ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Cyber Threats and Vulnerability Mapping in the Energy Sector: Laying the Groundwork for Smart Grid Resilience

Inda Kreso | Faculty of Criminal Justice, Criminology and Security Studies, University of Sarajevo | ORCID: 0000-0002-5556-4669

Abstract

Energy security is currently one of the most important topics worldwide. Maintaining a reliable energy supply is one of the biggest challenges in security science. Additionally, defending energy infrastructure from cyberattacks is an ongoing issue. Understanding the vulnerabilities of energy infrastructure, especially the Smart Grid, which relies on information technology and communications, is a significant advantage. Understanding which system vulnerabilities lead to specific cyber threats presents a significant opportunity, enhancing the defence of energy infrastructure. This paper uses a systematic literature review to identify the most common cyber threat and Smart Grid vulnerability mentioned and researched in the literature from 2018 to 2025. This paper also aims to map the vulnerabilities that allow for cyber threats to occur, with the idea that if we know what causes a weak spot, we can effectively prevent it. Identifying specific weaknesses that could lead to cyber threats allows us to mitigate these dangers by addressing and correcting those vulnerabilities.

Keywords

smart grid, cybersecurity, energy sector, cyber threats

Received: 07.06.2025

Accepted: 14.09.2025

Published: 16.10.2025

Cite this article as:
I. Kreso, "Cyber threats and vulnerability mapping in the energy sector: Laying the groundwork for smart grid resilience," ACIG, vol. 4, no. 1, 2025, doi: 10.60097/ACIG/211124.

Corresponding author:
Inda Kreso, Criminal Justice, University of Sarajevo, Bosnia and Herzegovina; E-mail: indakreso@fkn.unsa.ba
0000-0002-5556-4669

1. Introduction

Energy security is one of the most important pillars of modern society and the main pillar of stability of every country. Energy infrastructure is a part of critical infrastructure and represents, as its name suggests, a critical point of national security, since it is always a potential target for cyber warfare, cyber terrorism, or financially motivated cyberattacks [1–4]. As the energy industry is enhancing, developing, and digitalising, cyber threats are becoming bigger issues for energy infrastructure [5, 6]. Energy infrastructure is susceptible to cyberattacks, which pose a serious threat to the energy sector as a whole. These cyberattacks can lead to operational disruptions, financial losses, and may even jeopardise national security. The integration and digitalisation of Smart Grid technology has made energy infrastructure more susceptible to cyberattacks. Since the Smart Grid relies heavily on information and communication technologies, it has become an attractive target for cyber threats [7–10]. As a result, the security of energy supply is further jeopardised by the vulnerabilities associated with the Smart Grid technology. There are different types of cyber threats that target specific vulnerabilities in the energy system. Many threats can exploit a specific vulnerability, and a specific vulnerability can be a target for a particular cyber threat within the energy.

In the recent decade, the energy sector and energy infrastructure globally have suffered numerous high-profile cyberattacks. The best-known attack happened in 2010 at the Natanz nuclear facility in Iran, and it is considered the very first known malware (named Stuxnet) specifically constructed to damage physically critical infrastructure by exploiting Siemens Supervisory Control and Data Acquisition (SCADA) systems to sabotage centrifuges [11–13]. Stuxnet manipulated centrifuge frequencies, causing them to speed up and slow down until they failed. During this process, the system displayed normal data to avoid detection. As a result, approximately 1000–5000 centrifuges were damaged. Stuxnet was the first cyberattack to reveal vulnerabilities in SCADA systems [11–13]. Two years later, in 2012, the Shamoon malware attacked Saudi Aramco, causing the deletion of thousands of workstations and the loss of valuable data [14–17]. Saudi Aramco is one of the biggest oil companies in the world. Shamoon malware was not created to target control systems like SCADA. Instead, it was designed to delete hard disk data, rendering computers unable to start [14–17]. In 2015, the BlackEnergy malware caused power outages across Ukraine, and in 2016, the Industroyer/CrashOverride malware targeted grid control protocols in Ukraine [18–22]. BlackEnergy malware targeted three Ukrainian energy companies and it was injected by spear-phishing

emails. After infiltration in the system, the malware deleted all the data from the computer systems, and SCADA systems were turned off, which caused a break in energy distribution across the country [23–26]. About 225,000 people were left without electricity for several hours in the winter period. This was the first cyberattack that caused a physical interruption of electric power. In the Industroyer/CrashOverride attack in 2016, the target again was an energy company in Ukraine. The malware was specifically designed to manipulate industrial protocols (IEC 60870-5-101, IEC 60870-5-104, and IEC 61850), which are used in power grids, and its goal was manipulating grid control protocols. Industroyer is considered the most sophisticated cyberattacks on the energy infrastructure after Stuxnet [23–26]. Another well-known example of a cyberattack targeting energy sector happened in 2017 in Saudi Arabia. This malware, known as Triton/Trisis, was designed to attack the Safety Instrumented Systems (SIS) at a Saudi petrochemical plant [27, 28]. The goal was to destroy physically the infrastructure of the plant. Malware was designed for the sabotage of the SIS and it is the only known cyberattack so far that directly targeted the safety systems of industrial control networks (protection systems). In this case, the attack did not fully succeed, because the malware caused an unintended shutdown of the system, which led engineers to discover the problem [27–29]. If the attack had succeeded, it could have led to a massive explosion or an industrial incident with human casualties. The very fact that the safety systems were the target was a precedent in the cyber security of critical infrastructure [27, 28]. In 2021, the Colonial Pipeline ransomware attack in the United States caused fuel supply disruptions along the East Coast [30–32]. The DarkSide ransomware was designed as a form of financial blackmail and was financially motivated [18, 33]. The attackers exploited compromised virtual private network (VPN) credentials that did not have multi-factor authentication (MFA), and the attack caused 6 days of shutdown of the main pipeline. After infiltration, they deployed ransomware that locked the IT systems (billing and business networks) [18, 31–33]. All of these incidents and cyberattacks exploited specific vulnerabilities in the systems in order to penetrate and infect them.

