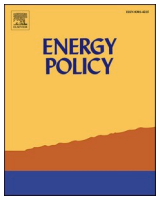
Energy Policy 208 (2026) 114913



Contents lists available at ScienceDirect

Energy Policy

journal homepage: www.elsevier.com/locate/enpol





Cyber threats and energy security: Development and analysis of an incident dataset for the period 2022–2024

Filip Marković *, Ana Kovačević

Faculty of Security Studies, University of Belgrade, Gospodara Vučića 50, Serbia

ARTICLE INFO

Keywords:
Cybersecurity
Energy security
Cyber threats
Energy sector
Critical infrastructure

ABSTRACT

Driven by technological progress, cyber threats present one of the most prominent security challenges in the modern world. The ongoing transformation of energy sector is creating increasingly interconnected energy systems that rely on digital technologies. As a vital component of the economy, the energy sector is highly exposed to numerous simultaneous threats, including cyber-attacks, where the motivations behind such incidents are difficult to understand and may range from financial gains to politically motivated targeting. By developing highly resilient components within the energy system, a country can strengthen its wider concept of energy security, protecting the critical infrastructure and continuity of energy supply. This paper aims to provide a sector analysis for a selected three-year period, from 2022 to 2024, applying a thorough research approach to create a broader picture of the current trend. The dataset was developed, reflecting the sector's vulnerability. As a result, major events are presented, indicating the scope of potential threats, their growing complexity and sophistication, and their eventual consequences. The paper highlights the importance of the cyber component within the energy security concept, one which is often insufficiently considered in both theoretical and practical terms. Accordingly, this work aims to provide evidence-based support for an alternative energy security theoretical framework combining security of critical infrastructure and security of supply principles.

1. Introduction

The accelerated digitization of energy systems has introduced new technological solutions, and cyber security is becoming an increasingly important issue (Gjesvik and Szulecki, 2023), as evidenced by a series of incidents with the primary goal of causing the operational disruption of industrial control systems, physical damage to infrastructure and the theft of strictly confidential operational data. There is a continuous rise in security incidents, which are becoming more advanced and increasingly damaging (Kovačević et al., 2020). According to the World Economic Forum (2025) maintaining cybersecurity remains a top priority, given the significant risk of attacks on digitally dependent resources and services. Malicious activities targeting energy systems have already become a common weapon used in conflicts, with competing powers utilizing these tools in their (geo)political rivalries (Gazula, 2017; Maliarchuk et al., 2019; Stoddart, 2022; Aljohani, 2024). Some of the most powerful cyber tools were developed specifically to cause cyber-physical disruptions and create damage (Kenney, 2015; Yaacoub et al., 2020; Ribas Monteiro et al., 2023; Diaba et al., 2024). Energy security is again becoming one of the key aspects of national security doctrines (Mara et al., 2022), with growing scholarly attention tending to analyze and reconceptualize existing theoretical framework (Strojny et al., 2023; Gitelman et al., 2023). Nevertheless, cyber threats continue to be perceived as abstract and futuristic regardless of their destructive potential and far-reaching consequences. Although some studies recognize and incorporate cyber security (Azzuni & Breyer, 2018a; Dinicu et al., 2021; Diaba et al., 2024; Ryu et al., 2024), those fail to provide a deep investigation on its impact on the energy sector. The focus of past research has mostly been limited to an analysis of the major examples of cyber-attacks on critical energy infrastructure (Venkatachary et al., 2017; Plėta et al., 2020; Venkatachary et al., 2024; Kazancı, 2024), while little emphasis is placed on a comprehensive study of the incident landscape within the sector.

Cyber-physical energy systems are often subject to various digital threats, especially those of government institutions and utilities, targeted with aim to cause far-reaching physical consequences. By 2022, a few such incidents were known, starting with Stuxnet in 2010 (Farwell and Rohozinski, 2011; Shakarian et al., 2013), the first powerful

This article is part of a special issue entitled: Resilience Strategy published in Energy Policy.

* Corresponding author.
E-mail addresses: filip.markovic@rgf.rs (F. Marković), kana@fb.bg.ac.rs (A. Kovačević).

https://doi.org/10.1016/j.enpol.2025.114913
Received 30 March 2025; Received in revised form 21 August 2025; Accepted 29 September 2025
Available online 3 November 2025
0301-4215/© 2025 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

offensive cyberweapon (Putnik, 2022). In 2013, Havex, a malware attributed to the Energetic Bear group[1] was used in an espionage campaign in North America and Europe (Mekdad et al., 2022). Then, in the armed conflict between Russia and Ukraine, the power sector in Ukraine suffered two consecutive attacks in a little less than a year, the first in 2015 caused by the BlackEnergy malware, and the second in 2016 by the Sandworm group using the Industroyer malware, the first ever known tailor-made malware, designed to cause physical damage to a power grid. Finally, the Triton malware[2] was used in 2017 to attack petrochemical facilities in Saudi Arabia, which is believed to be the first recorded incident in which attackers were able to gain control over an industrial control system (Di Pinto et al., 2018). Additionally, cybercrime activities have been on a continuously upward trajectory since their initial emergence (Dupont et al., 2024), with the energy sector becoming a highly attractive target due to its fundamental importance in modern society (Venkatachary et al., 2018). However, until the ransomware attack on the information system of the Colonial Pipeline Company from the USA in May 2021 (Beerman et al., 2023), the cyber component of energy security was not given enough attention among decision-makers nor researchers. Since then, it has become an increasingly important element of the paradigm.

The article is structurally organized with Section 2 presenting the basic research principles and objectives. Section 3 outlines the methodology used to map the cyber incidents recorded during the examined period, which led to the development of a database, resulting in a shortlisted data sample of profiled incidents presented in Section 4. A detailed discussion of our findings is provided in Section 5. Finally, Section 6 summarizes the key recommendations for addressing the critical challenge of achieving comprehensive energy security and concludes by offering insights into the main focus areas for future research.

2. Background

Still, only a limited number of studies have adopted such a sectoral approach (Onyeji et al., 2014; Smith, 2018; Kumar et al., 2018; Al-Mhiqani et al., 2018; Plėta et al., 2020; Trivić and Šošić, 2020; Konaszczuk, 2021; Zhao et al., 2024). The most common approach applied is to focus on a sub-sector, mostly the power sector (Pearson, 2011; Halder, 2014; Islam et al., 2014; Sun et al., 2018; Dagoumas, 2019; Mohan et al., 2020; Priyadarshini et al., 2021; Nejabatkhah et al., 2021; Zografopoulos et al., 2023; Kazancı, 2024; Tatipatri and Arun, 2024) or the fossil fuel sector (Bronk, 2014; Stergiopoulos et al., 2020; Progoulakis et al., 2021; Mohammed et al., 2022; Imran et al., 2022; Alsalama and Alzahrani, 2024). Furthermore, a considerable number of publications address the cyber-related topic of renewable energy sources (Vernotte et al., 2018; Ige et al., 2024a,b; Rekeraho et al., 2024), as well as the field of nuclear energy (Nye Jr, 2011; Son et al., 2019; Kim et al., 2020; Ayodeji et al., 2023) or heating systems (Ding et al., 2022) and even batteries (Azzuni and Breyer, 2018b; Kharlamova et al., 2020; Ogunleye et al., 2024) and electromobility (Bharathidasan et al., 2022). However, these studies address the cyber threat to energy security nominally, often focusing on their analysis from an economic standpoint, a technical point of view, or a legal aspect, but not a sector-wide security approach. In addition, such research are mostly country or region centric.

The purpose of this paper is to emphasize the need to distance from the traditional interpretation based on the security of supply as the central model and instead consider the full spectrum of current threats to energy systems. To contribute to the significant efforts of the academic community to establish a modern theoretical framework of energy security which recognizes the cyber dimension as an integral part, this study conducts a thorough investigation of cyber incidents in the global energy sector. The paper aims to offer a unique, comprehensive multi-year sectoral analysis to support the theoretical acceptance of the cyber component in the contemporary concept of energy security. Unlike most existing works, this study has adopted a broader approach by employing an integrated review, incorporating grey literature as an important source for building the dataset. The use of grey literature was motivated by the aim of collecting information on the most recent incidents.

In this study, we conducted a comprehensive investigation aiming to address the following questions.

1. How does accelerated digitalization, apart from upgrading energy systems and creating positive developments, affect their security?
2. What are the dominant characteristics of cyber incidents in the energy sector?
3. What does the threat landscape look like and what motivates actors to launch malicious activities?

The findings related to those questions led us to address the principal question - can the cyber component finally be considered an equal part of the conceptual framework of energy security?

In the past, numerous authors aimed at redefining energy security with a tendency to offer a deeper conceptual framework, critiquing the limitations of existing models, with a special focus on the shortcomings of the 4As principle, a model which considers energy security through the dimensions of availability, accessibility, affordability and acceptability (APERC, 2007). As security should not follow a one-size-fits-all approach (Baldwin, 1997), energy security must be context-specific as it varies based on the referent object, an issue which the 4As approach fails to address (Chester, 2010). Given the evolving nature of threats to integrated cyber-physical energy systems (Yergin, 2011), the conceptual framework of energy security should adequately reflect its complexity, understood through a systematic, multi-dimensional lens (Winzer, 2012), thus enabling a comprehensive, multi-scalar approach which accounts for systematic vulnerabilities and the diverse challenges of the 21st century. To address the simplicity and limitations of the 4As framework, and particularly its failure to recognize resilience as one of many critical factors (Cherp and Jewell, 2014; Azzuni and Breyer, 2018a), some authors introduce it as additional dimension(s) within the enhanced level of understanding the energy security paradigm, named "*hard, antagonistic or warlike*" (Stanojević and Šekarić Stojanović, 2023, p. 228), in line with the current geopolitical instability and need for framework which allows for capturing political dimensions (Kuzemko et al., 2016). Therefore, the introduction of resilience as the "*elasticity, resistance, endurance and adaptability of a (vital) energy system to changes or stressful events of various origins*" (Stanojević and Šekarić Stojanović, 2023, pp. 226–227) creates a balance between the security of supply and the security of critical infrastructure principles. This, in turn, facilitates a detailed assessment of vulnerability as a combination of risk exposure and resilience, with resilience as the link between energy systems and societal functioning (Cherp and Jewell, 2014; Stanojević and Šekarić Stojanović, 2023). The developed dataset fully complements the warlike approach to energy security as it focuses on a period characterized by military conflicts of global importance, involving major powers already engaged in ongoing industrial competition and trade wars, with energy issues as one of the key concerns.

3. Methodological approach

The dataset was compiled over a multi-year period, carried out periodically in a consistent and structured manner, starting in the third quarter of 2022 and continuing quarterly until end of the first quarter of 2025. Our research focused on developing an inclusive dataset in terms of energy sub-sectors and geography. The study employed the PRISMA 2020 framework as the latest version of internationally recognized guidelines for systematic reviews, explicitly including grey literature as

[1] Also known as Dragonfly.
[2] Also known as TRISIS and HatMan.

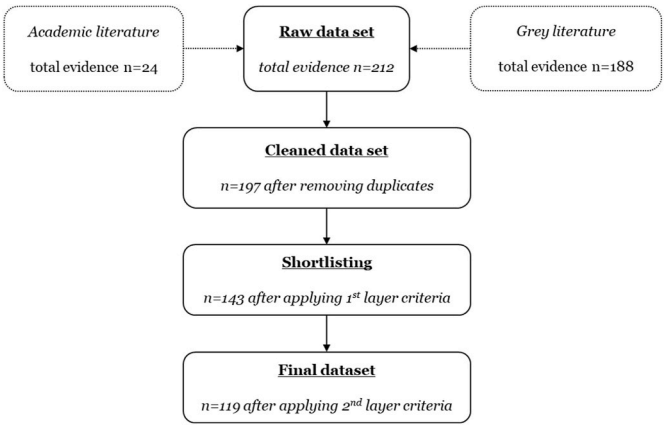


Fig. 1. Schematic presentation of methodological approach.

a legitimate data source (Page et al., 2021a), adjusting its principles to the research needs, making slight modifications to fit the context of a multi-year search procedure, conducted in successive rounds see (Fig. 1).

In the initial step, the search strategy involved a review of the recent academic literature, published in 2022, aiming to map those works dealing with a specific cyber incident in the energy sector, a group of incidents or an overview of cyber developments globally. Therefore, Google Scholar, AcademiaEdu, and Researchgate were the three general search engines employed. Representative examples of the search queries are given in the table below see (Table 1).

The exploration applied a two-layer search strategy. In the first layer search procedure, each keyword from cyber-related group was combined with each keyword from the sector-related group, while the second layer of search queries applied a combination of each first layer combination with each keyword from the geography-related group. This approach was applied to Google Scholar search initially, followed by the expanded search scope toward AcademiaEdu and ResearchGate as another two search engines, applying the same search strategy. Formal academic databases were searched separately from academia-related social networking platforms to account for their distinct indexing quality and coverage limitations. The time frame for each query on each platform was set for the period 2022 by using the custom year range option. The queries combining different keywords always used Boolean operators (Siva Kumar and Santhi Thilagam, 2019).

Following the discovery of a significant gap in comprehensive sectorial focus, an in-depth review of grey literature was conducted to obtain a solid data set for further research boundaries. It served as an identification exercise to investigate the scope and nature of cases overlooked in academic literature. As noted by Adams et al. (2016), grey literature complements conventional scholarly sources by reinforcing their conclusions, revealing inconsistencies between theoretical findings and practical applications, and, in some cases, challenging their underlying assumptions. By broadening the evidentiary base, essential for systematic, scoping, and state-of-the-art reviews (Benzies et al., 2006), especially where scholarly work often lags behind technological change, grey literature is vital and it also mitigates publication bias, as null findings are underrepresented in journals (Burdett et al., 2003). Another significant benefit is its potential to reduce publication bias, as studies reporting null or non-significant results are less likely to appear in conventional academic journals (Burdett et al., 2003). Crucially, it includes insights from practitioners and organizations beyond academia (Adams et al., 2016).

The search process was performed using the Google Advanced, applying the same two-layer search strategy. The grey literature review encompassed various sources – recognized cyber-related professional media, credible mainstream media platforms, professional reports from

Table 1
Search terminology and queries.

Group	Keywords
Cyber-related (9)	"cyber", "cyber-attack", "cyber incident", "cyber security", "cyber threats", "cybercrime", cyber espionage", "hacktivism", "cyber-physical sabotage"
Sector-related (26)	"energy", "energy sector", "energy system", "oil", "oil sector", "gas", "natural gas", "pipeline", "electricity", "electricity sector", "electricity system", "power sector", "power system", "power network", "electricity network", "transmission network", "power grid", "nuclear", "nuclear sector", "nuclear facility", "wind", "wind sector", "solar", "solar sector", "district heating", "e-mobility"
Geography-related (7)	"Europe", "Asia", "North America", "South America", "Africa", "Australia", "Middle East"

the leading consulting companies in the cyber industry, databases of prominent independent market research companies in the thematic field, official statements from the affected entities as victims, statements from government officials, publications, notifications and reporting by the national CERTs, as well as cyber-focused think tanks, cyber-oriented forums, social media and major technological companies. While PRISMA 2020 recommends providing the exact, line-by-line search strings for all sources (Page et al., 2021b), our research incorporated grey literature sources where the search process was dynamic and iterative, adapting to emerging events. Many of these platforms, such as social media and news feeds, do not offer formal query histories, making the complete reproduction of exact queries unfeasible. To maintain transparency, the authors have documented the keyword sets, date limits, and inclusion/exclusion rules used consistently across all sources. This ensures that future researchers can replicate the thematic and temporal scope, even if some original dynamic searches cannot be identically reproduced.

