout by opening several circuit breakers.

In contrast to attacks on the petroleum industry, attacks on the power grid—such as BlackEnergy, Industroyer, Triton, and the Ukraine grid incidents — are characterized by objectives that can result in immediate, large-scale service disruption. ICS environments in

the power sector, including SCADA master stations, substation automation, and protective relay systems, are inherently interconnected, which means that localized incidents can escalate into cascading blackouts. Although some techniques overlap with those in petroleum (e.g., phishing, ransomware, and APT footholds), their operational execution often targets grid instability or load-shedding events, exploiting control commands within operational protocols (e.g., IEC 60870-5-104, DNP3). Consequently, mitigation priorities in the power grid emphasize real-time operational state monitoring, fail-safe automation for protective relays, and coordinated CERT-utility incident response to minimize outage duration and prevent uncontrolled cascading failures.

5. Attack Evolution Summary

This section provides an in-depth examination of the types of cyber-attacks that have affected the energy infrastructure domain focusing on petroleum and power grid, based strictly on documented real-world incidents listed in Table 1. This structured mapping demonstrates how attackers typically employ Initial Access (TA0108), Impact (TA0105), and Command and Control (TA0101) techniques to disrupt operations or exfiltrate sensitive information, and the evolution of their sophistication.

5.1. Stuxnet (2010) — Iranian Nuclear Facility

MITRE Tactics: Initial Access (TA0108); Execution (TA0104); Discovery (TA0102); Impair Process Control (TA0106); Inhibit Response Function (TA0107); Impact (TA0105)

MITRE Techniques: Exploitation of Remote Services (T0866); Hardcoded Credentials (T0891); Manipulation of Control (T0831); Manipulation of View (T0832); Modify Controller Tasking (T0821); Rootkit (T0851)

Evolution Summary: The first known ICS-specific malware, Stuxnet was a highly sophisticated state-developed cyberweapon. It combined multiple zero-day exploits, a Windows rootkit, and PLC logic manipulation to physically sabotage nuclear centrifuges. This 2010 attack set a new benchmark for complexity, showing unprecedented automation in targeting ICS devices and causing physical damage. It marked a shift from traditional IT attacks to direct interference in industrial processes, demonstrating that determined adversaries (likely nation-states) could achieve stealthy intrusion and tailored destruction in critical infrastructure.

5.2. Havex (2013) — Energy Sector ICS (EU, US)

MITRE Tactics: Initial Access (TA0108); Execution (TA0104); Discovery (TA0102); Collection (TA0100); Impact (TA0105).

MITRE Techniques: Spearphishing Attachment (T0865); Supply Chain Compromise (T0862); User Execution (T0863); Remote System Discovery (T0846); Point & Tag Identification (T0861); Denial of Service (T0814).

Evolution Summary: Havex, an ICS-focused Remote Access Trojan used by the Dragonfly/Energetic Bear group, exemplified a shift to broad espionage in industrial networks. It infiltrated targets via trojanized software updates and phishing emails, then scanned ICS protocols (OPC) to gather system data. Compared to Stuxnet, Havex was less about immediate destruction and more about widespread access and data collection, indicating adversaries expanding their foothold in critical systems with moderate sophistication. This 2013 campaign showed how attackers began leveraging supply chain attacks and vendor software compromises to reach industrial control environments at scale.

5.2.1. Operation Cleaver (2014)—Global Energy Infrastructure

MITRE Tactics: Initial Access (TA0001); Credential Access (TA0006); Lateral Movement (TA0008); Collection (TA0009).

MITRE Techniques: Adversary-in-the-Middle (T1557.002 – ARP Cache Poisoning); Custom Malware Development (T1587.001); Credential Dumping (T1003); WMI for Lateral Movement (T1047).

Evolution Summary: Operation Cleaver was a large-scale covert campaign (attributed to Iranian actors) targeting critical infrastructure worldwide. Active around 2014, the attackers focused on stealthy network intrusion and data exfiltration rather than immediate damage. They developed custom malware and tools for functions such as ARP cache poisoning, credential theft, and backdoors, displaying an evolving sophistication in persistent espionage. Cleaver's global targeting of energy, transportation, and other sectors underscored an expansion of nation-state interest in ICS/SCADA environments, with emphasis on long-term access and potential pre-positioning for future disruption.

5.2.2. Dragonfly (Energetic Bear, 2014)—Energy Sector (EU, US)

MITRE Tactics: Initial Access (TA0108); Execution (TA0104); Discovery (TA0102); Persistence (TA0110).

MITRE Techniques: Supply Chain Compromise (T0862); Drive-by Compromise (T1189); Spearphishing Attachment (T0865).