This research systematically explores cyber threats in the energy sector with a specific focus on Smart Grids. This paper examines both cyber threats and possible vulnerabilities within the Smart Grids and energy sector in general. The existing literature primarily focuses on either cyber threats in the energy sector and smart grid or vulnerabilities within these areas. The focus in the literature is usually on the type of the threats and rarely on the vulnerability

with clear fragmentation between concepts of threats and vulnerability. Nevertheless, being able to understand the potential correlations between vulnerabilities within the Smart Grid and cyber threats is crucial for constructing an effective defence system. It is logical to expect that vulnerabilities in any system reduce its security. Likewise, certain vulnerabilities within the Smart Grid can be exploited by cyber threats. For instance, whenever a specific type of cyber threat is discussed in the literature, it is usually accompanied by a vulnerability that creates an opportunity for that threat to occur. Correlations between vulnerabilities and cyber threats mean vulnerabilities that lead to cyber threats and can be identified and prevented more effectively. This research conducts a systematic literature review in order to explore the relationships between the vulnerabilities inherent in Smart Grid systems and the potential cyberattacks on their infrastructure. To address this gap, a systematic literature review was conducted following the preferred reporting items for systematic reviews and meta-analyses (PRISMA) guidelines. The objectives were to identify the most frequently reported threats and the most critical vulnerabilities, and to map their interdependencies. Mapping threats to vulnerabilities in this paper offers a unified perspective and insights that directly contribute to improving the security and defence of Smart Grid architecture as it is the first attempt in the literature to systematically map cyber threats to corresponding vulnerabilities in the energy sector.

2. Methodology

There has been a substantial amount of research on cyber threats and vulnerabilities within the Smart Grid and the broader energy sector, as this topic is critical to security studies. Most of the studies are focused exclusively on either cyber threats or system vulnerabilities, exploring them separately and without examining potential correlations. Consequently, there is a significant and evident gap in the research concerning studies that explore the potential correlations or dependencies between cyber threats and vulnerabilities in the Smart Grid.

Two research questions were defined for this paper:

Q 1. What are the most commonly mentioned types of cyber threats targeting the Smart Grid in the existing literature?

Q 2. What are the most critical vulnerabilities exploited in cyberattacks against energy infrastructure in the Smart Grid?

A thorough literature review was conducted to address two research questions, following a clearly established review protocol. For illustrating the gap in the literature regarding studies that focus on both threats and vulnerabilities, a bibliometric analysis was conducted. As a part of bibliometric analysis, the co-occurrence network of keywords in the reviewed literature was created using R, a programming language widely used for statistical computing and data analysis, using the Biblioshiny interface and the Bibliometrix package. The co-occurrence network of keywords in the reviewed literature is presented and explained in the Results section.

A systematic search was performed searching the literature in six online databases: Scopus, IEEE Xplore, SpringerLink, ScienceDirect, Google Scholar, and ResearchGate. The inclusion criteria were: peer-reviewed journal and conference papers, publications in the time range of 6 years (2018–2025), studies that focus on cyber threats in energy and Smart Grids, studies that focus on vulnerabilities within the Smart Grid or energy sector, studies that address both cyber threats and vulnerabilities of the Smart Grid. This study focused on the last 6 years of publication in order to examine the most recent literature in the field of cybersecurity in the energy sector. Since the field of cybersecurity is developing very fast, it is important to include the most recent studies in order to get correct analysis. Exclusion criteria were: studies not related to the energy sector, opinion pieces, editorials, or blogs, and duplicate records. The process of systematic literature review consisted of three steps: identification phase, screening phase, and inclusion phase. The systematic literature review in this paper was conducted following the PRISMA guidelines [34]. Figure 1 presents the visual representation of the PRISMA flow diagram that was used for the identification phase, screening phase, and inclusion phase of the literature review.

Initially, a total of 87 studies were collected using the following keywords: smart grid, cyber threats, vulnerabilities of smart grid, and energy sector. From the initial 87 collected studies, 12 studies were excluded in the identification phase because they were duplicates, leaving 75 records for the next phase. As it is presented in the Figure 1, in the following screening phase, 24 records were excluded because they did not fully align with the inclusion criteria. The following step was a full-text review of the selected papers, and in this step 12 records were excluded because they did not fully align with the inclusion criteria. In the final step, 39 studies were included and the literature review was conducted on 39 studies that are presented in Table S1 in the Appendix. The findings were

analysed through qualitative synthesis to identify key trends, gaps, and recurring themes in the literature. The selection of these papers was based on their direct relevance to the objective of this research and on inclusion rules. While this study is based on a systematic review of 39 publications that met the defined inclusion criteria, additional literature was consulted to provide broader context and to frame the research problem. Together, these papers provided a comprehensive, multidisciplinary perspective on the cybersecurity challenges, threats, and vulnerabilities confronting the energy sector.

A data extraction table (Table S1 in the Appendix) for 39 selected studies was created to capture the following elements for each study:

- Title
- Authors and year
- Focus area
- Identified cyber threats (RQ1)
- Noted vulnerabilities (RQ2)

3. Results

In the Results section, the results of the literature review and bibliometric analysis are presented. When it comes to the analysed literature, most of the existing papers treat cyber threats and system vulnerabilities as separate domains. They either categorise types of attacks or list common weaknesses of the Smart Grid infrastructure, but rarely investigate how specific vulnerabilities are exploited by particular cyber threats. This lack of integrative analysis limits the practical applicability of the existing findings for operators who need to prioritise security investments. Figure 2 illustrates the co-occurrence network of keywords in the reviewed literature. The co-occurrence network of keywords is a bibliometric visualisation that shows how the keywords from the analysed literature co-occur together (in the same papers). The stronger the connection between clusters, the more frequently the terms that co-occur in the reviewed literature, indicating a closer conceptual or thematic relationship. This co-occurrence network visualisation was generated in R, a programming language widely used for statistical computing and data analysis, using the Biblioshiny interface and the Bibliometrix package.