The same search strategy was repeated quarterly within eleven rounds. The search of literature through Google Scholar and academic-related social platforms was performed four times, initially in July 2022, followed by year-focused searches in February 2023, February 2024 and February 2025. This approach was applied given that thematic journal papers are not published so frequently quarterly searches unnecessary. For the grey literature, searches were carried out in every quarter, in February, April, July and November of each year.

For both academic and grey literature, the first three pages or approximately 30 results per search query, per search engine, were analyzed. The open access journal papers published in ScienceDirect, MDPI, IEEE Xplore and Wiley Online Library were considered eligible. The authors screened the titles and abstracts, shortlisting relevant studies for further in-depth reading to identify incident examples. For the filtering of grey literature, the search results were screened by reviewing headlines and preview snippets for news articles and/or reports of different types. In the case of social networks, the posts were taken into consideration for further analysis and cross-checking only if they were published by the official accounts of threat actors or relevant cyber-specialized organizations. For each incident identified in the grey literature, a simultaneous cross-checking of academic literature was performed, employing an incident-specific search. This confirmed the obvious gap in the scholarly works for the second time, but grey literature successfully supplemented it and provided substantial material. Additionally, for each of the incidents identified, a manual search using Google was performed, aiming at collecting additional source(s), if available. Each mapped incident was inserted manually into an Excel-based dataset, with its references. After a few rounds the search process delivered a satisfying result, with the raw dataset of incidents exceeding two hundred cases in total, precisely 212 incidents after Round 11. The authors held regular quarterly meetings to consult on key findings and next research steps.

In order to examine the quality of the collected data and create a reliable sample, it was necessary to undergo systematic processing,

refining, structuring, and homogenization. The dataset built on extensive web research, drastically grew in volume, requiring the filtering, classification, and shortlisting of collected data to define a draft scope based on the credibility of sources. The applied approach followed a set rule of multiple verification of information for each incident, agreed by the authors, to confirm the accuracy and reliability and avoid unverified information, speculation, fake news, and misinformation. Aiming to achieve academic legitimacy, the shortlisted database sample included only those incidents credibly confirmed as per the criteria set. The final dataset was compiled through a two-layer procedure. Therefore, the first layer consisted of three major sub-criteria, determined as follows, where a minimum of two had to be met.

1) At least one research paper in a scientific journal and/or at least one credible media source refers to the cyber incident.
2) At least one official statement issued by a governmental institution and/or at least one by a credible security-oriented organization refers to the cyber incident.
3) At least one official statement issued by a victim entity and/or responsible threat actor refers to the cyber incident.

This step served to draft the shortlisted dataset, combined with the exclusion of any duplicates. As expected, almost one-third of the information lacked strong confirmation in other sources. To create a consistent final dataset useable for comparative analysis, the incidents had to be profiled systematically. For inclusion, the references on the cyber incident should have at minimum of 5 out of 8 of the following data points: (1) the date the incident occurred, (2) the country of the victim entity, (3) the sub-sector within the energy sector, (4) the victim/affected entity, (5) the type of attack, (6) the confirmed of suspected threat actor, (7) the impact in terms of the consequences caused, (8) the confirmed or suspected motive. Only a few exceptional cases were included fulfilling only four or fewer data points due to their political importance, significant impact, the involvement of a powerful threat actor, or high media attention.

One of the challenges was the fact that cyber incidents, particularly those state-related, are rarely subject to thorough investigation with public disclosure or accompanied by publicly available, mature information. Hence, the level of investigation varies among the incidents in the dataset. This was also partially due to the different times the incidents occurred. Usually, earlier incidents are supported by more consistent and comprehensive information, while recent cases might lack sufficient contextual data due to the early stages of an investigation. Aiming at building a reliable dataset and overcoming the challenges of underreporting, reporting with limited information, circular reporting and fake reporting,[3] the study used multiple sources to cross-check incident attributes. Commercial sources and social media posts were often consulted but always treated cautiously and combined with diverse sources.

Finally, the shortlisted evidence sample includes 119 incidents from 57 countries, caused by nearly fifty different threat actors, using data for the period from January 1st, 2022, to December 31st, 2024. It covers fossil fuels, renewable energy, and the nuclear sector, encompassing the entire energy value chain.

4. Results

In 2022, two more malware designed exclusively for attacks on industrial control systems were promptly discovered - a new version of the Industroyer malware[4] during a prevented incident in the power sector of Ukraine (ESET, 2022) and the malware Pipedream of the group Chernovite. The special importance of the latter is the noticeable evolution in its development as it represents the first known scalable malware, designed for multiple uses and in different sectors with the ability to influence the functionality of industrial protocols and applications on a wide range of devices from different manufacturers (Dragos, 2023b). Zarya, a pro-Russia-hacking group, had infiltrated an unnamed Canadian natural gas network operator, claiming the ability to remotely manipulate a gas distribution station, having access to valve pressure and alarms, and even the ability to initiate an emergency shutdown of the facility which could cause an explosion (Ropek, 2023; Koelemij, 2023; D'Andrea, 2023).

4.1. Dataset

As presented in the Table 2 of the final dataset, the sub-sectors are divided into the power sector ("ELE"), the oil sector ("OIL"), the natural gas sector ("NG"), the nuclear sector ("NCL"), and the district heating sector ("HEAT"). The power sector includes electricity generation from all sources except nuclear, as well as transmission, distribution, and storage, but also e-mobility. The oil sector includes crude oil exploitation, refining and processing, transport, and distribution. The same applies to the natural gas sector which covers both transport by pipelines and LNG routes. Some cases involve victim entities acting as integrated energy service providers or companies operating in more than one energy sub-sector.

For the type of attack category, the research classified incident into three types: (1) Distributed Denial of Service (DDoS) which disrupts access to systems or data by exhausting the service and its resources or overloading network infrastructure components (ENISA, 2024), (2) ransomware whereby the threat actor blocks access to a resources demanding a ransom to restore access or prevent the disclosure of sensitive data ENISA, 2024, or (3) malware as any malicious software or firmware which executes unauthorized processes aimed at compromising a system's security, its confidentiality, integrity or availability in particular ENISA, 2024.

In terms of impact, incidents are classified as those which cause operational disruption or data theft. Operational disruption includes interruptions to the normal operating of core business activities, covering both digital or physical infrastructure disruptions. Data theft includes either a data breach or data leak where a data breach is treated as stolen data and a data breach to stolen data being offered to the public for free or under-defined compensation.

Finally, motives are defined as either financial or political. The following categories are determined under political motivation: (1) espionage, which results in information-gathering actions (2) sabotage, which results in deliberate disruption or damage to digital assets or physical infrastructure (3) hacktivism, which results in political discrediting conducted by ideologically motivated groups. The financially motivated incidents are treated as a separate category with the primary aim of the threat actors to obtain financial gain. The approach followed the existing categorization into four groups – cybercrime, hacktivism, espionage/sabotage, and information warfare (Facchinetti et al., 2023), while for our research purpose we split espionage and sabotage into separate categories, while integrated information warfare into hacktivism. However, determining the attributes of cyber incidents remains inherently challenging, becoming even more complex for the energy sector due to its strategic importance in the current global crisis. The sector's attractiveness to diverse threat actors often creates an unclear distinction between political and financial motives. In cases where multiple motivations were identified, the authors applied the approach based on the predominant impact reported as a key factor, while also considering the key motivational characteristics of the threat actor, to distinguish between different categories. For instance, cyber espionage often forms part of broader tactics leading to further consequences, such as financial impacts, sabotage or hacktivism, but it can also be a standalone activity with the sole purpose of collecting information see (Table 2).

[3] Based on false claims of responsibility by different competing cyber actors.
[4] i.e. CrashOverride, the so-called Industroyer2 malware.

Table 2
Dataset of cyber incidents in the global energy sector for the period 2022–2024.

Date	Country	Sector	Victim	Type of attack	Threat Actor	Impact	Motive	Reference
Q4 2024	Costa Rica	OIL	Recope	Ransomware	Unknown	Operational disruption	Unclear	(Greig, 2024; Matishak, 2025)
	Germany	ELE	Tibber	Unspecified	Threat Actor 888	Data theft	Financial	Kunz (2024)
	Romania	ELE	Societatea Energetica Electrica S.A.	Ransomware	Lynx	Unclear	Unclear	(Gatlan, 2024a, 2024b)
	Finland and Sweden	ELE, NCL	Fortum	Unspecified	Unknown	Unclear	Sabotage	Kauranen and Lehto (2024)
	USA	OIL, NG	Victron Energy	Ransomware	Abyss	Data theft	Financial	(@HackManac., 2024a; FalconFeedsio, 2024a)
	Cyprus	OIL, ELE	EKO and Electricity Authority of Cyprus	DDoS	LulzSec Black	Operational disruption	Hacktivism	Ribeiro (2024a)
	Iran	NCL, OIL	An unknown group of companies	Malware	Unknown	Unclear	Sabotage	Schiaffino (2024)
	Spain	ELE, OIL, NG	Repsol	Unspecified	Unknown	Data theft	Unclear	"Repsol suffers" (2024)
Q3 2024	Israel	NCL	Soreq Nuclear Research Center	Ransomware	Handala	Data theft	Hacktivism	Dimitrov (2024)
	Colombia	ELE	Air-e	Ransomware	Unknown	Data theft	Unclear	("Third Largest Energy", 2024; Kondruss, 2025)
	Spain	OIL, NG	Decal España	Ransomware	BlackSuit	Data theft	Financial	(@FalconFeedsio, 2024b)
	USA	NG	Tellurian Inc.	Ransomware	RansomHub	Data theft	Financial	(@HackManac., 2024b)
	USA	OIL	Risser Oil Corporation	Ransomware	Qilin	Data theft	Financial	"Risser Oil" (2024)
	USA	OIL, NG	Anderson Feazel	Ransomware	Hunters International	Data theft	Financial	"Anderson Feazel" (2024)
	British Virgin Islands	ELE	BVI Electricity Corporation (BVIEC)	Ransomware	Akira	Unclear	Financial	("BVIEC falls victim", 2024a; "Premier promises", 2024b)
	USA	OIL, NG	Halliburton	Ransomware	RansomHub	Data theft	Financial	(Reddick, 2024; Jones, 2024)
	Canada	OIL, NG	Veren Inc and Crescent Point Energy	Ransomware	RansomHouse	Data theft	Financial	(HookPhish, 2024; "RansomHouse Ransomware Victim", 2024)
	Philippines, South Korea, Vietnam, Taiwan and Thailand	Unknown	Numerous actors in the energy sector	Malware	Earth Baxia	Unclear	Espionage	Lee et al. (2024)
	Israel	OIL, NG	Sonol	Ransomware	Handala	Data theft	Hacktivism	(@FalconFeeds.io, 2024c)
	Indonesia	ELE	Indika Energy	Ransomware	Hunters International	Data theft	Financial	(@FalconFeeds.io, 2024d; Baek, 2024)
	USA and other	Unknown	Various companies	Malware	UNC2970	Unclear	Espionage	(Mandiant, 2024a; Ribeiro, 2024b)
	Australia	OIL	North Coast Petroleum	Ransomware	Medusa	Data theft	Financial	Hollingworth (2024)
	USA	OIL, NG	Peregrine Petroleum	Ransomware	BlackSuit	Data theft	Financial	"Peregrine Group" (2024)
	USA	NG, HEAT	Hyde Fuel	Ransomware	Qilin	Unclear	Financial	(@FalconFeeds, 2024e)
Q2 2024	Mexico	NG	Ultragas Mexico	Ransomware	Lockbit3	Data theft	Financial	(@HackManac., 2024c)
	France	ELE, NG	Engie	Ransomware	Lapsus$	Data theft	Financial	Boero (2024)
	Nigeria	OIL, NG	Nestoil	Ransomware	BlackSuit	Data theft	Financial	Zoltan and Popa (2024)
	USA	OIL	Atlas Oil	Ransomware	Black Basta	Data theft	Financial	Croft (2024)
	Pakistan and Hong Kong	ELE	Unknown	Malware	Unknown	Data theft	Espionage	Son (2024)
	Israel	ELE	Transmission utility	Unspecified	CyberAv3ngers	Data theft	Hacktivism	(@CyberAveng3rs, 2024)
	USA	OIL, NG	Pioneer Oil Company	Ransomware	Bianlian	Data theft	Financial	HookPhish, 2024
	Colombia	ELE	Empresa de energía del Bajo Putumayo	Ransomware	RansomHub	Data theft	Financial	"Empresa De Energia" (2024)
	Vietnam	OIL	PetroVietnam Oil Corporation (PVOIL)	Ransomware	Unknown	Data theft	Financial	(Ministry of Science and Technology, 2024; "PRESS RELEASE", 2024)
	USA and UAE	Unknown	Numerous energy companies	Malware	APT33	Data theft	Espionage	Gatlan (2024)
Q1 2024	India	Unknown	Numerous energy companies	Malware	Unknown	Data theft	Espionage	"Analysing Operation FlightNight" (2024)
	North Macedonia	ELE	MEPSO	Unspecified	Unknown	Unclear	Financial	Kolekevski (2024)
	Canada	OIL, NG	Rush Energy	Ransomware	BlackCat	Data theft	Financial	Lyons (2024)
	USA	OIL, NG	Wapiti Energy	Ransomware	Hunters International	Data theft	Financial	(HookPhish, 2024)
	Israel	OIL	Bazan Group	DDoS	Anonymous Sudan	Operational disruption	Hacktivism	Khaitan (2024)
Q4 2023	Russia	Unknown	Numerous energy companies	Ransomware	Crypt Ghouls	Data theft	Financial	(Lakshmanan, 2024; Threat Advisory, 2024)
	Iran	OIL	Unknown, broader system	Malware	Predatory Sparrow	Operational disruption	Hacktivism	Paganini (2023a)

(*continued on next page*)

Table 2 (*continued*)