Evolution Summary: The Dragonfly group (also known as Energetic Bear) conducted a campaign in 2014 targeting Western and European energy companies via infected ICS software and phishing. Using Havex/Oldrea malware, they gained initial access through vendor websites and emails, then maintained presence with stolen credentials and backdoors. This attack furthered the trend of supply-chain and watering-hole tactics in ICS intrusions. While not causing physical damage, Dragonfly's operations were highly automated in discovery and data theft and showed improved operational security, indicating a maturing threat. This attack highlighted the fact that well-resourced adversaries (later identified with Russia's FSB) were systematically mapping and penetrating critical energy infrastructure, foreshadowing more destructive attacks to come.

5.2.3. BlackEnergy (2015)—Ukrainian Power Grid

MITRE Tactics: Initial Access (TA0108); Persistence (TA0110); Command & Control (TA0101); Impact (TA0105).

MITRE Techniques: Spearphishing Attachment (T0865); HTTP C2 (T0869); Valid Accounts (T0859); Unauthorized Command Message (T0855).

Evolution Summary: The 2015 Ukrainian power grid attack (by Russia's Sandworm group) used BlackEnergy3 malware and represented the first known cyber-induced electric outage. After initial penetration via phishing emails, the attackers moved laterally with stolen credentials and established C2 channels over HTTP. They ultimately issued unauthorized commands to open circuit breakers, causing a blackout for 225,000 customers. This incident marked a turning point from espionage to disruptive impact. BlackEnergy's modular design (plugins for keylogging, file collection) and the coordinated use of a wiper (KillDisk) to disable systems showed increased automation and aggressiveness. This attack demonstrated growing attacker confidence in leveraging access for physical disruption of utilities, with significant real-world impacts.

5.2.4. Industroyer (2016)—Transmission Substations (Ukraine)

MITRE Tactics: Execution (TA0104); Discovery (TA0102); Lateral Movement (TA0109); Impair Process Control (TA0106); Impact (TA0105).

MITRE Techniques: Firmware Update Mode (T0800); Brute Force I/O (T0806); Denial of Service (T0814); Loss of View (T0829).

Evolution Summary: Industroyer (used against Ukraine's power grid in Dec 2016) was the first malware specifically built to disrupt electric grid operations. It directly

communicated with substation control protocols (IEC-101, IEC-104, etc.), automating the process of opening breakers and disabling safety protections. This attack showed greater sophistication and automation than BlackEnergy, as Industroyer could scan the network, map out devices, and then send malicious commands in rapid sequence. Its multi-modular framework (wiper, protocol spoofer, DoS tool) illustrated a modular ICS attack toolkit designed for maximum impact. Industroyer's short automated execution (causing a substations outage for about 1 h) demonstrated an evolution to fully weaponized ICS malware, emphasizing speed and precision in causing power disruptions.

5.2.5. Triton (Trisis, 2017)—Saudi Petrochemical Plant

MITRE Tactics: Initial Access (TA0108); Execution (TA0104); Privilege Escalation (TA0111); Impair Process Control (TA0106); Impact (TA0105).

MITRE Techniques: System Discovery (T0846); Scripting (T0853); Firmware Modification (T0857); Upload Program (T0845)

Evolution Summary: Triton malware, discovered in 2017, targeted Schneider Triconex safety controllers in a petrochemical plant. The attackers gained access (likely via the OT network) and reprogrammed safety PLCs – using Python-based tools (likely developed in Python 2.7, the prevalent version at the time) to upload payloads that altered firmware and logic on the safety instrumented system. Triton's tactics were highly specialized: it performed network scans for SIS controllers and then downloaded new code into them. This represents an unprecedented level of ICS attack sophistication, as compromising safety systems could allow physical destruction (in this case, the malware caused a shutdown as a fail-safe). Triton highlights an evolution toward targeting human safety; the attack required deep ICS expertise and showed how adversaries could automate complex ICS actions. It underscored that by 2017 attackers were willing to push the boundaries of impact in critical infrastructure, even risking catastrophic outcomes.

5.2.6. Colonial Pipeline (2021)—U.S. Fuel Pipeline

MITRE Tactics: Initial Access (TA0001); Persistence (TA0003); Exfiltration (TA0010); Impact (TA0040).

MITRE Techniques: Phishing (T1566); Exploit Public-Facing App (T1190); Data Encrypted for Impact (T1486).

Evolution Summary: The Colonial Pipeline attack (May 2021) was perpetrated by the criminal DarkSide ransomware group, indirectly impacting ICS operations. The attackers likely gained initial access via phishing or exposed RDP/VPN credentials, then deployed ransomware to encrypt IT systems and steal data (double extortion). Tactically, this attack followed a classic ransomware playbook; nonetheless, its impact (a major fuel pipeline shutdown) showed that criminal operations can have national-scale ICS consequences. Compared to earlier state-sponsored ICS intrusions, the Colonial incident was less technically complex in ICS terms (no direct control of field devices), yet it forced a halt of pipeline operations. This reflects an evolving threat landscape in which ransomware crews exploit IT/OT convergence, achieving high impact with moderate sophistication. This attack spurred industry awareness that even "indirect" attacks on business networks can disrupt critical OT infrastructure.