The co-occurrence network visualisation (Figure 2) highlights the fragmented nature of the existing research on Smart Grid

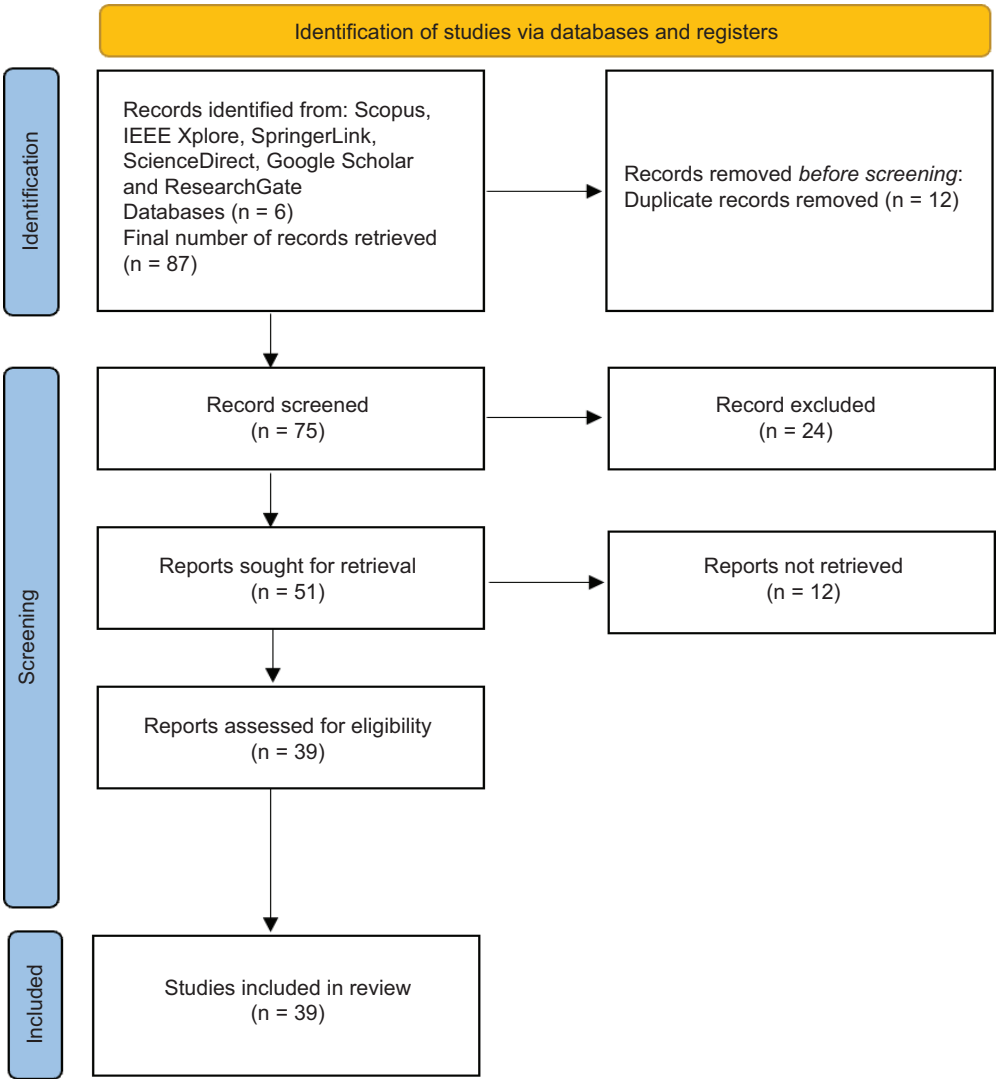

Figure 1. PRISMA flow diagram.

cybersecurity and clearly illustrates the gap that this study addresses. As it is presented in Figure 2, the most dominant cluster in the analysed literature is the purple cluster that connects 'Smart Grid', 'cybersecurity', 'SCADA', and 'industrial control system'. The purple cluster represents that the majority of the literature is focused on the general security challenges of critical infrastructure without linking those threats to specific vulnerabilities. The second cluster is the blue cluster that connects 'blockchain', 'artificial intelligence' (AI), 'cyberattacks', and 'intrusion detection systems'. The blue cluster represents a technology-based cluster that emphasises

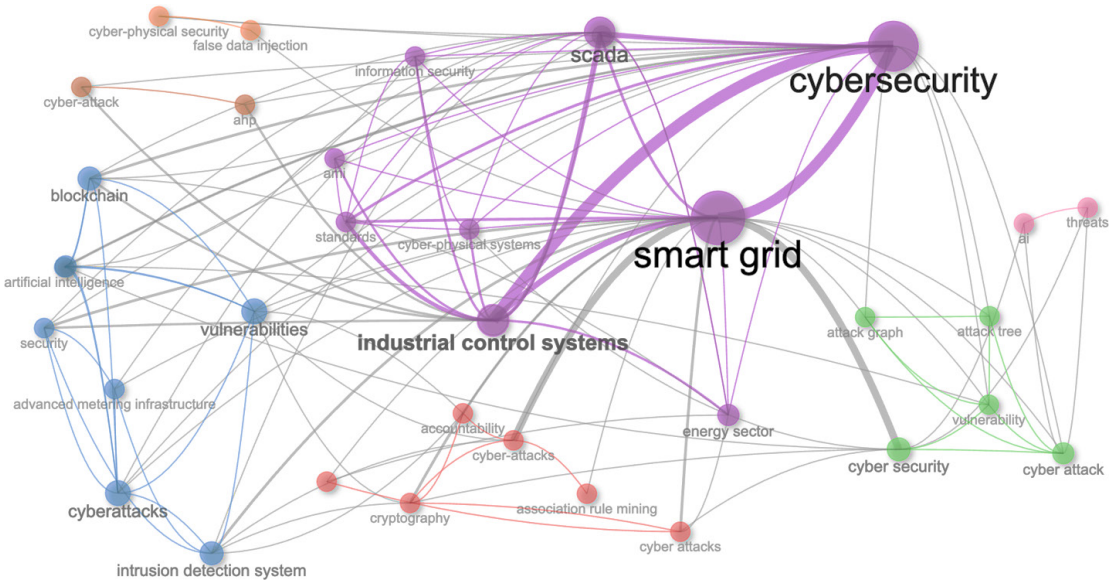

Figure 2. Co-occurrence network of keywords in the reviewed literature.

the importance of the vulnerabilities and new modern technologies such as blockchain and AI, but without strong integration into the broader Smart Grid security component. The third cluster is the green cluster centred around 'attack graph', 'attack tree', and 'vulnerability'. The green cluster is based more on a methodological focus and disconnected from real-world incidents and empirical validation. Smaller clusters are the red clusters (connecting 'cryptography', 'accountability', and 'association rule mining') and the pink cluster (connecting 'AI' and 'threats'), and these two represent subfields that are still isolated from the bigger clusters, which means that they are still in development. The biggest three clusters (the purple cluster, the blue cluster, and the green cluster) are not densely connected with each other and there is evidently no coherent bridge that systematically maps how vulnerabilities correspond to different threat vectors across technical, methodological, and applied dimensions. From Figure 2, the fragmentation of the existing literature is clearly visible, together with the gap in the literature that tends to examine threats or vulnerabilities separately but rarely integrates them with empirical evidence of attacks, which is precisely the contribution of this study.