Date	Country	Sector	Victim	Type of attack	Threat Actor	Impact	Motive	Reference
	USA	ELE	Lower Valley Energy	Ransomware	BlackCat	Data theft	Financial	Kaspersky ICS CERT (2023)
	Vietnam	ELE	Ho Chi Minh City Energy Company	Ransomware	BlackCat	Data theft	Financial	Khaitan (2023a)
	Israel	ELE	Israel Electric Company	Ransomware	CyberAv3ngers	Data theft	Hacktivism	Khaitan (2023b)
	USA	OIL, NG	Navitas Petroleum	Ransomware	Black Basta	Data theft	Financial	(Halcon Tech, 2025)
	Serbia	ELE	EPS	Ransomware	Qilin	Data theft	Financial	Spasić (2023)
	China	ELE	China Energy Engineering Corporation	Ransomware	Rhysida	Data theft	Financial	Paganini (2023b)
	Brazil	ELE	Goiasa	Ransomware	Akira	Data theft	Financial	Zoltan (2023)
	Slovenia	ELE	Holding Slovenske Elektrarne (HSE)	Ransomware	Rhysida	Data theft	Financial	"Power utility HSE" (2023)
	Israel	Unknown	Unknown	Malware	Storm-1133	Unclear	Hacktivism	(Antoniuk, 2023; CERT-EU, 2023a)
Q3 2023	Serbia and Russia	Unknown	Number of energy companies	Malware	Space Pirates	Unclear	Espionage	Lakshmanan (2023)
	France	ELE, NG	Engie	Unspecified	HommedeLombre	Data theft	Hacktivism	Egon (2023)
	Israel	OIL	Bazan Group	DDoS	CyberAv3ngers	Operational disruption	Hacktivism	Sharma (2023)
	Canada	OIL, NG	Suncor Energy	Unspecified	Unknown	Operational disruption	Unclear	Jones (2023)
	Belize	ELE	Belize Electricity Limited	Ransomware	Rangar Locker	Data theft	Financial	(Gonzalez, 2024; CMC, 2024)
Q2 2023	Eastern Europe	OIL, NG	Number of companies	Malware	Lazarus?	Unclear	Espionage	(Kaspersky GReAT & ICS CERT, 2023)
	Netherlands, Australia, Oman, UK and USA	ELE, OIL, NG	Number of companies	Ransomware	Clop	Data theft	Financial	Martin (2023)
	India	ELE	Madhya Pradesh Power Management Company Limited (MPPMC)	Ransomware	Unknown	Unclear	Financial	Agencies (2023)
	Denmark	ELE	22 energy companies	Combined tactics	NoName57(16)/ Sandworn	Unclear	Sabotage	(Paganini, 2023c; SectorCERT, 2023; Diaba et al., 2024)
Q1 2023	China	NCL	Wider sector	Malware	Bitter APT	Unclear	Espionage	(CERT-EU, 2023b)
	Italy	ELE, NG	Acea	Ransomware	Black Basta	Data theft	Financial	(CERT-EU, 2023c)
	Canada	NG	Unknown	Unspecified	Zarya	Operational disruption	Hacktivism	(CERT-EU, 2023d; Koelemij, 2023)
	Indonesia	OIL	PetroChina Indonesia	Ransomware	Medusa	Unclear	Financial	"Medusa Claims PetroChina" (2023)
	USA	OIL, NG	Encino Energy	Ransomware	BlackCat	Data theft	Financial	Greig (2023)
	Argentina	OIL, NG	Grupo Albanesi	Ransomware	LockBit	Unknown	Financial	(Brodersen, 2023; Glover, 2023)
	Russia	OIL, NG	Gazprom	Unspecified	IT Army of Ukraine	Data theft	Hacktivism	Paganini (2023d)
Q4 2022	Colombia	ELE, NG	Empresas Públicas de Medellín (EPM)	Ransomware	BlackCat	Data theft	Financial	(Abrams, 2023)
	Ukraine	ELE	Power grid of the city of Krivoy Rog	Malware	Cyber Army	Unclear	Hacktivism	(CERT-EU, 2022a)
	Estonia	ELE	Eesti Energia	DDoS	Unknown	Operational disruption	Hacktivism	(CERT-EU, 2022b)
	Greece	ELE	Public Power Corporation (PPC)	DDoS	Killnet	Operational disruption	Hacktivism	(Thales, 2023; CERT-EU, 2022e)
	Australia	ELE	EnergyAustralia	Unspecified	Unknown	Data theft	Financial	Rachwani (2022)
	India	ELE	Tata Power	Ransomware	Hive	Data theft	Financial	Sharma (2022a)
	Thailand	NCL	Thailand Institute of Nuclear Technology	Unspecified	Unknown	Data theft	Espionage	"CyberThreats Mushrooming" (2022a)
	South Africa	NCL	Koeberg Nuclear Power Station	Unspecified	Unknown	Data theft	Espionage	"CyberThreats Mushrooming" (2022a)
	India	NCL	Nuclear Power Corporation of India	Unspecified	Unknown	Data theft	Espionage	"CyberThreats Mushrooming" (2022a)
	Iran	NCL	Atomic Energy Organization	Unspecified	Black Reward	Data theft	Espionage	"CyberThreats Mushrooming" (2022a)
	Germany	ELE, NG, HEAT	Enercity	Unspecified	Unknown	Data theft	Financial	"IT-Störung bei enercity" (2023)
	Indonesia	NCL	Indonesia Nuclear Power Authority	Unspecified	Unknown	Data theft	Espionage	"CyberThreats Mushrooming" (2022a)
Q3 2022	Taiwan	NCL	Taipower	Unspecified	Unknown	Data theft	Espionage	("CyberThreats Mushrooming", 2022a; "Pelosi's Taiwan Visit, 2022b)
	Italy	ELE	Gse	Ransomware	BlackCat	Data theft	Financial	(Lepido, Gallangher & Brambilla, 2022)
	Italy	OIL	Eni S.p.A.	Ransomware	Unknown	Unclear	Financial	Lepido and Brambilla (2022)

(*continued on next page*)

Table 2 (*continued*)

Date	Country	Sector	Victim	Type of attack	Threat Actor	Impact	Motive	Reference
	Kyrgystan, Tajikistan and Uzbekistan	ELE	KyrgyzKomur	Malware	Yoro Trooper	Unclear	Espionage	(Malhotra and Ventura, 2023a,b)
	Ghana	ELE	Electricity Company of Ghana Limited	Ransomware	Unknown	Operational disruption	Financial	"ECG lost" (2024)
	Montenegro	ELE	Elektroprivreda Crne Gore (EPCG)	Ransomware	Cuba	Operational disruption	Financial	Spasić (2022)
	Moldova	ELE	Premier Energy	DDoS	Killnet	Unclear	Hacktivism	EclecticIQ Threat Research Team (2022)
	Ukraine	ELE	Energoatom	DDoS	People's Cyber Army	Unclear	Hacktivism	Antoniuk (2022)
	Greece	NG	DESFA	Ransomware	Ragnar Locker	Data theft	Financial	"Behind the News" (2022)
	USA, Canada and Japan	Unknown	Energy utilities	Malware	Lazarus/ATP38	Unclear	Espionage	"North Korean Hackers" (2022)
	Luxembourg	ELE, NG	Creos Luxembourg	Ransomware	BlackCat	Data theft	Financial	(CERT-EU, 2022c)
	France	ELE	Idex	Ransomware	Industrial Spy	Data theft	Financial	(CERT-EU, 2022d)
	Lithuania	ELE, NG, HEAT	Ignitis Group	DDoS	Unknown	Operational disruption	Hacktivism	Meehan (2022)
Q2 2022	Ukraine	ELE	Oblenergo	Malware	KAMACITE	Unclear	Sabotage	(Dragos, 2023a)
	Germany	NG	Entega	Ransomware	Unknown	Data theft	Financial	"Cyberangriff beim Darmstädter" (2022)
	Russia	OIL	Rosneft/oil depot in Belgorod	Unspecified	GURMO	Data theft	Sabotage	Lapienytė (2022)
	Russia	OIL	Lukoil and Gazprom	Unspecified	Aggressive Griffin	Data theft	Hacktivism	(CERT-EU, 2022e)
	Russia	OIL	SOCAR Energoresource	Unspecified	Anonymous	Data theft	Hacktivism	(@YourAnonTV, 2022)
	USA	OIL, NG	Devon	DDoS	Killnet	Operational disruption	Hacktivism	(Vedere Labs, 2022; "An In-Depth Look", 2022; "An Update", 2023)
	Russia, Georgia, Mongolia	ELE	A couple of companies	Malware	Space Pirates	Data theft	Espionage	(CERT-EU, 2022f; Toulas, 2022a)
	Russia	OIL, ELE, NG	Gazprom Neft and ALET	Unspecified	Anonymus	Data theft	Hacktivism	Greenwood (2022)
	India	OIL	Oil India Limited	Ransomware	BlogXX	Data theft	Financial	(Goud, n.d.; Cyber Threat Intelligence, 2023)
	Costa Rica	ELE	Junta Administrativa del Servicio Eléctrico de Cartago (JASEC)	Ransomware	Conti	Data theft	Financial	Greig (2022)
	Germany	ELE	Deutsche Windtechnik	Ransomware	Unknown	Operational disruption	Unclear	Paganini (2022a)
	Indonesia	NG	Perusahaan Gas Negara	Ransomware	Hive	Data theft	Financial	Glover (2022)
Q1 2022	Saint Martin	ELE	Utilities company GEBE	Ransomware	BlackByte	Operational disruption	Financial	(Openbar Ministerie, 2022)
	Russia	ELE	Rosenergoatom	Unspecified	GURMO	Data theft	Sabotage	Uchill (2022)
	Maldives	ELE	State Electric Company Limited (STELCO)	Ransomware	Hive	Data theft	Financial	(Rehan, 2022; Cyber Threat Intelligence, 2023)
	South Africa	ELE	Eskom	Ransomware	Everest	Data theft	Financial	Paganini (2022b)
	Russia	OIL	Transneft	Unspecified	Unknown	Data theft	Financial	Arghire (2022)
	India	ELE	Electricity Despatch Centers	Malware	TAG-38	No impact	Unclear	Insikt Group (2022)
	Spain	ELE	Iberdola	Unspecified	Unknown	Data theft	Financial	(Kemp, 2022; Sáiz-Pardo, 2022)
	Romania	OIL	Rompetrol	Ransomware	Hive	Unclear	Financial	Sharma (2022b)
	Russia	NCL	Joint Institute for Nuclear Research	Unspecified	Unknown	Data theft	Espionage	"CyberThreats Mushrooming" (2022a)
	Russia and Germany	OIL	Rosneft Deutschland GmbH	Unspecified	Anonymous	Unclear	Hacktivism	(AFP, 2022; Dinger et al., 2022)
	Germany	OIL	Oiltanking GmbH	Ransomware	BlackCat	Operational disruption	Financial	Beer (2022)
	Germany	ELE	Enercon	Malware	Unknown	Operational disruption	Sabotage	(Egan, 2022; Viasat, 2022)
	Russia	ELE	Rosseti	Malware	Unknown	Operational disruption	Hacktivism	Johnson et al. (2022)
	Netherlands, Belgium and Germany	OIL	At least 17 port facilities	Ransomware	BlackCat	Operational disruption	Unclear	(Baker, 2022; Pengili and Raszewski, 2024)
	USA	NG	21 LNG companies	Unspecified	Unknown	Unclear	Unclear	(Robertson and Charpa, 2022)
	Bulgaria	ELE	Kardzhali Hydroelectric Power Station and CEZ Electro	Malware	Fancy Bear/APT28 and Konni	Data theft	Espionage	(Bushido, 2022)

4.2. Limitations

While this paper provides valuable insights into the current landscape of cyber threats to energy security, it is important to acknowledge certain limitations which may affect the generalisability of our findings. Firstly, the database is unbalanced evidence in terms of literature type, with non-traditional resources outnumbering the open access academic publications as a direct consequence of the thematic gap identified in recent scholarly works. On the other hand, the use of alternative literature backing the research as a primary data source allowed us to capture emerging trends. At the same time, we acknowledge that the dataset presented here is not definitive since the consequences of cyber-attacks are often not identified in real time. Additionally, the sources used were limited to English language mostly, which puts certain limits as well. Furthermore, the global lack of transparency regarding cyber incidents also limits assumption on dataset completeness as information about many attacks is never officially released. Finally, although highly comprehensive, the evidence used for this analysis is time-bound and offers only a snapshot at a specific point in time, focused on English-language sources.

5. Findings, analysis and discussion

As presented in the Table 2, 53 incidents occurred in 2022, 27 in 2023, and 39 in 2024. In 2022, the majority of incidents were recorded in the EU countries and BRICS,[5] with Russia and Germany as leading, while non-EU countries in Eastern Europe and Southeast Europe, but also in Central Asia were significantly affected. The trend shifted in 2023 and 2024 with the largest number of incidents recorded in North America and Asia. The United States stood out as the single most affected country, with Israel emerging as a one of key targets. However, withing the context of Europe, the Southeast Europe, EU countries, Russia and Ukraine remained highly affected in 2023. In 2024, the focus clearly shifted to the United States, with mainly financially motivated attacks, while politically motivated threat actors were dominantly focused on Asia, as new conflicts in the Middle East continued to escalate see (Fig. 2).

The European Union and BRICS were found to be the most frequently impacted in the examined period with 34 incidents each, followed by the United States which recorded 19 cases. Within the European Union, the most affected member state was Germany with 8 incidents, followed by Italy, Spain and France accounting for 3 incidents each, while Russia ranked first within BRICS with 14 incidents. It is important to mention that Israel is ranked fourth in the overall country-level statistics with 7 incidents, followed by India with 6 and Canada with 5 incidents.

The power sector dominated among the most affected sub-sectors with 36 % of incidents recorded, followed by the oil sector and the natural gas sector, accounting for 25 % and 23 %, respectively. Taking into consideration 8 % of incidents in the nuclear sector alone, it additionally reinforces the impression of the power sector's attractiveness and vulnerability, accounting for 44 % in total. In 2022, nuclear energy accounted for about 8 % of world's electricity generation, but slightly less than 1.7 % in global primary energy (BP, 2024). For comparison, the oil and gas sectors, which have shares of 32 % and 24 % in the world's primary energy (BP, 2024), recorded 25 % and 23 % of total incidents, respectively. In terms of the potential impacts of eventual incidents, nuclear facilities possess a wider security risk, that of – an international nuclear crisis.

Several other important trends were identified. Firstly, although power utilities emerged as the dominant group of victims, significant geographical differences and uneven distribution in terms of affected sub-sectors were observed. For instance, the power sector was the most frequent target on all continents except North America, where in the United States and Canada the oil and natural gas industries were at the forefront. More precisely, Canada experienced cyber incidents in these sectors exclusively. Interestingly, despite being among the leading powers in the nuclear sector, neither the United States nor France faced any incidents related to this sub-sector. The nuclear sector also remained unaffected in South America and Australia, while incidents were concentrated on the European and Asian countries. Finally, the district heating sector was affected only in Europe and North America see (Fig. 3).

Financially motivated incidents affected almost exclusively stakeholders operating in the power sector (37 %), the natural gas sector (32 %), and the oil sector (28 %). Regarding geographic distribution, such incidents affected various countries but were predominantly evidenced in North America with the United States at the forefront, as well as in Western, Southern, and Central Europe. Among the politically motivated incidents, hacktivism dominated with 47 %, while espionage accounted for 36 % and sabotage at 16 %. The hacktivism-driven incidents mainly targeted the power sector (41 %), the oil sector (30 %) and the natural gas sector (16 %), while sabotage-driven incidents mostly affected the power sector (38 %), but also the nuclear sector and the oil sector (23 % each), and the natural gas sector (15 %). In terms of sabotage, the most affected countries were those at the center of the most pressing geopolitical developments such as the Russia-Ukraine war and the Israel-Palestine conflict, but also NATO enlargement policy in Europe. Therefore, incidents of sabotage were recorded in Iran, Ukraine, Russia, Canada, Germany, and Scandinavian countries. Similarly, Israel, France, Germany, Russia, Cyprus, Greece, Estonia, Lithuania, Ukraine,

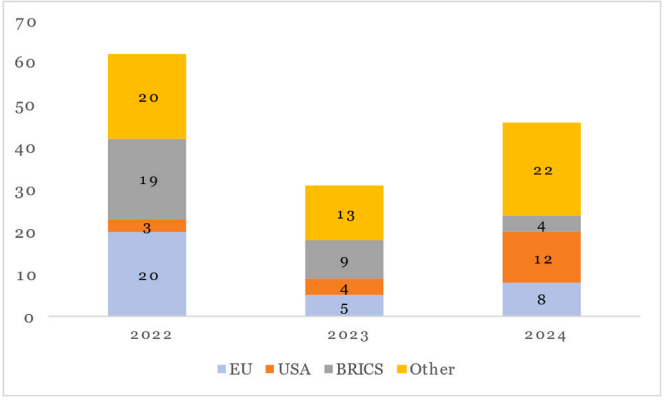


Fig. 2. Geographic distribution of incidents.