5.3. Oldsmar Water Plant (2021)

MITRE Tactics: Initial Access (TA0108); Execution (TA0104); Impair Process Control (TA0106); Impact (TA0105).

MITRE Techniques: Remote Services (T1133); Valid Accounts (T0859); Modify Parameter (T0836).

Evolution Summary: The Oldsmar water treatment hack (Feb 2021) involved an attacker remotely accessing an HMI via TeamViewer and attempting to poison the water by raising lye levels. The tactics were relatively unsophisticated; the adversary used legitimate remote access credentials (or unsecured access) to enter the OT network and directly manipulated the GUI controls of the chemical dosing system. This incident highlighted that even low-skill attacks (no custom malware, just misuse of remote admin tools) can threaten physical safety if proper network segregation and authentication are lacking. It underscored a trend in which opportunistic or insider-like attackers target smaller critical systems by relying on simplicity (valid accounts and GUI actions) rather than advanced exploits. Fortunately, an alert operator caught the malicious changes in time; however, Oldsmar serves as a cautionary example of the need for robust access controls and monitoring in ICS.

5.3.1. Industroyer2 (2022)—Ukraine Substations

MITRE Tactics: Discovery (TA0102); Impair Process Control (TA0106); Impact (TA0105).

MITRE Techniques: Brute Force I/O (T0806); Modify Parameter (T0836); Service Stop (T0881).

Evolution Summary: Industroyer2 [34] was an updated version of Industroyer deployed during the 2022 Russian invasion of Ukraine. Similar to its 2016 predecessor, it is a compact single-purpose malware that speaks IEC-104 protocol to open breakers and causes outages. Notably, Industroyer2 [35] was pre-scheduled to execute at a specific time on the grid, indicating a focus on rapid timed impact. Its technique set included brute-forcing through device I/O addresses and issuing malicious commands to switch power states. Industroyer2's emergence shows an evolution in state-sponsored attacks toward streamlined and efficient attack kits; it had fewer components than the original, suggesting lessons learned to reduce complexity and detection risk. Although quickly neutralized, this attack (paired with a disk wiper in IT systems) demonstrated that advanced adversaries are continuing to refine ICS malware for faster deployment and integration with broader military or sabotage campaigns.

5.3.2. FrostyGoop (2023)—Ukrainian Heating Systems

MITRE Tactics: Impair Process Control (TA0106); Command and Control (TA0101); Impact (TA0105).

MITRE Techniques: Modbus TCP (T0869); Manipulation of Control (T0831); Unauthorized Command Message (T0855).

Evolution Summary: FrostyGoop (disclosed 2023–2024) is the ninth known ICS-specific malware, and is unique for exploiting the common Modbus PLC protocol to directly issue malicious commands. Written in Go, it was used in an attack on Ukrainian city infrastructure (heating system) in early 2024 that turned off boilers, showing its ability to manipulate control outputs and change device parameters. FrostyGoop's design is somewhat simpler than earlier state malware—it leverages open-source libraries and straightforward read/write commands—yet it represents the continued evolution of ICS threats beyond elite state actors. By using Modbus (a widely deployed protocol) for C2 and payload actions, FrostyGoop demonstrates how attackers are broadening their toolkit to target industrial devices directly via standard channels. Its appearance underscores a trend toward more accessible ICS attack methods (potentially available to cybercriminals or hacktivists) while still having significant impact on operations (in this case, leaving civilians without heat in winter).

6. Comparative Technical Pathways of Cyberattack Methodology

To consolidate insights from the sector-specific analyses in Sections 3 and 4, this section presents a comparative mapping of the technical pathways used in documented cyber-attacks on petroleum and power grid infrastructures. The objective is to provide a structured, at-a-glance view of how different attack types progress from initial compromise to operational impact, highlighting sector-specific characteristics and commonalities.

The chart in Table 2 synthesizes case evidence from the selected incidents, organizing them into standardized attack phases derived from the MITRE ATT&CK for ICS framework. While individual tactics may vary in execution, the pathway mapping reveals recurring dependencies between intrusion vectors, lateral movement, and control system disruption. This visualization enables practitioners and researchers to:

- Identify convergence and divergence in attack sequences across critical energy sectors.
- Understand which MITRE ATT&CK tactics are most frequently exploited.
- Contextualize sector-specific resilience needs by mapping technical pathways to potential defensive measures.

Table 2. Comparative technical pathways of cyber-attacks in petroleum and power grid sectors.