In order to present the answer to two research questions, Tables 1–3 were created. The tables are based on the original literature review that is presented in Table S1 (Appendix). Table 1 displays the

number of occurrences (number of times mentioned in the literature) of various cyber threat types. Table 1 describes all the types of cyber threats within the energy sector and Smart Grid environment that are described in the literature. The first column of Table 1 lists the specific types of cyber threats, while the second column explains the type of the threat and gives a concrete example from the real incidents that happened in the world (if applicable). The third column indicates the frequency at which each threat is mentioned. References from the literature cited are included in the third column of Table 1. This table answers the first research question of this paper:

Q 1. What are the most commonly mentioned types of cyber threats targeting the Smart Grid in the existing literature?

The most common types of cyber threats targeting the Smart Grid include: malware, denial of service (DoS); distributed denial of service (DDoS), advanced persistent threats (APTs), cross-site, data breaches, spoofing, Sybil attacks, and jamming. Malware and DoS are mentioned for seven times, APTs, cross-site, data breaches are mentioned for four times, and spoofing, Sybil attacks, and jamming are mentioned thrice each in total, which indicate that malware and DoS are the most common cyber weapons used.

Table 2 lists all the vulnerabilities of the systems that are encountered in the energy sector and Smart Grid. This table shows the number of occurrences of different vulnerability types. The first column of Table 2 lists the specific types of vulnerabilities in the Smart Grid, while the second column explains the vulnerability in the system, and if applicable, gives an example of the real-world energy system vulnerability that was exploited by the cyber threat. The third column indicates the frequency at which each threat is vulnerable in the reviewed literature. Table 2 answers the second research questions of this paper:

Q 2. What are the most critical vulnerabilities exploited in cyberattacks against energy infrastructure in the Smart Grid?

The most mentioned type of vulnerability in Smart Grids is insecure or weak protocols and communication. The second most mentioned vulnerabilities are legacy systems, and outdated software and hardware. Insecure, weak protocols, and communication are mentioned for 11 times in the review literature, and legacy systems, and outdated software and hardware are mentioned for seven times.

Table 1. The most common types of cyber threats in the Smart Grid.

Cyber threat type	Explanation and example of the threat	Frequency of occurrences in the literature	References
Malware	Malicious software used to infiltrate, damage, or disrupt systems. Example: Stuxnet exploited Siemens SCADA systems of the nuclear plant to sabotage and compromise centrifuges at Natanz [11–13].	7	[7, 8, 35–39]
Denial of Service (DoS); DDoS	Attackers overload systems or communication channels, making services unavailable. Example: Attackers disrupted SCADA and power distribution systems, which lead to power outage in Ukraine 2015 blackout [18, 21, 25].	7	[5, 35, 40–44]
Spoofing; Sybil; jamming	Spoofing is falsifying or disguising an identity. Sybil is a creation of multiple fake identities within a network. Jamming is disrupting or interfering with communication. Example: Manipulating with signals in order to mislead operators and cause power blackout.	3	[45–47]
Other (cross-site, blockchain, etc.)	Attacks in this category are less known, but also dangerous. cross-site attacks that target web-based control platforms and blockchain-based vulnerabilities. These attacks usually exploit smart contracts or insecure dashboards. Example: Cross-site scripting on web-based SCADA dashboards.	4	[44, 48–50]
Advanced persistent threats (APTs)	Long-term stealthy campaigns using phishing and credential theft. ATP highly sophisticated cyberattacks, usually carried out by state-sponsored hacker groups or well-organised criminal groups.	4	[6, 43, 51, 52]
Insider threats	Authorised employees misuse access or credentials. Example: Shamoon in Saudi Aramco in 2012, helped by weak insider policies.	3	[52–54]
Cyber-physical attacks; sabotage	These attacks are targeting physical processes and safety systems. Example: Triton/Trisis attempted to disable SIS in Saudi Arabia [14–17, 27, 28, 55, 56].	3	[47, 57, 58]
Data breaches/ falsification	Attackers in the Stuxnet attack did not only sabotaged centrifuges, but they also made sure that operator displays correct data in order to camouflage the damage and the attack, showing how manipulated data can hide physical sabotage [11–13].	4	[8, 35, 38, 46]
Unauthorised access	Gaining entry via weak authentication or exposed systems. Example: Colonial Pipeline - compromised virtual private network (VPN) creds without multi-factor authentication (MFA) [18, 30–33].	3	[7, 52, 59]
Man-in-the-middle (MitM)	Intercepting and altering communications. Example: BlackEnergy in Ukraine manipulated grid commands [18, 20, 21, 25, 60].	3	[41, 54, 59]
Ransomware	Encrypting information technology/operation technology (IT/OT) data and demanding ransom in order to encrypt data. Example: Colonial Pipeline caused a 6-day fuel disruption [18, 30–33].	2	[40, 61]

(*continues*)

Table 1. Continued.

Cyber threat type	Explanation and example of the threat	Frequency of occurrences in the literature	References
Injection/packet injection	Malicious commands injected into control traffic. Example: Industroyer manipulated IEC protocols to trip breakers [18, 20, 21, 25, 60].	2	[42, 62]
Botnets	Botnet is a hidden network of infected computers remotely controlled by hackers to launch large-scale attacks. Shamoon malware in Saudi Aramco was spread mimicking botnet-like propagation. Because of the botnet style of operating malware was enabled automatic replication throughout the network, data erasure, and large-scale system disruption [14, 15–17, 55, 56].	2	[59, 61]
Firmware threats/ exploitation	Stuxnet malware was designed to alter Siemens PLC firmware in order to sabotage the performance of the centrifuges at Natanz [11–13]. Triton/Trisis malware attacked Schneider Electric Triconex safety controllers with the intention of disabling Safety Instrumented System [14–17, 55, 56].	1	[63]
Phishing	Phishing email enabled the BlackEnergy malware to spread during Ukraine 2015 power grid attack, allowing for malware to access the SCADA system [18, 20, 21, 25, 60].	1	[40]
Zero-day attacks	Industroyer malware in Ukraine exploited previously unknown vulnerabilities in industrial communication protocols (e.g., IEC 61850 and IEC 60870-5-104) and caused power outages [18, 20, 21, 25, 60].	1	[64]