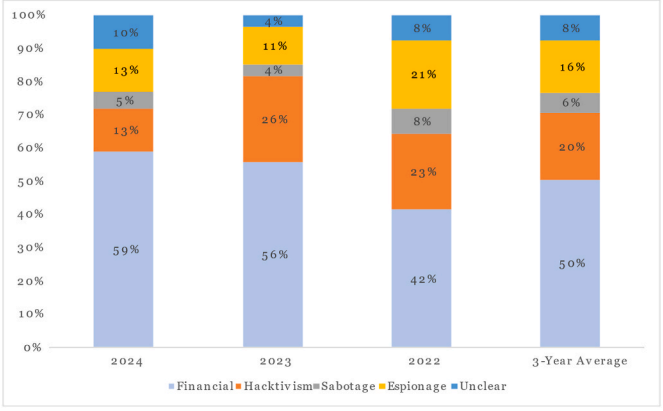


Fig. 3. Annual breakdown of incidents by motivation.

[5] Refers to the intergovernmental organization consisting of Brazil, Russia, India, China and South Africa, but also other countries which achieved full membership status in 2024 and 2025, including Iran, Egypt, Ethiopia, the United Arab Emirates (UAE) and Indonesia.

and some others were often subject to incidents motivated by hacktivism, almost all in close relation to the aforementioned geopolitical events. Finally, the nuclear sector and the power sector were the primary targets of espionage-motivated attacks accounting for 34 % and 23 %, while espionage was the most prevalent across Asia overall, but also in North America and Europe.

Linking the motivation and the impact of incidents reveals an obvious trend showing the predominance of political motives causing operational disruptions, especially hacktivism and also sabotage to a lesser extent. In contrast, in the case of incidents resulting in data theft, the dominant motivation was financial gain (67 %), while political motives are far from negligible (28 %) - with espionage and hacktivism as the main motives. Our findings confirm the results of the European Union Agency for Cybersecurity on ransomware as the dominant type of attack in the energy sector (ENISA, 2024). Notably, a significant number of incidents had an unclear impact, with political motives prevailing (67 %), followed by financial motives (27 %). The majority of incidents were caused by attacks using ransomware (51 %), predominantly resulted in data theft and driven by financial motives. On the other hand, malware-based attacks (17 %) caused both operational disruption and data theft, mainly aiming at espionage and sabotage. It is notable that a significant number of incidents were profiled as attacks of an unspecified type (22 %), resulting in data theft dominantly (72 %), and linked to the power sector (31 %), the oil and natural gas sectors (23 % each) and the nuclear sector (21 %). Additionally, 66 % of these incidents had a political motive, and 21 % a financial motive, where within the political category hacktivism and espionage dominated with 47 % and 37 %, respectively.

The analysis reveals that all types of threat actors were involved in malicious activities targeting the energy sector. Therefore, cybercriminal groups, hacktivists, hackers and crackers, terrorists, corporate cyber groups, espionage gangs, national cyber armies, and secret services (Putnik, 2022) all pose equal threat to the energy security. The specific threat actors, presented in Fig. 4, are discussed in more detail within Section 4.1 and Section 4.2.

One of the most unusual incidents recorded so far and the first of its kind registered in the energy sector took place just an hour before the start of the war in Ukraine, on February 24, 2022. The cyber-attack launched on the European branch of the American telecommunications company Viasat, more precisely on the KA-SAT network, successfully hit 30,000 terminals for satellite communication - SATCOM, including modems in 1217 wind power plants in Germany, i.e. a total of 5800 wind turbines (Egan, 2022; Viasat, 2022). Thus, the energy sector became collateral damage, where the utility lost the possibility to remotely control as much as 11 GW of wind power capacity equaling almost a fifth of electricity generation from wind farms in Germany (Boschetti et al., 2022). This showed how the core element of a national energy system can become an indirect victim of an attack of which it was not the primary target. Furthermore, the incident shows how large an attack can be in terms of the affected capacities which in this specific case exceeded the entire power systems of many countries. Another atypical example is a high-profile cyberattack from 2023 which exploited a widespread vulnerability in the managed file transfer software MOVEit with far-reaching effects on thousands of companies[6] with majority in the United States, but also other countries including Canada, Germany, the UK, Netherlands, Austria, Australia and many more (Kondruss, 2023; PwC, 2024). The responsibility was attributed to a ransomware group Clop, suspected of being a Russian-affiliated cyber gang (SOCRadar, 2023). Like the wind energy case in Germany, the MOVEit breach highlighted the growing risk of indirect threats to the energy sector.

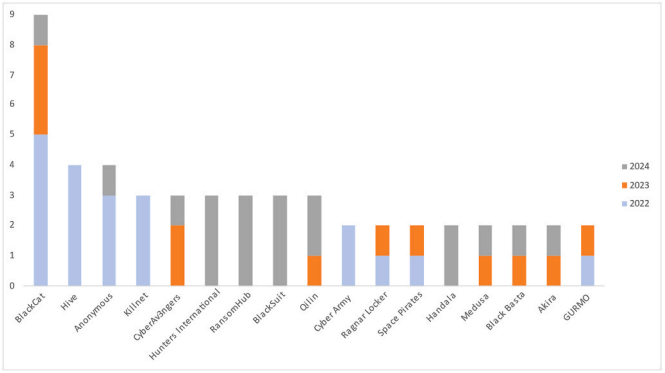


Fig. 4. Overview of the key threat actors in examined period.

5.1. Financially motivated attacks

Over the analyzed period, ransomware groups demonstrated a significant capacity for adaptation, with some groups rebranding and others emerging with new tactics and techniques. This suggests that the trend of refining operations and leveraging sophisticated methods to enhance attacks is set to continue. Most of the observed ransomware-caused incidents were financially motivated, representing typical cybercrime activity. Similarly, most of the financially motivated attacks used ransomware as a priority tool. Based on the characteristics of the suspected responsible group(s) or those who declared responsibility, the majority seem not to have state affiliation. However, the ongoing conflicts provided such ransomware gangs an additional incentive to intensify operations in line with the intensified politically motivated incidents.

As shown in Fig. 4, BlackCat is the most successful group[7] with nine incidents recorded. During 2022, all five incidents caused by BlackCat hit entities in Western Europe, while in 2023 shifted its focus to North America, South America, and Asia. However, the intensity of the group's focus on the energy sector significantly decreased with only one successful attack in 2024. The first incident in the examined period is noteworthy as it impacted companies operating oil terminals in Western Europe just weeks before the war in Ukraine started. The large-scale hacking operation targeted oil port terminal software in at least 17 ports, with two companies falling victim in Germany, one in Belgium, and one in the Netherlands. By paralyzing loading, unloading and logistical systems, the oil operations of some of the major European port facilities were temporarily disrupted as tankers were prevented from delivering oil supplies throughout the region (Baker, 2022). The affected companies in Germany were forced to declare force majeure, while oil company Shell, despite not being directly affected, had to re-route supplies by tankers. Therefore, the Amsterdam-Rotterdam-Antwerp refining hub was seriously disrupted. Just a few days later, the natural gas sector in the United States was hit by a large-scale attack targeting liquified natural gas (LNG) terminals and affecting twenty-one major companies (Robertson and Charpa, 2022). Some of the targeted companies form the backbone of the LNG industry in the United States such as Cheniere Energy, which is the largest LNG exporter in the country, the EQT Corp as the largest natural gas driller and producer in the country, and Kinder Morgan as the largest oil and gas pipeline operator in the country, as well as other important companies such as Chevron (Robertson and Charpa, 2022). While threat actor has not been identified to date, hackers linked to Strontium, a cyber group associated with the Russian intelligence group GRU, are suspected of being responsible (Hope, 2022). When considered in the timing and context of the EU's initial energy trade de-coupling with Russia and re-routing supply

[6] Within the pool of affected companies, about twenty were energy-related and confirmed as victims, including Shell, Chevron, Siemens Energy, Schneider Electric, and others.

[7] BlackCat, also known as ALPHV, is believed to be a successor of the ransomware operators REvil, DarkSide, and BlackMatter.

mostly toward the United States, these two incidents had serious short-term consequences for the energy security of both the European Union and the United States.

The other important actors to follow are Hunters International, RansomHub, BlackSuit, and Qilin, each recording three successful attacks since December 2023. BlackSuit group exclusively targeted oil and gas companies, classified as a typical cybercrime-oriented threat actor, similar to Qilin and RansomHub gangs. The same characteristics are attributed to Hunters International, but the group's formation is believed to relate to the former Hive group which was neutralized in January 2023. At the time, Hive had already carried out four successful attacks in 2022 alone. Currently, RansomHub is highlighted as the number one ransomware group in terms of the success of its activities overall (Symantec, 2024). Regardless of their minor success in the energy sector, it is important to mention other threat actors such as BlackBasta, which is believed to comprise former members of the Conti and REvil threat groups (Flashpoint Intel Team, 2024), and Akira, which operates as an affiliate-based ransomware group providing its software and infrastructure to other cybercriminal groups (Singapore Police Force, 2024). In addition to those major players, dozens of other successful threat actors have used ransomware techniques for malicious activities in the energy sector.

In terms of the consequences, although financially motivated ransomware incidents did not cause serious operational problems, but rather short-term operational disruptions, the financial losses, data theft, and reputational damage were significant. Moreover, data breach which often led to later distribution and offer of stolen information on illegal markets could enable other threat actor(s), with different motives, to purchase the information necessary to facilitate their tactics in future attacks. There were not recorded specific cases of a victim entity paying the ransom demanded in exchange for data encryption and not leaking allegedly stolen information such as was the case with the Colonial pipeline cyber incident in 2021. However, it was evidenced that the most ransomware incidents in 2024 involved ransom demands higher than one million dollars, while the average recovery costs amounted to approximately three million dollars per incident, which is four times higher than in 2023 (Sophos, 2024).

5.2. Politically motivated attacks

The greater focus of the research was on politically motivated attacks due to their potentially far-reaching implications for energy security. Following the outbreak of war between Russia and Ukraine in 2022 and between Israel and Palestine in 2023, numerous high-profile cyber operations ensued. These events did not only mobilize the resources of the opposing sides but also those of actors worldwide, intensifying the cyber playing field significantly. Furthermore, ongoing great power competition and overall global instability also induced a wave of malicious activities with varying goals. Therefore, the examined period abounds in examples of cyber espionage campaigns which significantly vary in their motives, targeted energy supply chain elements, geographic distribution, sophistication, duration, success, and complexity. Furthermore, hacktivism remained closely linked to major geopolitical developments, while attacks aimed at causing sabotage, albeit not as numerous, persisted at a steady level.

On the same day as the war in Ukraine started in 2022, the international decentralized hacker community Anonymous declared a cyber war against the Government of Russia (Anonymous, 2022a), launching a series of coordinated attacks. Consequently, numerous companies in the energy sector became direct victims either of DDoS attacks or massive data breaches, with stolen information made public. Anonymous also announced another cyber war, against Iran in September 2022, following the start of a wave of anti-regime protests as a reaction to the death of Mahsa Amini (Anonymous, 2022b). Following the outbreak of the Israel-Palestine military conflict in 2024, Anonymous launched third cyberwar campaign targeting Greece as a response to the country's support for Israel and successfully compromised several energy companies (FalconFeeds.io., 2023). The multi-day campaign against Cyprus, launched by LulzSec Black as a response to relations with Israel, included energy companies and was also the result of a cyberwar related to geopolitical developments. ("LulzSec Black Targets", 2024).

Cyberattacks occurring under the umbrella of the Russia-Ukraine conflict included several cases with disruptive cyber-physical capabilities. As previously mentioned, Industroyer2 malware was employed by the elite hacking group Sandworm, believed to be state-sponsored (Barnett, 2024), which has been singled out as the most significant actor to monitor in terms of its potential for devastating impacts. Some of Sandworm's malicious activities, which used a novel technique for impacting industrial control systems caused incidents, such as the short power outage in 2022 as a consequence of multi-month access to the SCADA system operating substations in Ukraine (Mandiant, 2023), while others were timely prevented as in the case of the plan to disrupt approximately twenty entities in the critical infrastructure sector including energy across ten Ukrainian regions in 2024 (CERT-UA, 2024). Furthermore, the Sandworm is also suspected of being one of the actors involved in the largest coordinated cyberattack ever recorded in Denmark where more than twenty companies operating energy infrastructure were targeted (Paganini, 2023c; SectorCERT, 2023; PwC, 2024).

Like the war in Ukraine, the outbreak of the military conflict between Israel and Palestine, and the tense geopolitical landscape in the region, initiated cyber activities on both sides mobilizing a variety of interested actors, especially Iran. For instance, the Cyber Av3ngers group targeted the power system operator and power utility in Israel[8] on the first day of the conflict (Avantika, 2023), while the hacktivist group had already claimed responsibility for the incident at the Bazan Group oil company earlier in July 2023 (Sharma, 2023). As well as being the victim of the CyberAv3ngers' attack, the Bazan Group was also targeted by Anonymous Sudan in January 2024 (Anonymous Sudan Targets Bazan Group, 2024). Additionally, an Iran-affiliated Handala threat actor carried out two successful incidents in the energy sector of Israel (Dimitrov, 2024). Importantly, the Israel-affiliated group Predatory Sparrow caused operational disruptions in Iran's fuel distribution, hitting approximately 70 % of gas stations across the country (Paganini, 2023a). This group is well-known for its highly developed capabilities and destructive cyber-physical potential having caused a fire in Iran's steel industry in 2022 (Tidy, 2022).

Focusing further on malicious activities aimed at espionage, the example of the US-China cyber confrontation over the threat actor Volt Typhoon indicates that the digital field has also become an area of reputational interest in addition to that of direct security. In 2024, China was accused by intelligence agencies from Western countries of implementing a large-scale cyber espionage campaign on critical infrastructure in the United States (Cybersecurity & Infrastructure Security Agency, 2023; Microsoft Threat Intelligence, 2023; Cybersecurity & Infrastructure Security Agency, 2024; Microsoft, 2024). The accusation followed a previous series of alerts from 2023, issued by the Five Eyes[9] intelligence alliance, warning that Chinese government-linked espionage campaigns might target critical infrastructure in those countries, primarily via Volt Typhoon (Cybersecurity & Infrastructure Security Agency, 2023; U.S. Department of Justice, 2024). It was subsequently disclosed that the threat actor had already infiltrated various systems of entities operating critical infrastructure in the United States back in 2023, with more than twenty pipeline operators being targeted (Bing, 2024). These espionage-related cyber threats did not involve Volt Typhoon alone, but clusters of threat actors carrying out multiple coordinated activities (Mandiant, 2024b). As a result of this open confrontation, China responded by its own investigation and releasing a

[8] Israel Independent System Operator (Noga) and Israel Electric Corporation.
[9] The United States, Great Britain, Canada, Australia, and New Zealand.

series of reports, strongly denying any links to Volt Typhoon and counter-accusing the United States of not only being behind this threat actor, but also of being strategically engaged in a long-term, large-scale espionage campaign against rival countries, as well as numerous allies such as Germany and France (National Computer Virus Emergency Response Center and National Engineering Laboratory for Computer Virus Prevention Technology, 2024a, 2024b, 2024c).

However, there were further incidents also attributed to the threat actors suspected of being China-affiliated such as espionage campaign targeting the energy sector among others, occurring simultaneously in Russia, Georgia, and Mongolia in 2023. The attack was launched by the Space Pirates group, using diverse malicious tools including three previously undocumented modular malware (Toulas, 2022a; PT Expert Security Center, 2022). Furthermore, the national electricity network of an unnamed Asian country was compromised by a 6-month cyber espionage operation (Hollingworth, 2023), carried out by the threat actor group Redfly in 2023 (Symantec, 2023). Finally, a sophisticated campaign utilizing advanced techniques was conducted by the Earth Baxia group, targeting the energy sector in South Korea, Thailand, the Philippines, Taiwan, Vietnam and China, in addition to other government agencies and telecommunication (Lee et al., 2024). China's nuclear sector was also the victim of an incident in 2023 attributed to South Asia-based threat group Bitter APT specializing in cyber espionage (Arghire, 2023; Robinson, 2023). Other countries were also implicated in certain incidents, especially North Korea in the case of the threat actor Lazarus, suspected of being backed by the government (Threat Intelligence, 2022). This espionage group compromised the energy and aerospace industries in the United States in 2024 (Ribeiro, 2024b; Mandiant, 2024a), a Russian nuclear energy organization in May 2023 (Burt, 2023), and energy companies in Japan, and Canada, and the United States (Adriano, 2022; Kapko, 2022).