Phase	Description	Representative Techniques (MITRE ATT&CK for ICS)	Observed in Petroleum Sector	Observed in Power Grid Sector
1. Reconnaissance	Adversaries gather technical and organizational information about the target	Gather Victim Host Information (T0866), Gather Victim Network Information (T0840), Phishing for Information (T1598)	Dragonfly/Havex reconnaissance of OPC servers in oil & gas vendors	Pre-Industroyer OSINT and network mapping of substation control systems
2. Initial Access	First entry into IT or OT environments through exploitation or deception	Spearphishing Attachment (T1566.001), Supply Chain Compromise (T1195), Exploit Public-Facing Application (T1190), Replication Through Removable Media (T1091)	Colonial Pipeline via compromised VPN credentials	Stuxnet via infected USB drives in nuclear power plant ICS
3. Execution	Running of malicious code or payload in target systems	Command-Line Interface (T1059), User Execution (T1204), Exploitation for Client Execution (T1203)	Havex malware execution after delivery via trojanized software installers	CrashOverride payload deployment on grid control systems
4. Persistence	Maintaining access to the environment despite system reboots or changes	Valid Accounts (T1078), Create Account (T1136), Modify Authentication Process (T1556)	Dragonfly maintaining persistence through legitimate remote access accounts	Industroyer persistence via scheduled tasks
5. Privilege Escalation	Gaining higher permissions within compromised systems	Exploitation for Privilege Escalation (T1068), Abuse Elevation Control Mechanism (T1548)	Operation Cleaver escalation within petroleum ICS networks	Industroyer escalation to manipulate relay protection systems
6. Lateral Movement	Moving between hosts or network zones to expand access	Remote Services (T1021), Pass the Hash (T1550.002), Exploitation of Remote Services (T1210)	Havex pivoting from vendor IT to OT via shared credentials	Ukraine 2015 attackers pivoting from IT to SCADA networks
7. Impact/Disruption	Manipulating or halting physical processes and operations	Modify Control Logic (T0831), Inhibit Response Function (T0803), Impair Process Control (T0814), Denial of Service (T0813)	Dragonfly attempting disruption of petroleum operations	Industroyer disrupting substation operations; Stuxnet impairing process control

7. Trends in Attack Evolution–Comparative Analysis

The historical progression of cyber-attacks on energy infrastructures demonstrates a clear shift in threat actor diversity, tactical focus, and technical sophistication. To ensure methodological rigor and strengthen the technical contribution, all documented incidents have been systematically mapped to the MITRE ATT&CK for ICS framework. This approach enables a consistent, case-by-case comparison of tactics, techniques, and procedural evolution across the study period, supported by both narrative descriptions and visualizations (Figures 1 and 2). By combining chronological sequencing, cross-case pattern analysis, and framework-based mapping, we highlight how attacker behavior, operational focus, and mitigation strategies have shifted over time.

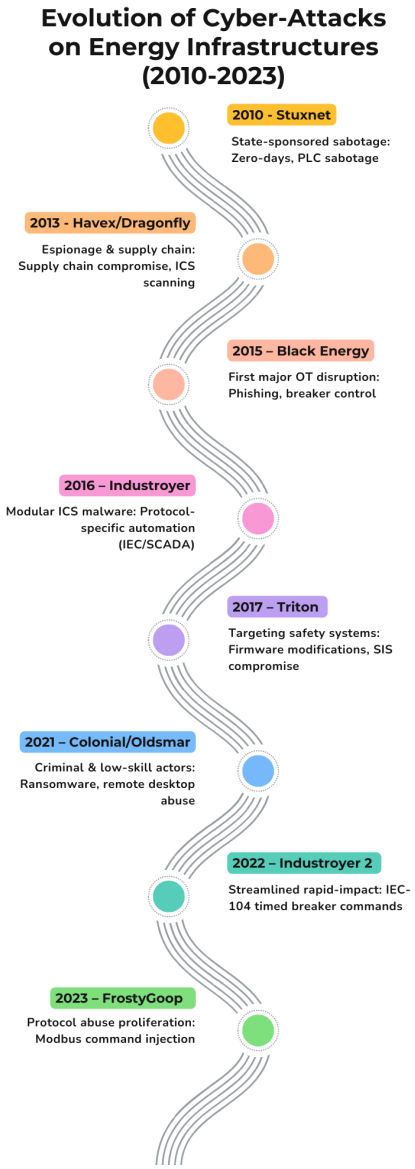


Figure 1. Evolution of Cyberattacks.