According to the literature, the biggest vulnerabilities that are present in the energy system and that are targeted by the cyber threats are insecure and weak protocols or communication. Industrial protocols are specific, and unlike IT protocols, they were not designed to protect data but to enhance the velocity of performance. The lack of built-in security mechanism, industrial protocols can be easily targeted and exploited. This vulnerability was targeted in the BlackEnergy cyberattack in Ukraine. Insecure and weak industrial protocols, such as IEC 60870-5-104, Modbus, and DNP3, were not originally designed with authentication or encryption mechanisms, which made them highly susceptible to manipulation. A clear example is the 2015 Ukraine power grid attack, in which malware exploited these protocol weaknesses in combination with stolen operator credentials disruption [18, 20, 21, 25, 60]. Unprotected industrial protocol IEC 60870-5-104 enabled the attackers to control substations. The unauthorised commands were sent (‘open breaker’ and ‘close breaker’ commands) to the substations, and

Table 2. The most critical vulnerabilities addressed in cyberattacks aiming the Smart Grid.

Critical vulnerability type	Explanation and example of vulnerability in the system	Frequency	References
Insecure; weak protocols; communication	Many ICS/SCADA protocols (e.g., Modbus, DNP3, and IEC 60870) lack built-in authentication/encryption/verification, enabling exploitation of the protocols. Example: exploited in BlackEnergy (Ukraine 2015) to shut down breakers [18, 20, 21, 25, 60]. SCADA components exposed online or with weak protocols. Example: Industroyer (2016) exploited IEC 61850/104 protocols to trip breakers [18, 20, 21, 25].	11	[8, 35, 37–39, 45, 47, 59, 65–67]
Legacy systems; outdated software; hardware	Old operating systems and control devices no longer receive patches, leaving them exposed. Example: Stuxnet malware targeted outdated Siemens PLC firmware at Natanz [11–13].	7	[6, 8, 37, 48, 50, 59, 68]
Lack of encryption; poor encryption	Lack of protocols and communication encryption enabled Ukraine power grid attacks in 2015 and 2016. Attacker exploited unencrypted IEC 60870 protocols and caused power outage [18, 20, 21, 25, 60]. Also, in Stuxnet attack, unsecured PLC communications were exploited in order to inject the malware [11–13]. Triton/Trisis malware exploited weak protective layers in safety controllers to sabotage the protection [15, 17, 55].	4	[45, 47, 65, 67]
Weak authentication; access control	Default or shared passwords, lack of multifactor authentication (MFA) make systems easy to breach. Example: Colonial Pipeline compromised VPN credentials without MFA [11–13].	5	[35, 36, 39, 45, 51]
Lack of standardised controls; governance gaps	Inconsistent security policies and lack of global cybersecurity standards weaken resilience of the energy sector. Example: Shamoon malware spread widely due to weak governance of endpoint security at Saudi Aramco [14–17, 55, 56].	3	[66, 69, 70]
Policy; strategy gaps; insufficient plans	Lack of or weak national or sectoral cyber strategies leave operators unprepared on a national level. Example: Ukraine in 2015 did not have coordinated national cyber defence, which ultimately enabled the malware to penetrate the grid [18, 25]. Furthermore, because of the weak contingency planning and lack of response mechanisms, ransomware exploited the weakness and attacked Colonial Pipeline [30, 32].	3	[40, 69, 70]
Insecure; poor network topology; segmentation	Flat networks allow attackers to move from IT to operational technology (OT) environments. Example: Triton/Trisis malware attackers reached SIS controllers due to poor segmentation [14, 15, 17, 27, 28, 55, 56].	4	[8, 37, 39, 57]
Firmware; device vulnerabilities	Exploitable flaws in PLC or device firmware. Example: Stuxnet replaced Siemens PLC code to manipulate centrifuge speeds [11–13].	2	[7, 35]
IoT integration flaws; insecure internet of things (IoT)	IoT devices in Smart Grids and energy infrastructure do not have security features implemented (strong authentication or patching), which makes them a weak spot.	2	[35, 39]
Human error; lack of training; awareness	Employees fall for phishing or misconfigure systems. Example: BlackEnergy (2015) initial infection vector via spear-phishing [18, 20, 21, 25].	2	[40, 48]

(*continues*)

Table 2. Continued.

Critical vulnerability type	Explanation and example of vulnerability in the system	Frequency	References
Lack of real-time threat detection; monitoring	Without timely detecting malware or anomalies in the system, advanced persistent threat (APT) is in a persistent presence. Example is Ukraine Industroyer and CrashOverride malware that was undetected when injected and detected after activation, which means malware was in the system undetected for significant amount of time [25].	3	[63, 71, 72]
Insufficient endpoint protection	Lack of antivirus or endpoint security leaves IT systems open. Example: Shamoon wiped 30,000 PCs at Saudi Aramco [14–17, 55, 56].	1	[5]
Testing and simulation exposure	When testing certain functionality within the system, testing environment must be protected. For example, Colonial Pipeline attack showed how lack of testing, simulations, and preparedness for ransomware attack could be fatal.	2	[46, 71]
Ethical framework gaps	Lack of norms and laws around critical infrastructure cyber defence. Example: Policy debates after Stuxnet highlighted legal and ethical gaps in cyber warfare [11–13].	1	[40]
Lack of resilience; redundancy	No backup systems for critical operations. Example: Ukraine 2015 blackout showed how lack of redundancy worsened outages [18, 20, 21, 25].	1	[35]
Chip-level hardware vulnerabilities	Exploitable failures at hardware/firmware level. Example: Stuxnet malware altered Siemens PLC firmware in order to sabotage centrifuges at the power plant [11–13].	1	[50]

the used protocol was not able to detect malicious instructions or to verify the authenticity of the commands that lead to blackouts [18, 20, 21, 25, 60]. This case demonstrates that insecure communication protocols act as an enabler of cyber threats, transforming a credential theft into a large-scale operational disruption [18, 20, 21, 25, 60]. The second biggest vulnerability is legacy system and outdated software or hardware. Usually in the energy infrastructure legacy systems, outdated software and hardware are used for many years (even decades). This is because energy infrastructure and environment (or industrial infrastructure in general) have to work 24×7, without interruptions, and doing update or patch of the system can be very complicated because every system shutdown can be very risky. That is why energy infrastructure is an attractive target for advanced malware [11–13]. A well-known example is the Stuxnet malware attack, which specifically targeted Siemens S7-300 Programmable Logic Controller (PLC) running outdated firmware in the Natanz nuclear facility [11–13]. The attackers exploited multiple zero-day vulnerabilities in Windows systems to successfully infect the malware. The malicious code was injected into PLCs' firmware.