The research also found a wide global espionage campaign targeting the nuclear sector, discovered in 2022, with the victims including institutions and facilities in Russia, Brazil and Taiwan[10] in February, August and September 2022, respectively, as well as in Indonesia, India and Iran[11] in October 2022, and South Africa[12] in November 2022 ("CyberThreats Mushrooming", 2022a). Not only was this espionage campaign successfully carried out, but documentation was subsequently published containing operational plans, confidential reports, management instructions, and similar data of exceptional value to the security of the nuclear sector. The responsible threat actor is yet unknown, while the Black Reward claimed responsibility only for the incident in Iran (SOCRadar, 2022).

Additionally, the espionage-motivated threat actor Yoro Trooper, believed to be Kazakhstan-associated, conducted two campaigns in 2022 and 2023, mainly targeting countries in Eastern Europe and the Community of Independent States (CIS),[13] but also EU and Turkey (Malhotra & Ventura, 2023a, 2023b). A long-term international espionage campaign in the South China Sea was discovered in 2022, attributed to Red Ladon/TA423 or APT40, targeting entities involved in offshore drilling and deep-water oil and gas exploration in the Kasawari gas field off the coast of Sarawak in Malaysia, as well as those in the offshore windfarm projects in the Strait of Taiwan, precisely in the construction of the Yunlin Offshore Windfarm (Raggi and Scenarelli, 2022; Subramanian, 2023). Another espionage campaign uncovered in 2022 targeted the wider international RES-related industry. Ongoing since 2019, this large-scale campaign conducted by Russia-linked APT28[14] and North Korea-linked Konni, targeted renewable energy companies, industrial technology entities, and environmental protection organizations including the Kardzhali Hydroelectric Power Station and CEZ Electro in Bulgaria (Bushido, 2022; Toulas, 2022b; Ribeiro, 2022). Finally, numerous private energy entities in India experienced data breaches at the beginning of 2024, caused by malware deployed by an unidentified threat actor within a wider espionage campaign, resulting in compromised information regarding on oil and natural gas drilling activities (Büyükkaya, 2024).

To conclude, the trend of politically motivated cyber activities seems likely to continue to escalate in the future. Combined with the rapid spread of global political turmoil, military conflicts and open rivalries, which have intensified great power competition and overall political instability, the motives for such incidents have multiplied. Given such global dynamics along with the constantly growing sophistication of threat actors, and the application of artificial intelligence in malicious activities, which is identified as a major emerging source of cyber threats (WEF, 2025), cyber security risks in the energy sector are expected to undoubtedly grow in frequency, intensity, and impact.

6. Conclusion

Despite the limited number of cyber-physical examples, the analysis shows the continued emergence of new threats to energy security. At the same time, our paper highlights the fragility of the information systems and digital solutions used in energy sector. The findings indicate that no energy sub-sector is invulnerable, regardless of a state's level of technological development, economic and financial capability, military power, or global political influence. This suggests that the practice of energy security has entered a transformative period, with the digital dimension equal to the physical, but also that the security of supply and security of critical infrastructure are equally important aspects of energy security.

The research demonstrates that all types of threats are simultaneously present, increasing in intensity, sophistication, and impact potential. The cyber threat landscape is characterized by a diverse set of actors, including state-sponsored groups, cybercriminals, and hacktivists, often with overlapping agendas and motivations ranging from financial gain to political leverage, geostrategic and industrial competition, and physical disruption. Notably, collaboration between state and non-state actors is also increasing, serving to support geopolitical agendas in particular regions of interest and advance strategic goals.

It is also noticeable that although financial motivation still dominates attacks, incidents increasingly have a certain political connotation due to geopolitical rivalry and armed conflicts. This is evident in increasingly frequent extensive espionage campaigns or the creation of sophisticated, specially designed tools capable of inflicting far-reaching consequences. Therefore, the theoretical paradigm of energy security should not be considered static framework within the context of dynamic and fragmented international relations, but one which must be able to adapt to reflect reality, while policymakers should fully recognize cyber threats by placing them at the forefront of modern energy security doctrines.

Security of energy infrastructure as critical, covering both physical and cyber assets, reflects resilience as a missing component of understanding the energy security paradigm. Having universal risks, without distinction between importing or exporting countries, the security of energy infrastructure recognizes energy security risks of extreme weather risks, cyber risks and physical risks. By merging the principles of security of supply and security of critical infrastructure under the umbrella of the security studies approach, the conceptual framework of the energy security of a country is enhanced and strengthened.

[10] Joint Institute for Nuclear Research in Russia, utility Taipower in Taiwan and nuclear utility in Brazil.

[11] Indonesian nuclear power authority, the Atomic Energy Organization in Iran, the Nuclear Power Corporation of India (NPCIL) and the Thailand Institute of Nuclear Technology.

[12] Koeberg Nuclear Power Station.

[13] Namely Russia, Belarus, Azerbaijan, Tajikistan, Uzbekistan, and Kyrgyzstan.

[14] Also known as Fancy Bear.

CRediT authorship contribution statement

Filip Marković: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Ana Kovačević:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Methodology, Investigation, Formal analysis, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

Abrams, L., 2023. Colombian energy supplier EPM hit by BlackCat ransomware attack. Bleeping Computer. https://www.bleepingcomputer.com/news/security/colombian-energy-supplier-epm-hit-by-blackcat-ransomware-attack/.

Adams, R.J., Smart, P., Huff, A.S., 2016. Shades of grey: guidelines for working with the grey literature in systematic reviews for management and organizational studies. Int. J. Manag. Rev. 19 (4), 432–454. https://doi.org/10.1111/ijmr.12102.

Adriano, L., 2022. State-Sponsored Hackers Exploit Vulnerability to Hit Energy Providers. Insurance Business America. https://www.insurancebusinessmag.com/us/news/cyber/statesponsored-hackers-exploit-vulnerability-to-hit-energy-providers-420096.aspx.

AFP, 2022. Hackers target German branch of Russian oil giant rosneft. Security. https://www.securityweek.com/hackers-target-german-branch-russian-oil-giant-rosneft/.

Agencies, 2023. Ransomware attack on state-run power management firm's IT system in Madhya Pradesh. ETGovernment. https://government.economictimes.indiatimes.com/news/secure-india/ransomware-attack-on-state-run-power-management-firms-it-system-in-madhya-pradesh/100579139.

Aljohani, T.M., 2024. Cyberattacks on energy infrastructures as modern weapons—part I: analysis and motives. IEEE Technol. Soc. Mag. 43 (2), 59–69. https://doi.org/10.1109/MTS.2024.3395688.

Al-Mhiqani, M.N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z.Z., Ali, N.S., Abdulkareem, K.H., 2018. Cyber-security incidents: a review cases in cyber-physical systems. Int. J. Adv. Comput. Sci. Appl. 9 (1), 499–508. https://doi.org/10.14569/IJACSA.2018.090169.

Alsalama, A.M., Alzahrani, M.S., 2024. Cybersecurity in oil & gas 4.0: a systematic literature review of challenges, threats, and mitigating measures. *ADIPEC*, SPE-222581-MS. SPE. https://doi.org/10.2118/222581-ms.

An In-Depth Look at Russian Threat Actor, 2022. Killnet. Avertium. https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-russian-threat-actor-killnet.

An Update on the Pro-Russia Threat Actor, 2023. Killnet. Avertium. https://www.avertium.com/resources/threat-reports/an-update-on-pro-russia-threat-actor-killnet.

Analysing operation FlightNight: a cyber espionage campaign targeting Indian government and energy sectors. Foresiet, 2024. https://foresiet.com/blog/analysing-operation-flightnight-a-cyber-espionage-campaign-targeting-indian-government-and-energy-sectors.

Anderson Feazel Management Data Breach Investigation, 2024. Strauss borelli PLLC. https://straussborrelli.com/2024/09/19/anderson-feazel-management-data-breach-investigation/.

Anonymous Sudan Targets Bazan Group, 2024. CyberMaterial. https://cybermaterial.com/anonymous-sudan-targets-bazan-group/.

Anonymous TV. [@YourAnonTV], 2022. Just in: #anonymous hacked 116,500 emails (130 GB. In: From SOCAR Energoresource, which Operates the Antipinsky Refinery and Several Oilfields, vol. X. *#OpRussia* [Post]. https://x.com/YourAnonTV/status/1525122853389090818.

Anonymous. [@YourAnonOne], 2022a. *The anonymous collective launches a cyber operation against Russian government* [Post]. X. https://twitter.com/YourAnonOne/status/1496965766435926039?t=KJCNbnozwLnlp05qL_q2Wg&s=19.

Anonymous. [@YourAnonOne], 2022b. The Anonymous Collective Launches a Cyber Operation Against the Iranian Government. *#Anonymous #OpIran* [Post], p. X. https://twitter.com/YourAnonOne/status/1572305056489168896?t=2q4i9DBab0zs0eNJ85QxCg&s=19.

Antoniuk, D., 2022. Ukraine's state-owned nuclear power operator said Russian hackers attacked website. The Record. https://therecord.media/ukraines-state-owned-nuclear-power-operator-said-russian-hackers-attacked-website.

Antoniuk, D., 2023. Hacktivists take sides in Israel-Palestinian war. The Record. https://therecord.media/hacktivists-take-sides-israel-palestinian.

APERC, 2007. A Quest for Energy Security in the 21st Century: Resources and Constraints. Asia Pacific Energy Research Centre, Institute of Energy Economics. https://aperc.or.jp/file/2010/9/26/APERC_2007_A_Quest_for_Energy_Security.pdf.

Arghire, I., 2022. Hacktivists leak data allegedly stolen from Russian energy giant transneft. Securit. Week. https://www.securityweek.com/hacktivists-leak-data-allegedly-stolen-russian-energy-giant-transneft/.

Arghire, I., 2023. China's nuclear energy sector targeted in cyberespionage campaign. Security. https://www.securityweek.com/chinas-nuclear-energy-sector-targeted-in-cyberespionage-campaign/.

Avantika, C., 2023. Israel-Hamas cyber war: a comprehensive analysis. The Cyber Express. https://thecyberexpress.com/analysis-of-the-israel-hamas-cyber-war/.

Ayodeji, A., Mohamed, M., Li, L., Di Buono, A., Pierce, I., Ahmed, H., 2023. Cyber security in the nuclear industry: a closer look at digital control systems, networks and human factors. Prog. Nucl. Energy 161, 104738. https://doi.org/10.1016/j.pnucene.2023.104738.

Azzuni, A., Breyer, C., 2018a. Definitions and dimensions of energy security: a literature review. WIREs Energy and Environment 7 (1), e268. https://doi.org/10.1002/wene.268.

Azzuni, A., Breyer, C., 2018b. Energy security and energy storage technologies. Energy Proc. 155, 237–258. https://doi.org/10.1016/j.egypro.2018.11.053.

Baek, D.S., 2024. Ransomware attacks targeting critical infrastructure: electricity, energy, and water. Medium. https://medium.com/@davidsehyeonbaek/ransomware-attacks-targeting-critical-infrastructure-electricity-energy-and-water-c7b2e5f79d31.

Baker, M.R., 2022. Ransomware Attacks Targeting Western European Oil Port Terminals. Baker Botts. https://www.bakerbotts.com/thought-leadership/publications/2022/february/ransomware-attacks-targeting-western-european-oil-port-terminals.

Baldwin, A., 1997. The concept of security. Rev. Int. Stud. 23 (1), 5–26. https://doi.org/10.1017/S0260210597000053.

Barnett, P., 2024. Understanding sandworm, a state-sponsored threat group. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2024/understanding-sandworm-a-state-sponsored-threat-group#19.

Beer, E., 2022. Major German oil supplier confirms cyber-attack – "Oiltanking" says incident has crippled inland supply. Stacks. https://www.thestack.technology/oiltanking-cyber-attack/.

Beerman, J., Berent, D., Falter, Z., Bhunia, S., 2023. A review of colonial pipeline ransomware attack. 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), pp. 8–15. https://doi.org/10.1109/CCGridW59191.2023.00017.

Behind the News, 2022. The ragnar locker attack on Greek natural gas supplier DESFA. Radiflow. https://www.radiflow.com/blog/behind-the-news-the-ragnar-locker-attack-on-greek-natural-gas-supplier-desfa/.

Benzies, K.M., Premji, S., Hayden, K.A., Serrett, K., 2006. State-of-the-Evidence reviews: advantages and challenges of including grey literature. Worldviews Evidence-Based Nurs. 3 (2), 55–61. https://doi.org/10.1111/j.1741-6787.2006.00051.x.

Bharathidasan, M., Indragandhi, V., Suresh, V., Jasiński, M., Leonowicz, Z., 2022. A review on electric vehicle: technologies, energy trading, and cyber security. Energy Rep. 8, 9662–9685. https://doi.org/10.1016/j.egyr.2022.07.145.

Bing, C., 2024. FBI Says Chinese Hackers Preparing to Attack US Infrastructure. Reuters. https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18/.

Boero, A., 2024. ENGIE : un groupe de hackers revendique le piratage de données sensibles de clients, le fournisseur confirme. Clubic. https://www.clubic.com/actualite-526124-engie-un-groupe-de-hackers-revendique-le-piratage-de-donnees-sensibles-de-clients-du-fournisseur-d-energie.html.

Boschetti, N., Gordon, N.G., Falco, G., 2022. Space Cybersecurity Lessons Learned from the ViaSat Cyberattack. *Ascend*, AIAA 2022-4380. American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.2022-4380.

BP, 2024. bp energy outlook: 2024 edition. https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/energy-outlook/bp-energy-outlook-2024.pdf.

Brodersen, J., 2023. LockBit suma a otra empresa argentina entre sus víctimas de ransomware: Grupo Albanesi. Clarinet. https://www.clarin.com/tecnologia/lockbit-suma-empresa-argentina-victimas-ransomware-grupo-albanesi_0_BMKf1P4dVj.html.

Bronk, C., 2014. *Hacks on gas: energy, cybersecurity, and U.S. defense*. James A. Baker III institute for public policy of rice university. https://www.bakerinstitute.org/sites/default/files/2014-02/import/Pub-IT-HacksonGas-020514.pdf.

Burdett, S., Stewart, L.A., Tierney, J.F., 2003. Publication bias and meta-analyses: a practical example. Int. J. Technol. Assess. Health Care 19 (1), 129–134. https://doi.org/10.1017/s0266462303000126.

Burt, T., 2023. Espionage fuels global cyberattacks. Microsoft. https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/.

Bushido, Token, 2022. Tracking A renewable energy intelligence gathering campaign. @BushidoToken Threat Intel. https://blog.bushidotoken.net/2022/01/tracking-renewable-energy-intelligence.html.

Büyükkaya, A., 2024. Operation FlightNight: indian government entities and energy sector targeted by cyber espionage campaign. EclecticlQ. https://blog.eclecticiq.com/operation-flightnight-indian-government-entities-and-energy-sector-targeted-by-cyber-espionage-campaign.

BVIEC falls victim to cyber-attack- electricity company's internal & external operations affected, 2024. Virgin Islands news online. https://www.virginislandsnewsonline.com/en/news/bviec-falls-victim-to-cyber-attack.