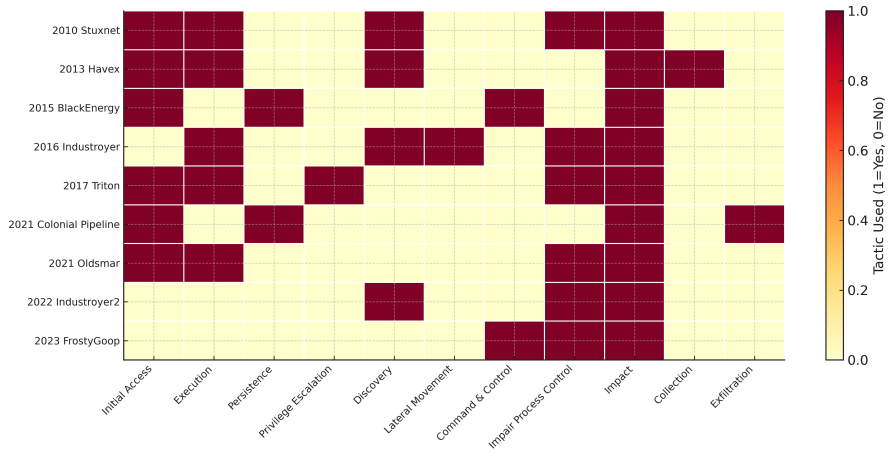


Figure 2. MITRE ATT&CK ICS Heatmap.

7.1. Comparative Evolution of Attack Patterns and Techniques

The evolution of cyber-attacks targeting energy infrastructures reveals a dynamic shift in threat actor objectives, operational tactics, and technical capabilities over time. By examining major incidents within a chronological framework, it is possible to identify recurring patterns, emerging techniques, and corresponding defensive adaptations. This comparative analysis, grounded in MITRE ATT&CK for ICS mapping, highlights how attackers have transitioned from targeted sabotage to highly agile, protocol-specific campaigns. The following subsections present a structured breakdown of representative incidents, observed tactics, and mitigation trends across three distinct phases of attack evolution.

7.1.1. Shift from Targeted Sabotage to Strategic Persistence (2010–2014)

- **Representative incidents:** Stuxnet (2010), Havex (2013), Dragonfly and Operation Cleaver (2014).
- **Patterns:** State-sponsored actors leveraged bespoke ICS malware, exploiting zero-days and supply chain vulnerabilities to infiltrate critical systems. Early campaigns balanced sabotage (Stuxnet) with broad industrial espionage (Havex/Dragonfly).
- **Techniques:** Initial Access via zero-day exploitation (T0866) and trojanized vendor software (T0862); Discovery of ICS assets using OPC scanning (T0843).
- **Mitigation Trends:** Vendor software integrity verification, segmentation between IT and OT, and proactive patch management.

7.1.2. Operational Disruption and Weaponized ICS Malware (2015–2017)

- **Representative incidents:** BlackEnergy (2015), Industroyer (2016), Triton (2017).
- **Patterns:** A tactical shift from espionage to deliberate operational disruption. Industroyer introduced modular, protocol-aware automation for rapid substation breaker manipulation, while Triton expanded targeting to Safety Instrumented Systems (SIS), raising direct safety risks.
- **Techniques:** Credential harvesting via phishing (T0865), valid account abuse (T0859), firmware modification (T0857), and unauthorized control commands (T0855).
- **Mitigation Trends:** Deployment of ICS-aware intrusion detection, SIS monitoring, and strict firmware change control.

7.1.3. Diversification of Threat Actors and IT/OT Convergence (2020–2021)

- **Representative incidents:** Colonial Pipeline ransomware (2021), Oldsmar water facility intrusion (2021).

- **Patterns:** Cybercriminal groups achieved OT impact indirectly via IT compromise, while low-skill adversaries exploited misconfigured remote access tools for direct process manipulation.
- **Techniques:** Use of stolen credentials (T1078), ransomware encryption for impact (T1486), and GUI manipulation over remote desktop (T0856).
- **Mitigation Trends:** Multi-factor authentication, restrictive remote access policies, and continuous activity monitoring.

7.1.4. Streamlined, Rapid-Impact ICS Malware and Protocol Abuse (2022–2023)

- **Representative incidents:** Industroyer2 (2022), FrostyGoop (2023).
- **Patterns:** Highly focused, compact attack toolkits designed for fast execution with minimal detection footprint. Industroyer2 deployed timed IEC-104 breaker commands; FrostyGoop leveraged Modbus to directly manipulate device parameters.
- **Techniques:** Brute-forcing I/O addresses (T0806), unauthorized command messaging (T0855), exploitation of unpatched network devices.
- **Mitigation Trends:** Real-time anomaly detection, protocol command whitelisting, and hardening of endpoint network devices.

7.2. Cross-Case Comparative Insights

The comparison in Table 3 outlines how ICS/OT attack objectives, tactics, and defenses have evolved across four phases: Early State-Sponsored (2010–2014), Disruption-Oriented (2015–2017), Persistence- Oriented (2020–2021), and Streamlined-Modular (2022–2023). It highlights shifts in adversary goals, access methods, and skill levels, alongside the progression of mitigation measures from basic patching to real-time monitoring and targeted device hardening.