The legacy devices did not have any modern security mechanisms implemented (such as code signing, intrusion detection, or integrity verification), and the malicious malware ran undetected. Stuxnet altered the logic of the centrifuge controllers while simultaneously sending falsified feedback signals to operators, hiding the sabotage. The outdated and unpatched hardware and firmware was the core vulnerability that enabled the attack to succeed [11–13].

Table 3 shows the correlation between vulnerabilities and cyber threats discussed in the reviewed literature. Table S1 of the systematic literature review is available in the Appendix. The first column of Table 3 displays the various types of cyber threats that have been researched in the literature. For each type of cyber threat, there is a corresponding critical vulnerability that enables that specific threat to jeopardise the Smart Grid. The idea is to understand the vulnerability that can be exploited by the threat. The second column contains mapped vulnerability; the third column of the table has the mechanism of exploitation; and the last column gives a real-world example (if it exists for that particular threat or vulnerability). It is important to stress that some of the vulnerabilities overlap across different types of cyber threats. This is because, in the real-world scenarios, different types of energy infrastructure and system vulnerabilities are dependent on each other, meaning that vulnerabilities cannot be definitely segregated from each other. For example, malware, APTs, ransomware, and botnets exploit both weak authentication and insecure protocols, whereas legacy systems and poor segmentation are responsible for both cyber-physical sabotage and data breaches. An important conclusion that can be drawn from Table 3 is that one type of cyber threat can exploit more than one vulnerability. This again means that if one vulnerability is taken under control, more than one threat can be neutralised. Table 3 also shows the exact mechanisms through which vulnerabilities enable specific attacks. Mapping of vulnerabilities and cyber threats in Smart Grid and energy infrastructure proves that a relatively small set of critical vulnerabilities enables multiple cyber threats, which is again underscoring the need for integrated and systemic defence strategies. For example, the Stuxnet attack on Iran's Natanz facility in 2010 demonstrated how malware exploited firmware vulnerabilities and SCADA system in order to physically destroy critical assets of the infrastructure [11–13, 37, 47]. Another example is the Ukraine blackouts of 2015 and 2016, caused by the BlackEnergy and Industroyer malware that exploited weak authentication mechanisms and weak protocols, which at the end led to power disruption on the national level [18, 21, 25]. In 2017, Triton/Trisis targeted Safety Instrumented Systems (SIS) in Saudi petrochemical plant

and exploited insecure control mechanism. When it comes to Colonial Pipeline ransomware attack, weak VPN credential management vulnerability caused fuel shortage in East Coast. In Saudi Aramco, 30,000 hard disks were deleted due to compromised internal accounts and the abuse of access rights.

All of the described vulnerabilities that cyber threats exploited stress how important it is to understand the negative cause-and-effect relationship between vulnerabilities and cyber threats in the Smart Grid. If vulnerability exists, it will be exploited. Furthermore, in nearly all documented real-world cases, the detection of malware, ransomware, and other threats required several days, during which evident disruptions in energy distribution or internal system operations had already manifested [11, 13–15, 17, 18, 20, 25, 30, 31, 33, 55]. Most of the attackers stay under the radar in the system for a while in order to gather all necessary data for the attack to be fully successful and even more destructive.

4. Discussion

Table 3 highlights that insecure or weak protocols and poor communication are among the major issues and common vulnerabilities that facilitate cyberattacks in the Smart Grid. Insecure or weak protocols and poor communication are identified as significant weaknesses and potential vulnerabilities for cyber threats across nearly all types listed in Table 3. Certain types of cyber threats, such as firmware threats, insider threats, and phishing, do not rely directly on insecure or weak protocols. However, it is important to note that the most common threats mentioned in the literature (presented in Table 1), malware and DoS attacks, are primarily dependent on these insecure or weak protocols and communication methods. Other vulnerabilities mapped for malware and DoS attacks are weak authentication, inadequate access control, outdated systems, poor network design, and insecure Internet of things (IoT) devices. Alongside the most common vulnerability, weak, or insecure communication protocols, these factors create an optimal opportunity for cyber attackers to exploit Smart Grid systems. When addressing cyber threats, such as spoofing, Sybil attacks, and jamming, one of the most common vulnerabilities is the use of insecure or weak protocols and communication methods. Additionally, a significant vulnerability associated with these cyber threats is the lack of encryption or the use of ineffective encryption methods. Both the absence of encryption and poor encryption practices are particularly relevant to spoofing, Sybil attacks, and jamming. Cyber threats categorised as others, such as cross-site,

Table 3. Mapped critical vulnerabilities and corresponding cyber threats with the real-world cyberattack examples.