CERT-EU, 2022a. Cyber security brief - november 2022. https://cert.europa.eu/publications/threat-intelligence/cb22-12/pdf.

CERT-EU, 2022b. Cyber brief - may 2022. https://cert.europa.eu/publications/threat-intelligence/cb22-06/pdf.

CERT-EU, 2022c. Cyber security brief - november 2022. https://cert.europa.eu/publications/threat-intelligence/cb22-12/pdf.
CERT-EU, 2022d. Cyber brief - august 2022. https://cert.europa.eu/publications/threat-intelligence/cb22-09/pdf.
CERT-EU, 2022e. Cyber brief - july 2022. https://cert.europa.eu/publications/threat-intelligence/cb22-08/pdf.
CERT-EU, 2022f. Cyber brief - june 2022. https://cert.europa.eu/publications/threat-intelligence/cb22-07/pdf.
CERT-EU, 2023a. Cyber security brief 23-11 - october 2023. https://cert.europa.eu/publications/threat-intelligence/cb23-11/pdf.
CERT-EU, 2023b. Cyber security brief (march 2023). https://cert.europa.eu/publications/threat-intelligence/cb23-04/pdf.
CERT-EU, 2023c. Cyber security brief 23-03 - february 2023. https://cert.europa.eu/publications/threat-intelligence/cb23-03/pdf.
CERT-EU, 2023d. Cyber security brief - april 2023. https://cert.europa.eu/publications/threat-intelligence/cb23-05/pdf.
CERT-UA, 2024. Плани UAC-0133 (Sandworm) ⅋одо кібердиверсії на МайЖе 20 об'єктах критичної інфраструктури України. https://cert.gov.ua/article/6278706.
Cherp, A., Jewell, J., 2014. The concept of energy security: beyond the four as. Energy Policy 75, 415–421. https://doi.org/10.1016/j.enpol.2014.09.005.
Chester, L., 2010. Conceptualising energy security and making explicit its polysemic nature. Energy Policy 38 (2), 887–895. https://doi.org/10.1016/j.enpol.2009.10.039.
CMC, 2024. Belize Electricity Limited has Had its IT Network Hacked. Caribbean Today. https://www.caribbeantoday.com/fr/sections/news-2/belize-electricity-limited-has-had-its-it-network-hacked.
Croft, D., 2024. Major US fuel distributor allegedly breached by black basta. Cyber Daily. https://www.cyberdaily.au/security/10606-major-us-fuel-distributor-allegedly-breached-by-blackbasta.
Cyber Threat Intelligence, 2023. Ransomware attacks against the energy sector on the rise - nuclear and oil & gas are major targets in 2024. Resecurity. https://www.resecurity.com/blog/article/ransomware-attacks-against-the-energy-sector-on-the-rise-nuclear-and-oil-gas-are-major-targets-2024.
Cyberangriff beim Darmstädter Energieversorger Entega. Heise Online. https://www.heise.de/news/Cyberangriff-beim-Darmstaedter-Energieversorger-Entega-7138161.html.
CyberAveng3rs. [@CyberAveng3rs], 2024. We (CyberAv3ngers) took electricity transmission lines and dispatching power plants of Tel Aviv out of the circuit! [Post]. X. https://x.com/CyberAveng3rs/status/1779221896891953314.
Cybersecurity & Infrastructure Security Agency, 2023. People's Republic of China state-sponsored cyber actor living off the land to evade detection. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.
Cybersecurity & Infrastructure Security Agency, 2024. PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.
CyberThreats Mushrooming over Global Nuclear Facilities, 2022. Cyble. https://cyble.com/blog/cyberthreats-mushrooming-over-global-nuclear-facilities/.
D'Andrea, A., 2023. Cyberattacks on Canada's Gas Infrastructure Left 'No Physical Damage,' Trudeau Says. Global News. https://globalnews.ca/news/9614872/cyberattack-gas-infrastructure-justin-trudeau/.
Dagoumas, A., 2019. Assessing the impact of cybersecurity attacks on power systems. Energies 12 (4), 725. https://doi.org/10.3390/en12040725.
Di Pinto, A., Dragoni, Y., Carcano, A., 2018. TRITON: the first ICS cyber attack on safety instrument systems. Nozomi Networks [Research Paper]. https://i.blackhat.com/us-18/Wed-August-8/us-18-Carcano-TRITON-How-It-Disrupted-Safety-Systems-And-Changed-The-Threat-Landscape-Of-Industrial-Control-Systems-Forever-wp.pdf.
Diaba, S.Y., Shafie-khah, M., Elmusrati, M., 2024. Cyber-physical attack and the future energy systems: a review. Energy Rep. 12, 2914–2932. https://doi.org/10.1016/j.egyr.2024.08.060.
Dimitrov, F., 2024. Inside the handala hack: iranian cyber warfare and the rise of wiper attacks targeting Israeli systems. OP Innovative. https://op-c.net/blog/handala-hack-cyber-warfare-wiper-attacks-on-israel/.
Ding, S., Gu, W., Lu, S., Yu, R., Sheng, L., 2022. Cyber-attack against heating system in integrated energy systems: model and propagation mechanism. Appl. Energy 311, 118650. https://doi.org/10.1016/j.apenergy.2022.118650.
Dinger, A., Brause, C., Bewarder, M., 2022. Hacker Treffen Deutsche Rosneft-Tochter. Welt. https://www.welt.de/politik/deutschland/article237518665/Rosneft-Deutsche-Tochter-wurde-Ziel-eines-Cyberangriffs.html.
Dinicu, A., Oancea, R., Bârsan, G., 2021. The multidimensional impact on society of cyber attacks targeting the energy critical infrastructure sector. Land Forces Academy Review 26 (4), 406–417. https://doi.org/10.2478/raft-2021-0053.
Dragos, 2023a. ICS/OT cybersecurity year in review 2022. https://www.dragos.com/year-in-review/#section-report.
Dragos, 2023b. 2022 ICS/OT Threat Landscape Recap & what to Watch for This Year. Dragos Blog. https://www.dragos.com/blog/2022-ics-ot-threat-landscape-recap-what-to-watch-for-this-year/.
Dupont, B., Fortin, F., Leukfeldt, R., 2024. Broadening our understanding of cybercrime and its evolution. J. Crime Justice 47 (4), 435–439. https://doi.org/10.1080/0735648X.2024.2323872.
ECG Lost Nearly GH'500 Million due to Ransomware Attack - Managing Director Confirms, 2024. Electricity Company of Ghana Limited. https://www.ecg.com.gh/index.php/fr/media-centre/news-events/ecg-lost-nearly-gh-500-million-due-to-ransomware-attack-managing-director-confirms.
EclecticIQ Threat Research Team, 2022. Killnet Effectively Amplifies Russian Narratives but Has Limited Ddos Capabilities. EclecticIQ. https://blog.eclecticiq.com/killnet-effectively-amplifies-russian-narratives-but-has-limited-ddos-capabilities.
Egan, M., 2022. *A Retrospective on 2022 Cyber Incidents in the Wind Energy Sector and Building Future Cyber Resilience* [Graduate Student Project. Boise State University. https://scholarworks.boisestate.edu/cyber_gradproj/3.
Egon, N., 2023. Engie : les données de 110.000 clients ont fuité à cause d'une cyberattaque. Economie Matin. https://www.economiematin.fr/engie-les-donnees-de-110-000-clients-ont-fuite-a-cause-dune-cyberattaque.
Empresa De Energia Del Bajo Putumayo, 2024. Breachsense. https://www.breachsense.com/breaches/empresa-de-energia-del-bajo-putumayo-data-breach/.
ESET, 2022. Threat report T1 2022. https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf#page=4ese.
European Union Agency for Cybersecurity, 2024. ENISA threat landscape 2024: july 2023 to June 2024. https://doi.org/10.2824/0710888.
Facchinetti, S., Osmetti, S.A., Tarantola, C., 2023. Network models for cyber attacks evaluation. Soc. Econ. Plann. Sci. 87, 101584. https://doi.org/10.1016/j.seps.2023.101584.
FalconFeeds.io. [@FalconFeedsio], 2023. Anonymous Collective is Starting a Cyber Attack Campaign Against Greece with Name OpGreece, vol. X [Post]. https://x.com/FalconFeedsio/status/1732679719794139386?s=20.
FalconFeeds.io. [@FalconFeedsio], 2024a. Abyss Ransomware Alert [Post]. X. https://x.com/FalconFeedsio/status/1843947925141098590.
FalconFeeds.io. [@FalconFeedsio], 2024b. BLACK SUIT Ransomware Alert. https://x.com/FalconFeedsio/status/1840726962979090779.
FalconFeeds.io. [@FalconFeedsio], 2024c. Sonol Data Breach X [Post]. https://x.com/FalconFeedsio/status/1811419867901513814.
FalconFeeds.io. [@FalconFeedsio], 2024d. HUNTERS INTERNATIONAL Ransomware Alert. https://x.com/FalconFeedsio/status/1810738447533101194.
FalconFeeds.io. [@FalconFeedsio], 2024e. Hyde Fuel Falls Victim to Qilin Ransomware [Post]. X. https://x.com/FalconFeedsio/status/1800945358194999311.
Farwell, J.P., Rohozinski, R., 2011. Stuxnet and the future of cyber war. Survival 53 (1), 23–40. https://doi.org/10.1080/00396338.2011.555586.
Flashpoint Intel Team, 2024. From origins to operations: understanding black basta ransomware. Flashpoint. https://flashpoint.io/blog/understanding-black-basta-ransomware/.
Gatlan, S., 2024. New tickler malware used to backdoor US govt, defense orgs. Bleeping Computer. https://www.bleepingcomputer.com/news/security/APT33-Iranian-hacking-group-uses-new-tickler-malware-to-backdoor-us-govt-defense-orgs/.
Gatlan, S., 2024a. Romanian energy supplier electrica hit by ransomware attack. Bleeping Computer. https://www.bleepingcomputer.com/news/security/romanian-energy-supplier-electrica-hit-by-ransomware-attack/.
Gatlan, S., 2024b. Lynx ransomware behind electrica energy supplier cyberattack. Bleeping Computer. https://www.bleepingcomputer.com/news/security/lynx-ransomware-behind-electrica-energy-supplier-cyberattack/.
Gazula, M.A., 2017. *Cyber Warfare Conflict Analysis and Case Studies* [Master Thesis. Boston University. https://dspace.mit.edu/bitstream/handle/1721.1/112518/1012611628-MIT.pdf?sequence=1&isAllowed=y.
Gitelman, L., Magaril, E., Kozhevnikov, M., 2023. Energy security: new threats and solutions. Energies 16 (6), 2869. https://doi.org/10.3390/en16062869.
Gjesvik, L., Szulecki, K., 2023. Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout. Eur. Secur. 32 (1), 104–124. https://doi.org/10.1080/09662839.2022.2082838.
Glover, C., 2022. Hive ransomware gang strikes Indonesian gas giant PGN. Tech Monitor. https://www.techmonitor.ai/technology/cybersecurity/hive-ransomware-gang-pgn.
Glover, C., 2023. LockBit ransomware spree hits three large companies. Tech Monitor. https://www.techmonitor.ai/technology/cybersecurity/lockbit-spree-hits-three-large-companies?cf-view.
Gonzalez, Z.P., 2024. Belize Electricity Limited Confirms Cyber Leak of over 10,000 Customer Application Forms. Breaking Belize News. https://www.breakingbelizenews.com/2023/07/19/belize-electricity-limited-confirms-cyber-leak-of-over-10000-customer-application-forms/.
Goud, N. (n.d.). Sophisticated ransomware attack on oil India limited triggers fuel supply concerns. Cyber Security Insiders. https://www.cybersecurity-insiders.com/sophisticated-ransomware-attack-on-oil-india-limited-triggers-fuel-supply-concerns/.
Greenwood, J., 2022. ATW hackers linked with anonymous breached into Russian energy giant. The Cyber Security Times. https://www.thecybersecuritytimes.com/atw-hackers-linked-to-anonymous-breached-into-russian-energy-giant/.
Greig, J., 2022. Conti ransomware attack was aimed at destabilizing government transition, Costa Rican president says. Record. https://therecord.media/conti-ransomware-attack-was-aimed-at-destabilizing-government-transition-costa-rican-president-says.
Greig, J., 2023. Ohio's largest oil producer says 'no impact' seen after cyberattack. Record. https://therecord.media/encino-energy-cyberattack-alleged-data-leak-alphv.
Greig, J., 2024. Costa Rica state energy company calls in US experts to help with ransomware attack. The Record. https://therecord.media/costa-rica-state-energy-company-ransomware.
HackManac. [@H4ckManac], 2024a. *#CyberAttack(s) alert* [Post]. X. https://x.com/H4ckManac/status/1788658201090539637.
HackManac. [@H4ckManac], 2024b. Cyberattack alert [Post]. X. https://x.com/H4ckManac/status/1843979116691005706.
HackManac. [@H4ckManac], 2024c. *Cyberattack alert* [Post]. X. https://x.com/H4ckManac/status/1838457682673434747.
Halcon Tech, 2025. The halcyon attacks lookout database. https://www.halcyon.ai/attacks.