Table 3. Comparative technical pathways of cyber-attacks in petroleum and power grid sectors.

Dimension	Early State-Sponsored (2010–2014)	Disruption-Oriented (2015–2017)	Persistence-Oriented (2020–2021)	Streamlined-Modular (2022–2023)
Primary Objective	Espionage & sabotage preparation	Physical disruption of OT	Financial gain/opportunistic	Rapid, high-impact disruption
Target Systems	PLCs, ICS management stations	SCADA, substations, SIS	IT systems, exposed OT HMIs	ICS endpoints via protocol
MITRE Tactics Emphasis	Initial Access, Discovery, Collection	Impair Process Control, Impact	Persistence, Exfiltration, Impact	Discovery, Impair Process Control
Access Vectors	Zero-days, supply chain	Phishing, credential theft	Stolen creds, RDP/VPN abuse	Known protocol abuse, device exploit
Skill/Resource Level	High (nation-state)	High (nation-state)	Medium to low	Medium to high
Mitigation Evolution	Patch mgmt., vendor assurance	Protocol-aware IDS, SIS security	MFA, remote access controls	Real-time monitoring, network device hardening

7.3. Visual Comparative Overview

Figure 1 presents a vertical chronological timeline of major incidents, showing the progression of attacker focus and key techniques. This visualization underscores the transition from complex, multi-vector campaigns to rapid, protocol-specific disruption in recent years.

Figure 2 maps the MITRE ATT&CK for ICS tactics used across each major incident. The heatmap reveals three clear trends:

1. **Early campaigns (2010–2014)** exhibited broader tactic coverage, often spanning from Initial Access through Collection and Impact.

2. **Disruption-oriented campaigns (2015–2017)** emphasized Impair Process Control and Impact, reflecting a shift toward operational consequences.
3. **Recent campaigns (2022–2023)** concentrate on a minimal set of high-impact tactics, often omitting intermediate stages to reduce exposure time.

7.4. Implications for Mitigation Strategies

The comparative analysis yields three key defensive imperatives:

1. Integrate IT/OT security operations to address the blending of attack surfaces.
2. Adopt protocol- and device-specific monitoring, as adversaries increasingly abuse trusted industrial protocols.
3. Implement threat-informed resilience planning, using frameworks like MITRE ATT&CK for ICS to model adversary pathways and design layered mitigations.

7.5. Mitigation Measures, Resilience Strategies, and Lessons Learned

Analysis of historical cyber-attacks on energy infrastructures reveals recurring security gaps and common mitigation opportunities. By mapping lessons learned to the MITRE ATT&CK for ICS Mitigation knowledge base, we ensure these recommendations follow a standardized, actionable framework. Although our dataset covers documented incidents between 2010 and 2023, the mitigation measures and resilience strategies presented in this section are equally applicable to emerging threats observed in 2024–2025. These recommendations consider the unique operational characteristics of energy infrastructures—such as high availability requirements, interdependent OT/IT networks, and long asset lifecycles—ensuring their continued relevance against evolving attack vectors.

7.5.1. Technical Controls (MITRE ATT&CK Mitigation IDs)

- Network Segmentation (M0930): Segregate operational technology (OT) from corporate IT networks to limit lateral movement. Post-Stuxnet, many operators implemented strict firewall zoning and unidirectional gateways to prevent cross-network propagation.
- Access Management (M0912): Enforce strong authentication, least privilege, and regular credential rotation. Multi-factor authentication was deployed after BlackEnergy to protect remote access points.
- Restrict Removable Media (M0953): Disable or tightly control USB and portable device use to mitigate initial infection vectors, as recommended after Stuxnet.
- Application Whitelisting (M0811): Allow only approved executables in control networks, reducing the risk of malware execution.
- Filter Network Traffic (M0937): Implement ICS-protocol-aware intrusion detection systems (IDS) and deep packet inspection to detect suspicious commands.

7.5.2. Resilience & Operational Strategies

- Redundant Systems & Automated Failover: Ensures operational continuity during disruptive attacks (e.g., Industroyer's effect on grid substations).
- Incident Response Exercises (M0918): Regularly simulate OT-specific attack scenarios to improve coordination between IT and OT teams.
- Threat Intelligence Sharing (M0942): Participate in ISACs and national CERT programs to exchange indicators of compromise (IOCs) and TTPs.
- Continuous Monitoring (M0808): Deploy security monitoring tailored to OT environments, capable of detecting MITRE ATT&CK technique patterns.

7.5.3. Lessons Learned Overview

- Purely reactive measures are insufficient; proactive threat hunting (M0804) and regular control system security audits are essential.
- Providing OT engineers with dedicated cybersecurity awareness training can reduce their susceptibility to phishing and social engineering tactics, complementing their existing operational expertise. (M0910).
- Adoption of IEC 62443 and NIST Cybersecurity Framework aligns with MITRE mitigation strategies, offering a structured, repeatable approach for risk reduction.