Cyber threat	Mapped critical vulnerabilities	Mechanism of exploitation	Real-world case example
Malware	Insecure protocols [8, 35, 37–39]; weak authentication [35, 36, 39]; firmware/device vulnerabilities [7, 37]; legacy systems [8, 37]; poor segmentation [8, 37, 39]; insecure IoT [35, 39]; lack of redundancy [35]	Exploits unpatched SCADA/ICS or outdated operating systems (spreading via weak authentication and outdated PLC firmware)	Stuxnet (2010) – sabotaged Natanz centrifuges via Siemens SCADA/PLC [11–13]
Denial of service (DoS/ DDoS)	Weak protocols [35, 40, 42, 43, 44]; policy gaps [40, 70]; governance gaps [66, 70]; human error [40]; testing exposure [46, 71]	Flooding protocols like Modbus/DNP3 channels; exploiting lack of redundancy	BlackEnergy (Ukraine 2015) – SCADA shutdown and power outage [18, 20, 21, 25, 60]
Spoofing/ jamming	Weak protocols [45, 47]; poor encryption [45, 47]; weak authentication [45]; testing exposure [46]	GPS spoofing; falsified grid synchronisation signals	Stuxnet created false data displayed on Human-Machine Interface (HMI) in order to maintain hidden and in order not to be detected [11–13].
Other (XSS, blockchain flaws)	Legacy systems [48, 50]; human error [48]; governance gaps [66, 69]; policy gaps [69]	Cross-site scripting on SCADA dashboards; smart contract flaws	General ICS/blockchain risks – less linked to major outages
Advanced persistent threats (APTs)	Weak authentication [36, 51]; legacy systems [2]; SCADA protocol flaws [6, 70]; weak protocols [35, 39]	Long-term infiltration via spear-phishing, credential theft	Industroyer (2016) – automated manipulation of IEC 61850/104 [18, 20, 21, 25, 60].
Insider threats	Weak authentication [51]; policy gaps [40]; governance gaps [69]	Employees exploiting access rights, lack of monitoring/logs	Shamoon (2012) – internal spread, 30,000 PCs wiped in Saudi Aramco [14–17, 55, 56].
Cyber-physical attacks/ sabotage	Poor segmentation [37, 57]; SCADA exposure [6, 70]; weak protocols [47]	Manipulation of safety systems	Triton/Trisis (2017) – targeted Triconex SIS, risk of explosion [14–17, 55, 56].
Data breaches/ falsification	Weak protocols [8, 38]; weak authentication [35]; poor encryption [47, 65]	Intercepting grid communication; falsifying data	Stuxnet (2010): falsified centrifuge data, so operators saw normal values while sabotage occurred [11–13].
Unauthorised access	Weak authentication [35, 52]; legacy systems [59]; SCADA flaws [59]	Remote access abuse through default passwords or outdated VPNs	Colonial Pipeline (2021) – VPN creds without MFA and ransomware shutdown [18, 30–33]
Man-in-the-middle (MitM)	Weak protocols [41, 54]; weak authentication [45]; SCADA flaws [59]	Intercepting and altering grid commands	BlackEnergy (2015) – adversaries manipulated breaker commands [18, 20, 21, 25, 60].

(*continues*)

Table 3. Continued.

Cyber threat	Mapped critical vulnerabilities	Mechanism of exploitation	Real-world case example
Ransomware	Weak authentication [40]; policy gaps [40]	Encrypting IT/OT data, ransom demand	Colonial Pipeline (2021) – DarkSide ransomware disrupted fuel supply chain [18, 30–33].
Injection/ packet injection	Weak protocols [42, 62]	Malicious commands injected into control traffic	Industroyer (2016) – injected packets into IEC protocols to trip breakers [18, 20, 21, 25, 60].
Botnets	Weak authentication [59, 61]	Using insecure IoT devices for DDoS	Shamoon (2012): spread rapidly across 30,000 systems, mimicking botnet-like propagation through worm-style replication explosion [14–17, 55, 56].
Firmware exploitation	Device vulnerabilities [7, 35, 63]; chip-level vulnerabilities [50]	Exploiting firmware flaws or supply-chain tampering	Stuxnet (2010): modified Siemens PLC firmware to alter centrifuge operations [11–13].
Phishing	Human error [40]	Employees deceived into clicking malicious links that were entry vector for APTs	BlackEnergy (2015) – initial spear-phishing compromise [18, 20, 21, 25, 60].
Zero-day exploits	Lack of real-time detection [64]	Exploiting unknown flaws before patches exist	Industroyer (2016): exploited previously unknown flaws in industrial communication protocols (IEC 61850 and IEC 60870-5-104) to trip breakers [18, 20, 21, 25, 60].

blockchain, and sabotage, result from outdated software, human errors, or insufficient training. Additionally, there are risks associated with chip-level hardware vulnerabilities. APTs are linked to vulnerabilities, such as weak authentication, inadequate access control, legacy systems, outdated software, exposure of SCADA systems, and flaws in protocols. Insider threats and phishing arise from human error, insufficient training and awareness, a lack of standardised controls, and governance gaps. Vulnerabilities in firmware and devices lead to firmware threats. Conversely, data breaches, data falsification, unauthorised access and zero-day attacks arise from insecure or weak protocols, poor communication, lack of encryption or poor encryption, weak authentication, poor access control, firmware, and device vulnerabilities. Man-in-the-middle (MitM) attacks and ransomware stem from vulnerabilities such as

insecure or weak protocols, poor communication, weak authentication, inadequate policies, strategic gaps, insufficient planning, human error, and a lack of training. Botnets originate from insecure or weak protocols as well as ineffective communication methods.

As mentioned previously, vulnerabilities and corresponding cyber threats do overlap. In order to reduce redundancy and get more clear view on the dependencies, Table 4 presents mapping of critical vulnerabilities and the corresponding cyber threats without overlapping. Both threats and vulnerabilities are grouped into five clusters (clusters were based on the similarities between categories, and grouping-related vulnerabilities under broader themes) and contain all the overlapping threats and vulnerabilities. Table 4 gives a more comprehensive and direct groups of the threats and vulnerabilities, whereas Table 3 gives a more fine-grained and in-depth overview of each threat and vulnerability present in the Smart Grid.

Names of the clusters in Table 4 describe the essence of vulnerability. For example, the first cluster named 'authentication & access weaknesses' consists of following vulnerabilities: weak authentication, poor access control, and insecure VPNs. Hence, the name of the first cluster: authentication and access weaknesses. It can be concluded from Table 3 that threats associated with authentication or access vulnerabilities are: malware, APTs, insider threats, unauthorised access, ransomware, and botnets. For the second cluster named 'protocol and communication gaps', which consists of insecure SCADA/ICS protocols (Modbus, DNP3, and IEC 60870), lack of encryption, and MitM vulnerabilities, the associated threats are: malware, DoS/DDoS, APTs, data falsification, and MitM injection. For the third cluster of vulnerabilities 'legacy and device vulnerabilities', the mapped threats are: malware, firmware exploitation, and cyber-physical sabotage. The fourth cluster is named 'governance and policy gaps', which contains lack of standardised controls, weak governance, and insufficient resilience planning vulnerabilities, which again correspond to APT entry vectors, phishing, and insider threats. The final cluster is named 'human and organisational factors', and it consists of human error, phishing susceptibility, and lack of training, which can be exploited by APT entry vectors, phishing, and insider threats.

Mapping of cyber threats and system vulnerabilities in the Smart Grid and energy infrastructure in general is highly useful in practice and can be applied in different fields. Table 5 gives a presentation of the areas where mapping of cyber threats and system

Table 4. Mapped critical vulnerabilities and the corresponding cyber threats without overlapping.