Halder, T., 2014. A cyber security for a smart grid. 2014 6th IEEE Power India International Conference (PIICON), pp. 1–6. https://doi.org/10.1109/poweri.2014.7117705.
Hollingworth, D., 2023. Chinese-linked hackers target Asian security grid in 6-month campaign. Cyber Daily. https://www.cyberdaily.au/critical-infrastructure/9560-chinese-linked-hackers-target-asian-security-grid-in-six-month-campaign.
Hollingworth, D., 2024. Exclusive: Medusa claims hack of aussie fuel distributor North Coast petroleum. Cyber Daily. https://www.cyberdaily.au/security/10743-exclusive-medusa-claims-hack-of-aussie-fuel-distributor-north-coast-petroleum.
Hope, A., 2022. Cyber attack targeted 21 natural gas producers on the eve of the Russian invasion of Ukraine. CPO Magazine. https://www.cpomagazine.com/cyber-security/cyber-attack-targeted-21-natural-gas-producers-on-the-eve-of-the-russian-invasion-of-ukraine/.
Ige, A.B., Kupa, E., Ilori, O., 2024a. Aligning sustainable development goals with cybersecurity strategies: ensuring a secure and sustainable future. GSC Adv. Res. Rev. 19 (3), 344–360. https://doi.org/10.30574/gscarr.2024.19.3.0236.
Ige, A.B., Kupa, E., Ilori, O., 2024b. Developing comprehensive cybersecurity frameworks for protecting green infrastructure: conceptual models and practical applications. GSC Adv. Res. Rev. 20 (1), 25–41. https://doi.org/10.30574/gscarr.2024.20.1.0237.
Imran, H., Salama, M., Turner, C., Fattah, S., 2022. Cybersecurity risk management frameworks in the oil and gas sector: a systematic literature review. In: Arai, K. (Ed.), Lecture Notes in Networks and Systems: Vol. 439. Advances in Information and Communication. Springer, pp. 871–894. https://doi.org/10.1007/978-3-030-98015-3_59.
Insikt Group, 2022. Continued targeting of Indian power grid assets by Chinese state-sponsored activity group. Recorded Future. https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf.
Islam, M.T., Shahir, S.A., Uddin, T.M.I., Saifullah, A.Z.A., 2014. Current energy scenario and future prospect of renewable energy in Bangladesh. Renew. Sustain. Energy Rev. 39, 1074–1088. https://doi.org/10.1016/j.rser.2014.07.149.
IT-Störung bei enercity, 2023. Enercity. https://www.enercity.de/presse/betrieb-und-baustellen/2022/it-stoerung.
Johnson, J., Berg, T., Anderson, B., Wright, B., 2022. Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. Energies 15 (11), 3931. https://doi.org/10.3390/en15113931.
Jones, D., 2023. Suncor energy continues probe of cyber incident disrupting gas station payments. Cybersecurity Dive. https://www.cybersecuritydive.com/news/suncor-energy-probe-cyber/654151/.
Jones, D., 2024. Halliburton incurs about $35M in expenses related to August cyberattack. Cybersecurity Dive. https://www.cybersecuritydive.com/news/halliburton-35-million-cyberattack/732397/.
Kapko, M., 2022. Energy Providers Hit by North Korea-linked Lazarus Exploiting Log4j VMware Vulnerabilities. Cybersecurity Dive. https://www.cybersecuritydive.com/news/energy-providers-log4j-vmware/631673/.
Kaspersky GReAT, & ICS CERT, 2023. Updated MATA attacks industrial companies in Eastern Europe. Kaspersky. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/10/18092216/Updated-MATA-attacks-Eastern-Europe_full-report_ENG.pdf.
Kaspersky ICS CERT, 2023. H2 2023 – a brief overview of main incidents in industrial cybersecurity. https://ics-cert.kaspersky.com/publications/reports/2024/04/11/h2-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/.
Kauranen, A., Lehto, E., 2024. Exclusive: Finnish Utility Fortum Reports Pick up in Cyberattacks and Surveillance. Reuters. https://www.reuters.com/business/energy/finnish-utility-fortums-power-assets-targeted-with-surveillance-cyber-attacks-2024-10-10/.
Kazancı, B.A., 2024. The strategic importance of cyber security in electric energy policies. Int. J. Energy Econ. Pol. 14 (4), 599–605. https://doi.org/10.32479/ijeep.16244.
Kemp, L., 2022. Personal Data of 1.3 Million Iberdrola Customers Stolen in Cyberattack. Euro Weekly News. https://euroweeklynews.com/2022/03/31/iberdrola-cyber attack/.
Kenney, M., 2015. Cyber-terrorism in a post-stuxnet world. Orbis 59 (1), 111–128. https://doi.org/10.1016/j.orbis.2014.11.009.
Khaitan, A., 2023a. BlackCat ransomware strikes Ho Chi Minh City power corporation. The Cyber Express. https://thecyberexpress.com/vietnam-electricity-data-breach/.
Khaitan, A., 2023b. CyberAv3ngers Offers 1TB of Alleged Israeli Electricity Data for 5 BTC. The Cyber Express. https://thecyberexpress.com/iec-data-breach-israels-power-attack/.
Khaitan, A., 2024. Israel's largest oil refinery, bazan group, hit by anonymous Sudan. The Cyber Express. https://thecyberexpress.com/cyberattack-on-bazan-group/.
Kharlamova, N., Hashemi, S., Træholt, C., 2020. The cyber security of battery energy storage systems and adoption of data-driven methods. In: 2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), pp. 188–192. https://doi.org/10.1109/AIKE48582.2020.00037.
Kim, S., Heo, G., Zio, E., Shin, J., Song, J.-g., 2020. Cyber attack taxonomy for digital environment in nuclear power plants. Nucl. Eng. Technol. 52 (5), 995–1001. https://doi.org/10.1016/j.net.2019.11.001.
Koelemij, S., 2023. Pro-russian group zarya claims hacking a Canadian pipeline. Industrial Cyber. https://industrialcyber.co/analysis/pro-russian-group-zarya-claims-hacking-a-canadian-pipeline/.
Kolekevski, I., 2024. Bochvarski: working to overcome MEPSO cyberattack. Media Information Agency (MIA). https://mia.mk/en/story/bochvarski-working-to-overcome-mepso-cyberattack.
Konaszczuk, W., 2021. Cybersecurity threats in the sectors of oil, natural gas and electric power in the context of technological evolution. Studia Iuridica Lublinensia 30 (4), 333–351. https://doi.org/10.17951/sil.2021.30.4.333-351.
Kondruss, B., 2023. MOVEit hack victim list: progress software MOVEit vulnerability cyber incident. KonBriefing Research. https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html.
Kondruss, B., 2025. Cyber Attack News Today 2025/2024. KonBriefing. https://konbriefing.com/en-topics/cyber-attacks.html.
Kovačević, A., Putnik, N., Tošković, O., 2020. Factors related to cyber security behavior. IEEE Access 8, 125140–125148. https://doi.org/10.1109/ACCESS.2020.3007867.
Kumar, V.S., Prasad, J., Ravi, R., 2018. A critical review of cyber security and cyber terrorism - threats to critical infrastructure in the energy sector. Int. J. Crit. Infrastruct. 14 (2). https://doi.org/10.1504/IJCIS.2018.10013025.
Kunz, C., 2024. Electricity Provider Tibber Hacked, 50,000 German Customers Affected. Heise Online. https://www.heise.de/en/news/Electricity-provider-Tibber-hacked-50-000-German-customers-affected-10031690.html.
Kuzemko, C., Lockwood, M., Mitchell, C., Hoggett, R., 2016. Governing for sustainable energy system change. Politics, contexts and contingency. Energy Research & Social Science 12, 96–105. https://doi.org/10.1016/j.erss.2015.12.022.
Lakshmanan, R., 2023. Researchers Expose Space Pirates' Cyber Campaign Across Russia and Serbia. The Hacker News. https://thehackernews.com/2023/08/researchers-expose-space-pirate-cyber.html.
Lakshmanan, R., 2024. Crypt Ghouls Targets Russian Firms with LockBit 3.0 and Babuk Ransomware Attacks. The Hacker News. https://thehackernews.com/2024/10/crypt-ghouls-targets-russian-firms-with.html.
Lapienytė, J., 2022. Ukrainian Hackers Attacked Gazprom, Says Expert. Cybernews. https://cybernews.com/cyber-war/ukrainian-hackers-attacked-gazprom-says-expert/.
Lee, T., Tseng, C., Lee, P., Lu, S., Chen, P., 2024. Earth baxia uses spear-phishing and GeoServer exploit to target APAC. Trends Microbiol. https://www.trendmicro.com/en_us/research/24/i/earth-baxia-spear-phishing-and-geoserver-exploit.html.
Lepido, D., Brambilla, A., 2022. Italian Oil Giant Eni Hit by Cyber Attack. Insurance Journal. https://www.insurancejournal.com/news/international/2022/09/01/683313.htm.
Lepido, D., Gallagher, R., Brambilla, A., 2022. Suspected Russian Ransomware Group Hacks Italian Energy Agency. Bloomberg. https://www.bloomberg.com/news/articles/2022-09-02/suspected-russian-ransomware-group-hacks-italian-energy-agency.
LulzSec Black Targets Critical, 2024. Infrastructure in Cyprus. Odyssey. https://odysseycs.com/resources/threat-alerts/lulzsec-black-targets-critical-infrastructure-in-cyprus/.
Lyons, J., 2024. ALPHV blackmails Canadian pipeline after 'stealing 190GB of vital info'. The Register. https://www.theregister.com/2024/02/13/alphv_canadian_pipeline/.
Malhotra, A., Ventura, V., 2023a. Talos uncovers espionage campaigns targeting CIS countries, embassies and EU health care agency. Talos. https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/.
Malhotra, A., Ventura, V., 2023b. Kazakhstan-associated YoroTrooper disguises origin of attacks as Azerbaijan. Talos. https://blog.talosintelligence.com/attributing-yorotrooper/.
Maliarchuk, T., Danyk, Y., Briggs, C., 2019. Hybrid warfare and cyber effects in energy infrastructure. Connections 18 (1/2), 93–110. https://www.jstor.org/stable/26948851.
Mandiant, 2023. Sandworm disrupts power in Ukraine using a novel attack against operational technology. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/.
Mandiant, 2024a. An offer you can refuse: UNC2970 backdoor deployment using trojanized PDF reader. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/unc2970-backdoor-trojanized-pdf-reader.
Mandiant, 2024b. Cutting edge, part 4: ivanti connect secure VPN post-exploitation lateral movement case studies. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement.
Mara, D., Nate, S., Stavytskyy, A., Kharlamova, G., 2022. The place of energy security in the national security framework: an assessment approach. Energies 15 (2), 658. https://doi.org/10.3390/en15020658.
Martin, A., 2023. Oil and gas giant shell confirms it was impacted by clop ransomware attacks. The Record. https://therecord.media/shell-impacted-in-clop-ransomware-attack.
Matishak, M., 2025. Costa Rica refinery cyberattack was first deployment for new US response program, ambassador says. The Record. https://therecord.media/state-department-falcon-cyber-response-costa-rica-recope.
Medusa Claims PetroChina Ransomware Attack, 2023. The cyber express. https://thecyberexpress.com/medusa-claims-petrochina-ransomware-attack/.
Meehan, A., 2022. Lithuanian energy firm disrupted by DDOS attack. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/lithuanian-energy-ddos-attack/.
Mekdad, Y., Bernieri, G., Conti, M., El, Fergougui A., 2022. The rise of ICS malware: a comparative analysis. In: Katsikas, et al. (Eds.), Lecture Notes in Computer Science, Computer Security. ESORICS 2021 International Workshops, 13106. Springer, pp. 496–511. https://doi.org/10.1007/978-3-030-95484-0_29.
Microsoft Threat Intelligence, 2023. Volt typhoon targets US critical infrastructure with living-off-the-land techniques. Microsoft Security. https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.
Ministry of Science and Technology, 2024. Enhancing network security critical to defend against attacks. https://english.mic.gov.vn/enhancing-network-security-critical-to-defend-against-attacks-19724042309573251.htm.

Mohammed, A.S., Reinecke, P., Burnap, P., Rana, O., Anthi, E., 2022. Cybersecurity challenges in the offshore oil and gas industry: an industrial cyber-physical systems (ICPS) perspective. ACM Transactions on Cyber-Physical Systems (TCPS) 6 (3), 1–27. https://doi.org/10.1145/3548691.

Mohan, A.M., Meskin, N., Mehrjerdi, H., 2020. A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems. Energies 13 (15), 3860. https://doi.org/10.3390/en13153860.

National Computer Virus Emergency Response Center and National Engineering Laboratory for Computer Virus Prevention Technology, 2024a. Volt Typhoon: a Conspiratorial Swindling Campaign Targets with U.S. Congress and Taxpayers Conducted by U.S. Intelligence Community. https://www.cverc.org.cn/head/zhaiyao/futetaifengEN.pdf.

National Computer Virus Emergency Response Center and National Engineering Laboratory for Computer Virus Prevention Technology, 2024b. Volt Typhoon II: a Secret Disinformation Campaign Targeting U.S. Congress and Taxpayers Conducted by U.S. Government agencies. https://www.cverc.org.cn/head/zhaiyao/futetaifengerEN.pdf.

National Computer Virus Emergency Response Center and National Engineering Laboratory for Computer Virus Prevention Technology, 2024c. Volt Typhoon III–Unraveling Cyberespionage and Disinformation Operations Conducted by U.S. Government Agencies. https://www.cverc.org.cn/head/zhaiyao/futetaifeng3_EN.pdf.

Nejabatkhah, F., Li, Y.W., Liang, H., Reza Ahrabi, R., 2021. Cyber-security of smart microgrids: a survey. Energies 14 (1), 27. https://doi.org/10.3390/en14010027.

North Korean hackers target US, 2022. Canada and Japan energy sectors via Log4j exploit. Cyber Daily. https://www.cyberdaily.au/government/8255-north-korean-hacking-group-targeting-us-energy-sector-via-log4j-exploit.

Nye, J.S., 2011. Nuclear lessons for cyber security? Strategic Studies Quarterly 5 (4), 18–38. http://www.jstor.org/stable/26270536.

Ogunleye, O., Adeniji, S., Onih, V., Simo, Y., Elom, E., Kanu, E., Bello, A.-W., Obunadike, C., Chukwu, N., Ejiofor, O., Ogutu, J., Obudinake, C., Clement, T., Kizor-Akaraiwe, S., 2024. Improving resilience and efficiency in the energy sector: a perspective on cybersecurity and renewable energy storage. International Journal of Scientific Research and Management (IJSRM) 12 (5).

Onyeji, I., Bazilian, M., Bronk, C., 2014. Cyber security and critical energy infrastructure. Electr. J. 27 (2), 52–60. https://doi.org/10.1016/j.tej.2014.01.011.

Openbar Ministerie, 2022. Police, OM submit GEBE hack report to government. https://www.openbaarministerie.org/en/police-om-submit-gebe-hack-report-to-government.

Paganini, P., 2022a. Wind turbine giant deutsche windtechnik hit by a professional cyberattack. Security Affairs. https://securityaffairs.com/130648/hacking/deutsche-windtechnik-professional-cyberattack.html.

Paganini, P., 2022b. Everest gang demands $200K for data stolen from South Africa state-owned electricity company ESKOM. Security Affairs. https://securityaffairs.com/136866/cyber-crime/south-africa-eskom-everest-ransomware.html.

Paganini, P., 2023a. Pro-Israel predatory sparrow hacker group disrupted services at around 70% of Iran's fuel stations. Security Affairs. https://securityaffairs.com/156065/hacktivism/pro-israel-predatory-sparrow-iran-fuel-stations.html.

Paganini, P., 2023b. Rhysida ransomware gang claimed China energy hack. Security Affairs. https://securityaffairs.com/154785/cyber-crime/rhysida-ransomware-china-energy.html.

Paganini, P., 2023c. Danish critical infrastructure hit by the largest cyber attack in Denmark's history. Security Affairs. https://securityaffairs.com/154156/apt/denmark-critical-infrastructure-record-attacks.html.

Paganini, P., 2023d. IT army of Ukraine gained access to a 1.5GB archive from gazprom. Security Affairs. https://securityaffairs.com/141640/hacktivism/it-army-of-ukraine-hacked-gazprom.html.

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A., Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P., Moher, D., 2021a. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. Br. Med. J. n71. https://doi.org/10.1136/bmj.n71.

Page, M.J., Moher, D., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A., Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P., McKenzie, J.E., 2021b. PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews. Br. Med. J. n160. https://doi.org/10.1136/bmj.n160.

Pearson, I.L.G., 2011. Smart grid cyber security for Europe. Energy Policy 39 (9), 5211–5218. https://doi.org/10.1016/j.enpol.2011.05.043.

Pelosi's Taiwan Visit Widens Taipei-Beijing Rift, 2022. Cyble. https://cyble.com/blog/pelosis-taiwan-visit-widens-taipei-beijing-rift/.

Pengili, M., Raszewski, S., 2024. Transnational cyber governance for risk management in the gas sector: exploring the potential of G7 cooperation. Gas 4 (4), 327–350. https://doi.org/10.3390/gases4040019.

Peregrine Group Data Breach Investigation, 2024. Strauss borelli PLLC. https://strauss borrelli.com/2024/07/16/peregrine-group-data-breach-investigation/.

Plėta, T., Tvaronavičienė, M., Casa, S.D., Agafonov, K., 2020. Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. Insights into Regional Development 2 (3), 703–715. https://doi.org/10.9770/ird.2020.2.3(7).

Power utility HSE recovering from cyberattack, 2023. The Slovenia times. https://sloveniatimes.com/40021/power-utility-hse-recovering-from-cyberattack.

Premier promises to look into BVIEC's handling of cyber-attack PR- BVIEC remains silent. Virgin Islands News Online, 2024. https://www.virginislandsnewsonline.com/en/news/premier-promises-to-look-into-bviecs-handling-of-cyber-attack-pr.

PRESS RELEASE, 2024. Regarding the Restoration of Pvoil's Information Technology System, p. PVOIL. https://pvoil.com.vn/en/press-release-regarding-the-restoration-of-pvoils-information-technology-system.