The synthesized mitigation measures and resilience practices derived from historical incidents are summarized in Table 1. This table links each documented cyber-attack to its primary exploited root cause, lessons learned and the recommended mitigation measures. By connecting lessons learned directly to a standardized mitigation framework, Table 1 enables practitioners to map real-world events to actionable defense strategies in a consistent, repeatable manner.

8. Conclusions and Future Work

NATO and the EU have both established new measures to improve cyber resilience and strengthen collaboration between civilian and military entities across both the Alliance and EU. The threat of cyberattacks is increasing and offensive cyberspace operations are actively being used as an operational domain, as demonstrated in the war in Ukraine. This has resulted in the establishment of the NATO Integrated Cyber Defence Centre (NICC) as well as multiple EU directives such as NIS2 and CER, among other measures. From a research standpoint, it is important to support these advances; this paper contributes with an overview of cyberattacks and Advanced Persistent Threats (APTs) targeting power grids and petroleum installations. Furthermore, this paper discusses the societal impacts observed from cyberattacks and APTs against power grids and petroleum sectors. Examples include the temporary power outage caused by a 2015 cyberattack in Ukraine, as well as the damage potential of the Industroyer 2 malware used by the Sandworm team as part of the Russian invasion of Ukraine in April 2022.

This paper is part of a larger suite of cyberattack and APT analysis being performed as part of the Research Council of Norway-funded CORESIM (Context-Based Real-Time OT-IT Systems Integrity Management) project. Future work involves further analysis of malware samples from cyberattacks and APTs on power grids and petroleum sectors as well as replicating parts of these attacks in two research laboratories, namely, the Digital Station (DS) enclave at the Institute for Energy Technique (IFE) and the NORCE OpenLab research laboratory in Stavanger.

Author Contributions: Writing—original draft, D.A., S.H.H. and L.E.; Writing—review & editing, D.A., S.H.H. and L.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by The Research Council of Norway grant number 344244.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. North Atlantic Treaty Organization (NATO). *Nato Standard AJP-3.20 Allied Joint Doctrine for Cyberspace Operations*; Nato Standardization Office (NSO) ©NATO/OTAN: Brussels, Belgium, 2020.
2. North Atlantic Treaty Organization (NATO). Allies Agree New NATO Integrated Cyber Defence Centre. Available online: https://www.nato.int/cps/en/natohq/news_227647.htm (accessed on 11 November 2024).