Priyadarshini, I., Kumar, R., Sharma, R., Singh, P.K., Satapathy, S.C., 2021. Identifying cyber insecurities in trustworthy space and energy sector for smart grids. Comput. Electr. Eng. 93, 107204. https://doi.org/10.1016/j.compeleceng.2021.107204.

Progoulakis, I., Nikitakos, N., Rohmeyer, P., Bunin, B., Dalaklis, D., Karamperidis, S., 2021. Perspectives on cyber security for offshore oil and gas assets. J. Mar. Sci. Eng. 9 (2), 112. https://doi.org/10.3390/jmse9020112.

PT Expert Security Center, 2022. Space pirates: исследуеМ инструМенты и связи новой хакерской группировки. Positive Technologies. https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/space-pirates-tools-and-connections/.

Putnik, N., 2022. Sajber Rat i Sajber Mir. Inovacioni centar Fakulteta bezbednosti/Academic Mind.

PwC, 2024. Under the lens: the energy sector. https://www.pwc.de/de/energiewirtschaft/under-the-lens-the-energy-sector.pdf.

Rachwani, M., 2022. EnergyAustralia latest to be hit by cyber-attack as details of hundreds of customers exposed. Guardian. https://www.theguardian.com/australia-news/2022/oct/21/energyaustralia-latest-to-be-hit-by-cyber-attack-as-details-of-hundreds-of-customers-exposed.

Raggi, M., Scenarelli, S., 2022. Rising Tide: Chasing the Currents of Espionage in the South China Sea. Proofprint. https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea.

RansomHouse Ransomware Victim, 2024. Veren inc and crescent point energy. RedPacket Security. https://www.redpacketsecurity.com/ransomhouse-ransomware-victim-veren-inc-and-crescent-point-energy/.

Ransomware BianLian Group Hits: Pioneer Oil Company, Inc[.]. (2024, April 17). *HookPhish*. https://www.hookphish.com/blog/ransomware-bianlian-group-hits-pioneer-oil-company-inc/.

Reddick, J., 2024. Oil Titan halliburton confirms data was stolen in cyberattack. The Record. https://therecord.media/halliburton-confirms-data-stolen-in-incident.

Rehan, M., 2022. STELCO Hit with Ransomware Attack; Interrupts Services, The Edition https://edition.mv/sports/24298.

Rekeraho, A., Cotfas, D.T., Cotfas, P.A., Tuyishime, E., Balan, T.C., Acheampong, R., 2024. Enhancing security for IoT-Based smart renewable energy remote monitoring systems. Electronics 13 (4), 756. https://doi.org/10.3390/electronics13040756.

Repsol suffers a cyberattack against its databases. Intech, 2024. https://inteccybersecurity.com/en/2024/09/repsol-sufre-un-ciberataque-contra-sus-bases-de-datos.html.

Ribas Monteiro, L.F., Rodrigues, Y.R., de Souza, Z.A.C., 2023. Cybersecurity in cyber–physical power systems. Energies 16 (12), 4556. https://doi.org/10.3390/en16124556.

Ribeiro, A., 2022. Honeywell, schneider electric targeted in cyber-espionage campaign aimed at renewable energy companies. Industrial Cyber. https://industrialcyber.co/threats-attacks/honeywell-schneider-electric-targeted-in-cyber-espionage-campaign-aimed-at-renewable-energy-companies/.

Ribeiro, A., 2024a. Cyprus critical infrastructure targeted in series of cyberattacks, as authorities stress on readiness. Industrial Cyber. https://industrialcyber.co/critical-infrastructure/cyprus-critical-infrastructure-targeted-in-series-of-cyberattacks-as-authorities-stress-on-readiness/.

Ribeiro, A., 2024b. Google details UNC2970 North Korea-linked espionage hackers targeting US energy, aerospace sectors. Industrial Cyber. https://industrialcyber.co/ransomware/google-details-unc2970-north-korea-linked-espionage-hackers-targeting-us-energy-aerospace-sectors/.

Risser oil - Data breach on August 30, 2024. Breachsense, 2024. https://www.breachsense.com/breaches/risser-oil-data-breach/.

Robertson, J., Charpa, S., 2022. Hackers Targeted U.S. LNG Producers in Run-Up to Ukraine War. Bloomberg. https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine?page=0.

Robinson, R., 2023. Phishing Campaign Targets Chinese Nuclear Energy Industry. Intezer. https://intezer.com/blog/research/phishing-campaign-targets-nuclear-energy-industry/.

Ropek, L., 2023. Pentagon leaks show Russian hacktivists claim to have targeted a Canadian pipeline. Gizmodo. https://gizmodo.com/russian-hackers-zarya-canadian-pipeline-pentagon-leak-1850318999.

Ryu, D., Lee, S., Yang, S., Jeong, J., Lee, Y., Shin, D., 2024. Enhancing cybersecurity in energy IT infrastructure through a layered defense approach to major malware threats. Appl. Sci. 14 (22), 10342. https://doi.org/10.3390/app142210342.

Sáiz-Pardo, M., 2022. A cyber-attack on Spain's electricity giant iberdrola has accessed data of 1.3 million clients. English. https://www.surinenglish.com/spain/cyberattack-iberdrola-accessed-20220401183800-nt.html.

Schiaffino, M., 2024. Iran, cosa sappiamo dell'attacco informatico israeliano. Wired. https://www.wired.it/article/iran-attacco-hacker-israele-cosa-sappiamo/.

SectorCERT, 2023. The attack against Danish, critical infrastructure. https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-Angrebet-mod-dansk-kritisk-infrastruktur-TLP-CLEAR.pdf.

Shakarian, P., Shakarian, J., Ruef, A., 2013. Introduction to Cyber-Warfare: a Multidisciplinary Approach. Elsevier Inc. https://doi.org/10.1016/C2012-0-06618-5.

Sharma, A., 2022a. Hive claims ransomware attack on Tata power, begins leaking data. Bleeping Computer. https://www.bleepingcomputer.com/news/security/hive-claims-ransomware-attack-on-tata-power-begins-leaking-data/.

Sharma, A., 2022b. Rompetrol gas station network hit by hive ransomware. Bleeping Computer. https://www.bleepingcomputer.com/news/security/rompetrol-gas-station-network-hit-by-hive-ransomware/.
Sharma, A., 2023. Israel's largest oil refinery website offline after DDoS attack. Bleeping Computer. https://www.bleepingcomputer.com/news/security/israels-largest-oil-refinery-website-offline-after-ddos-attack/.
Singapore Police Force, 2024. Joint advisory on akira ransomware. Singapore Police Force. https://www.police.gov.sg/media-room/news/20240607_joint_advisory_on_akira_ransomware.
Siva Kumar, D.V.N., Santhi Thilagam, P., 2019. Approaches and challenges of privacy preserving search over encrypted data. Inf. Syst. 81, 63–81. https://doi.org/10.1016/j.is.2018.11.004.
Smith, D.C., 2018. Enhancing cybersecurity in the energy sector: a critical priority. J. Energy Nat. Resour. Law 36 (4), 373–380. https://doi.org/10.1080/02646811.2018.1516362.
SocRadar, 2022. Hacktivist Group Black Reward Leaked Iran's Nuclear Program Secrets. SOCRadar® Cyber Intelligence Inc. https://socradar.io/hacktivist-group-black-reward-leaked-iran-nuclear-program-secrets/.
SocRadar, 2023. Attackers Exploit Critical Zero-Day Vulnerability in Moveit Transfer. SOCRadar® Cyber Intelligence Inc. https://socradar.io/attackers-exploit-critical-zero-day-vulnerability-in-moveit-transfer/.
Son, D., 2024. Cyber-Espionage Campaign Unveiled: Operation Cobalt Whisper Hits Sensitive Industries. Cybersecurity News. https://securityonline.info/cyber-espionage-campaign-unveiled-operation-cobalt-whisper-hits-sensitive-industries/.
Son, J., Choi, J., Yoon, H., 2019. New complementary points of cyber security schemes for critical digital assets at nuclear power plants. IEEE Access 7, 78379–78390. https://doi.org/10.1109/ACCESS.2019.2922335.
Sophos, 2024. The state of ransomware 2024. https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf.
Spasić, V., 2022. EPCG Prešla Na Manuelno Upravljanje Elektranama Zbog Opasnosti Od Hakerskog Napada. Balkan Green Energy News. https://balkangreenenergynews.com/rs/epcg-presla-na-manuelno-upravljanje-elektranama-zbog-opasnosti-od-hakerskog-napada/.
Spasić, V., 2023. Serbia's Power Utility EPS Under Unprecedented Hacker Attack. Balkan Green Energy News. https://balkangreenenergynews.com/serbias-power-utility-eps-under-unprecedented-hacker-attack/.
Stanojević, P., Šekarić Stojanović, N., 2023. Novelties in the paradigm of understanding energy security. War in Ukraine: what we Know and what we Don'T Know, pp. 211–231. https://doi.org/10.18485/iipe_rat_ukrajina.2023.ch13.
Stergiopoulos, G., Gritzalis, D.A., Limnaios, E., 2020. Cyber-attacks on the oil & gas sector: a survey on incident assessment and attack patterns. IEEE Access 8, 128440–128475. https://doi.org/10.1109/ACCESS.2020.3007960.
Stoddart, K., 2022. Cyberwar: attacking critical infrastructure. In: Cyberwarfare: Threats to Critical Infrastructure. Palgrave Macmillan, pp. 147–225. https://doi.org/10.1007/978-3-030-97299-8_3.
Strojny, J., Krakowiak-Bal, A., Knaga, J., Kacorzyk, P., 2023. Energy security: a conceptual overview. Energies 16 (13), 5042. https://doi.org/10.3390/en16135042.
Subramanian, S., 2023. Phishing in the South China Sea. The Diplomat. https://thediplomat.com/2023/04/phishing-in-the-south-china-sea/.
Sun, C.-C., Hahn, A., Liu, C.-C., 2018. Cyber security of a power grid: state-of-the-art. Int. J. Electr. Power Energy Syst. 99, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020.
Symantec, 2023. Redfly: espionage actors continue to target critical infrastructure. Symantec Enterprise Blogs/Threat Intelligence. https://www.security.com/threat-intelligence/critical-infrastructure-attacks.
Symantec, 2024. RansomHub: new ransomware has origins in older knight. Symantec Enterprise Blogs/Threat Intelligence. https://www.security.com/threat-intelligence/ransomhub-knight-ransomware.
Tatipatri, N., Arun, S.L., 2024. A comprehensive review on cyber-attacks in power systems: impact analysis, detection, and cyber security. IEEE Access 12, 18147–18167. https://doi.org/10.1109/ACCESS.2024.3361039.
Thales, 2023. Killnet claims attack on the public power corporation of Greece and the television network "Mega TV". Cyber Solutions by Thales. https://cds.thalesgroup.com/en/node/518.
Third Largest Energy Distributor in Colombia hit by Cyberattack, 2024. ICS strive. https://icsstrive.com/incident/third-largest-energy-distributor-in-colombia-hit-by-cyberattack/.
Threat Advisory, 2024. Crypt ghouls deployed babuk LockBit and to paralyze Russian firms. Hive Pro. https://hivepro.com/wp-content/uploads/2024/10/TA2024404.pdf?utm_sr=(direct)&utm_cmd=(none)&utm_ccn=(not%20set).
Threat Intelligence. Energy sector targeted by lazarus. Quorum Cyber. https://www.quorumcyber.com/threat-intelligence/energy-sector-targeted-by-lazarus/.
Tidy, J., 2022. Predatory Sparrow: Who are the Hackers who Say they Started a Fire in Iran? BBC. https://www.bbc.com/news/technology-62072480.
Toulas, B., 2022a. Chinese 'Space Pirates' are hacking Russian aerospace firms. Bleeping Computer. https://www.bleepingcomputer.com/news/security/chinese-space-pirates-are-hacking-russian-aerospace-firms/?&web_view=true.
Toulas, B., 2022b. Cyber espionage campaign targets renewable energy companies. Bleeping Computer. https://www.bleepingcomputer.com/news/security/cyber-espionage-campaign-targets-renewable-energy-companies/.
Trivić, B., Šošić, D., 2020. Sajber bezbednost u energetskom sektoru. Journal of Scientific and Research Publications 10 (10). https://doi.org/10.29322/IJSRP.X.X.2018.pXXXX.
U.S. Department of Justice, 2024. U.S. government disrupts botnet people's Republic of China used to conceal hacking of critical infrastructure. https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical.
Uchill, J., 2022. In a First, Ukraine Leaks Russian Intellectual Property as Act of War. *SC Media*. https://www.scworld.com/analysis/in-a-first-ukraine-leaks-russian-intellectual-property-as-act-of-war.
Vedere Labs, 2022. Killnet: Analysis of Attacks from a Prominent Pro-russian Hacktivist Group. Forescout. https://www.forescout.com/resources/analysis-of-killnet-report/.
Venkatachary, S.K., Prasad, J., Samikannu, R., 2017. Economic impacts of cyber security in energy sector: a review. Int. J. Energy Econ. Pol. 7 (5), 250–262. https://www.econjournals.com/index.php/ijeep/article/view/5283.
Venkatachary, S.K., Prasad, J., Samikannu, R., 2018. Cybersecurity and cyber terrorism - in energy sector – a review. Journal of Cyber Security Technology 2 (3–4), 111–130. https://doi.org/10.1080/23742917.2018.1518057.
Venkatachary, S.K., Prasad, J., Alagappan, A., Andrews, L.J.B., Raj, R.A., Duraisamy, S., 2024. Cybersecurity and cyber-terrorism challenges to energy-related infrastructures – cybersecurity frameworks and economics – comprehensive review. International Journal of Critical Infrastructure Protection 45, 100677. https://doi.org/10.1016/j.ijcip.2024.100677.
Vernotte, A., Välja, M., Korman, M., Björkman, G., Ekstedt, M., Lagerström, R., 2018. Load balancing of renewable energy: a cyber security analysis. Energy Informatics 1 (5). https://doi.org/10.1186/s42162-018-0010-x.
Viasat, 2022. KA-SAT network cyber attack overview. Viasat. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/.
Winzer, C., 2012. Conceptualizing energy security. Energy Policy 46, 36–48. https://doi.org/10.1016/j.enpol.2012.02.067.
World Economic Forum, 2025. Global cybersecurity outlook 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.
Yaacoub, J.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M., 2020. Cyber-physical systems security: limitations, issues and future trends. Microprocess. Microsyst. 77, 103201. https://doi.org/10.1016/j.micpro.2020.103201.
Yergin, D., 2011. The Quest: Energy, Security, and the Remaking of the Modern World. Penguin Press.
Zhao, A.P., Li, S., Gu, C., Yan, X., Hu, P.J.-H., Wang, Z., Xie, D., Cao, Z., Chen, X., Wu, C., Luo, T., Wang, Z., Hernando-Gil, I., 2024. Cyber vulnerabilities of energy systems. IEEE Journal of Emerging and Selected Topics in Industrial Electronics 5 (4), 1455–1469. https://doi.org/10.1109/jestie.2024.3434350.
Zografopoulos, I., Hatziargyriou, N.D., Konstantinou, C., 2023. Distributed energy resources cybersecurity outlook: vulnerabilities, attacks, impacts, and mitigations. IEEE Syst. J. 17 (4), 6695–6709. https://doi.org/10.1109/jsyst.2023.3305757.
Zoltan, M., 2023. Akira ransomware group attacks Australia and Brazil. Privacy Affairs. https://www.privacyaffairs.com/akira-ransomware-australia-brazil/.
Zoltan, M., Popa, M., 2024. BlackSuit breaches Nigerian company. Privacy Affairs. https://www.privacyaffairs.com/blacksuit-breaches-nigerian-company/.