3. European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union*, L 333, 27 December 2022, pp. 1–116. Available online: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (accessed on 20 October 2024).
4. European Union. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. *Official Journal of the European Union*, L 333, 27 December 2022, pp. 164–196. Available online: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed on 20 October 2024).
5. Liu, Y.; Deng, Q.; Zeng, Z.; Liu, A.; Li, Z. A hybrid optimization framework for age of information minimization in UAV-assisted MCS. *IEEE Trans. Serv. Comput.* **2025**, *18*, 527–542. [CrossRef]
6. Chen, M.; Luo, K.; Wang, P.; Xiao, W.; Liu, Z.; Liu, A.; Farouk, A.; Chen, M. Federated deep reinforcement learning for combating cyber-threats specific to EV charging in next-gen WPT infrastructure. *IEEE Trans. Intell. Transp. Syst.* **2025**, 1–12. [CrossRef]
7. Vassiliou, M.S. *The A to Z of the Petroleum Industry*; Scarecrow Press: Lanham, Maryland, 2009.
8. Norwegian Oil Industry Association (OLF). Summary Report: Deepwater Horizon-Lessons Learnt and Follow-Up. Available online: https://www.offshorenorge.no/contentassets/0ff3e58e6da243eeb0db267cff486c7d/dwh-summary-june-2012.pdf (accessed on 21 October 2024).
9. Gutierrez, S.; Botero, J.F.; Gaviria, N.; Fletscher, L.A.; Leal, E.A. *Next-Generation Power Substation Communication Networks: IEC 61850 Meets Programmable Networks*; IEEE: Piscataway, NJ, USA, 2022.
10. International Electrotechnical Commission (IEC). *IEC 61850:2024 SER Communication Networks and Systems for Power Utility Automation—All Parts*; IEC: Geneva, Switzerland, 2024. Available online: https://webstore.iec.ch/publication/6028 (accessed on 20 October 2024).
11. Stergiopoulos, G.; Gritzalis, D.A.; Limnaios, E. Cyber-attacks on the Oil & Gas sector: A survey on incident assessment and attack patterns. *IEEE Access* **2020**, *8*, 128440–128475. [CrossRef]
12. Cybersecurity and Infrastructure Security Agency (CISA). Ransomware Impacting Pipeline Operations. 18 February 2020. Available online: https://www.us-cert.gov/ncas/alerts/aa20-049a (accessed on 11 September 2024).
13. Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51. [CrossRef]
14. Venkatachary, S.K.; Prasad, J.; Samikannu, R. *Cybersecurity and Cyber Terrorism in Energy Sector—A Review*; Taylor & Francis: Abingdon, UK, 2018; Volume 2, pp. 111–130.
15. Kovanen, T.; Nuojua, V.; Lehto, M. Cyber Threat Landscape in Energy Sector. In Proceedings of the ICCWS 2018 13th International Conference on Cyber Warfare and Security, Academic Conferences and Publishing Limited, Reading, UK, 8–9 March 2018; p. 353.
16. Wangen, G. The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information* **2015**, *6*, 183–211.
17. Defense Use Case. *Analysis of the Cyber Attack on the Ukrainian Power Grid*; Electricity Information Sharing and Analysis Center (E-ISAC): Washington, DC, USA, 2016; Volume 388, p. 3.
18. Slowik, J. *Crashoverride: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*; Dragos, Inc.: Hanover, MD, USA, 2019.
19. Di Pinto, A.; Dragoni, Y.; Carcano, A. TRITON: The First ICS Cyber Attack on Safety Instrument Systems. In Proceedings of the Black Hat USA, Las Vegas, NV, USA, 8–9 August 2018; pp. 1–26.
20. Beerman, J.; Berent, D.; Falter, Z.; Bhunia, S. A Review of Colonial Pipeline Ransomware Attack. In Proceedings of the 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), Bangalore, India, 1–4 May 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 8–15.
21. Grubbs, R.; Stoddard, J.; Freeman, S.; Fisher, R. *Evolution and Trends of Industrial Control System Cyber Incidents Since 2017*; Wiley Online Library: Hoboken, NJ, USA, 2021; Volume 2, pp. 45–79.
22. Gaspar, J.; Cruz, T.; Lam, C.-T.; Simões, P. *Smart Substation Communications and Cybersecurity: A Comprehensive Survey*; IEEE Communications Surveys & Tutorials; IEEE: Piscataway, NJ, USA, 2023; Volume 25, pp. 2456–2493.
23. Parsons, D. *What's the Scoop on FrostyGoop: The Latest ICS Malware and ICS Controls Considerations*; SANS Institute Blog: North Bethesda, MA, USA, 2024. Available online: https://www.sans.org/blog/whats-the-scoop-on-frostygoop-the-latest-ics-malware-and-ics-controls-considerations/ (accessed on 15 July 2024).
24. IEEESpectrum. The Real Story of STUXNET. February 2013. Available online: https://spectrum.ieee.org/the-real-story-of-stuxnet (accessed on 22 August 2024).
25. Chlela, M. *Cyber Security Enhancement Against Cyber-Attacks On Microgrid Controllers*; McGill University Montréal: Montréal, QC, Canada, 2017. Available online: https://escholarship.mcgill.ca/concern/theses/1c18dh978 (accessed on 22 August 2024).
26. Bencsáth, B.; Pék, G.; Buttyán, L.; Félegyházi, M. Duqu: A Stuxnet-like malware found in the wild. *CrySyS Lab Technical. Rep.* **2011**, *14*, 1–60.
27. SANS Blog. Confirmation of a Coordinated Attack on the Ukrainian Power Grid, January 2016. Available online: https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid (accessed on 22 August 2024).

28. Finance News. Hackers Attacked Prykarpattiaoblenerho, de-Energizing Half of the Region for 6 h. January 2016. Available online: http://news.finance.ua/ua/news/-/366136/hakery-atakuvaly-prykarpattyaoblenergo-znestrumyvshy-polovynu-regionu-na-6-godyn (accessed on 22 August 2024).
29. Cybersecurity & Infrastructure Security Agency. Cyber-Attack Against Ukrainian Critical Infrastructure. February 2016. Available online: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (accessed on 22 August 2024).
30. Geiger, M.; Bauer, J.; Masuch, M.; Franke, J. An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems. In Proceedings of the International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 8–11 September 2020.
31. Zetter, K. Everything We Know about Ukraine's Power Plant Hack. Available online: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ (accessed on 20 October 2024).
32. REUTERS. Ukraine's power outage was a cyber attack: Ukrenergo. January 2017. Available online: https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA (accessed on 24 August 2024).
33. DRAGOS. CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations. February 2017. Available online: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf (accessed on 24 August 2024).
34. ESET Research. Industroyer2: Industroyer Reloaded. Available online: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (accessed on 21 October 2022).
35. Netresec. Industroyer2 IEC-104 Analysis. Available online: https://www.netresec.com/?page=Blog&month=2022-04&post=Industroyer2-IEC-104-Analysis (accessed on 21 October 2022).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.