Cluster	Core vulnerabilities	Associated threats	Real-world examples
Authentication and access weaknesses	Weak authentication, poor access control, insecure VPNs	Malware, APTs, insider threats, unauthorised access, ransomware, botnets	Shamoon (2012), Colonial Pipeline (2021)
Protocol and communication gaps	Insecure SCADA/ICS protocols (Modbus, DNP3, and IEC 60870), lack of encryption, man-in-the-middle (MitM)	Malware, DoS/DDoS, APTs, data falsification, MitM injection	Ukraine Blackouts (2015, 2016), Industroyer (2016)
Legacy and device vulnerabilities	Outdated OS, legacy PLCs, firmware flaws, chip-level risks	Malware, firmware exploitation, cyber-physical sabotage	Stuxnet (2010), Triton/Trisis (2017)
Governance and policy gaps	Lack of standardised controls, weak governance, insufficient resilience planning	DoS/DDoS, insider threats, ransomware, others (cross-site, blockchain flaws)	General industrial control systems (ICS) governance failures, blockchain exploits
Human and organisational factors	Human error, phishing susceptibility, lack of training	APT entry vectors, phishing, insider threat	BlackEnergy (2015 spear-phishing), Saudi Aramco (2012)

vulnerabilities can be applied. The first column indicates application area; the second column describes and gives an example how mapping of threat and vulnerabilities can be applied, and the third column suggests the potential users. For example, mapping can be very useful for regulatory alignment. By prioritising threats and vulnerabilities, the findings provide a structured basis for demonstrating compliance with established cybersecurity regulations and standards, such as the European Union's NIS2 (Directive on Security of Network and Information Systems 2) directive and the NERC CIP framework (North American Electric Reliability Corporation). This alignment is particularly relevant for policymakers and regulators, as it enables them to translate technical vulnerabilities into actionable regulatory requirements and oversight mechanisms. Furthermore, mapping of critical vulnerabilities and threats can be helpful in risk assessment frameworks, because it helps in enhancing risk assessment processes in the energy sector. Both energy providers and critical infrastructure operators can correctly enhance risk assessment processes. When it comes to defence strategy, mapping of cyber threats and system vulnerabilities can be crucial for developing efficient defence strategies (intrusion detection systems, network segmentation, or encryption). Finally, knowing the vulnerability that enables the threat can help in incident response by stressing correlation of vulnerabilities and specific attack vectors.

Table 5. Practical application of threats and vulnerabilities mapping.

Application area	Description	Potential users
Regulatory alignment	Supports alignment with cybersecurity regulations and standards (e.g., NIS2, NERC CIP) by prioritising threats and vulnerabilities.	Policymakers, regulators
Risk assessment frameworks	Provides a structured mapping of threats and vulnerabilities to enhance risk assessment processes in the energy sector.	Energy providers, critical infrastructure operators
Defence strategy improvement and design	Facilitates the development of layered defence strategies, such as intrusion detection systems, network segmentation, and encryption.	Security architects, system engineers
Incident response and forensics	Improves incident response by highlighting correlations between vulnerabilities and specific attack vectors.	Computer emergency response teams (CERT) response, forensic investigators

Furthermore, the vulnerabilities that are identified in this paper can be mapped to a requirement of the NERC CIP standard. For example, weak authentication and poor access control can be mapped to CIP-005 (electronic security perimeter and access control), and legacy systems and outdated firmware can correspond to CIP-007 (system security management, patching, and updates). Weak incident reporting and response procedures can be correlated to CIP-008 (incident reporting and response planning).

Furthermore, mapping of cyber threats and vulnerabilities can be used as a part of risk assessment frameworks in order to explain how human error, weak authentication, and insecure communication protocols continuously enable for cyberattacks to happen and be successful, while NIS2 focuses on systematic risk assessment, incident management, and employee awareness. The NERC CIP standards focus on who, and how, can access critical systems and on detection, response, and reporting of security incidents, which are directly reflected in unauthorised access via weak VPN credentials, legacy systems lacking updates, and unpatched firmware exploited in high-profile attacks like Stuxnet and Triton. This study can be viewed as an evidence-based mapping of the vulnerabilities that most often lead to the types of cyber threats and a suggestion on how high-level regulatory requirements with concrete and real-world attack pathways provide regulators, policymakers, and operators with a clearer foundation for prioritising compliance, strengthening defences, and directing resources with the most critical risks. Another application is in designing defence strategies. By understanding threat vulnerability mapping, a secure defence mechanism can be constructed in order to protect energy

infrastructure. For example, the evident problem of insecure industrial protocols used in the energy infrastructure highlights the need for better encryption of industrial control protocols. Finally, threat vulnerability mapping can be useful for incident response and forensics. After a cyberattack, it is crucial to understand all steps undertaken by the attackers. Digital forensics is the best tool to uncover all the steps and potential entry points, attack process, and progression. Threat vulnerability mapping helps responders to focus their analysis and containment efforts more effectively.

There are several limitations to this study that have to be acknowledged. The study is based and relies on secondary literature reviewed in the systematic literature review, which again is a product of the lack of primary studies, research, and direct empirical evidence. Even though the study is based on secondary sources, its contribution lies in the first systematic mapping between threats and vulnerabilities in the energy sector and offers an insight that was not provided in the literature before. Another limitation is the fact that the literature analysed is predominantly in English, which may narrow down relevant studies that may explore correlations between threats and vulnerabilities within the energy sector. It is also important to stress that this study is specifically focused on the Smart Grid and energy infrastructure and cannot be fully applicable to all other types of critical infrastructure.

The future research should focus on developing real-time threat detection models, ideally utilising AI and machine learning. The goal of these models is to identify and respond to threats in real time within the Smart Grid. AI is increasingly integrated into IoT, especially within Smart Grids. This integration complicates the cyber threat landscape. Therefore, it is essential to continually improve and strengthen cybersecurity measures for Smart Grids. This paper does not focus on proposing specific solutions to address the vulnerabilities within the Smart Grid or on minimising associated threats. Instead, this research is dedicated to identifying correlations between cyber threats and vulnerabilities in the Smart Grid by mapping these threats to the identified vulnerabilities. For the future research, it would be beneficial to concentrate specifically on addressing these vulnerabilities and reducing the likelihood of cyberattacks that exploit them.

5. Conclusions

As critical structure is becoming even more endangered in the modern digital world, the need for deeper understanding of the

cyber threats and the vulnerabilities of the energy infrastructure and system is becoming even more evident. Energy infrastructure as a part of critical infrastructure has been a target of cyberattacks numerous times in the last decade. There are many examples from the real-world cyberattacks on energy infrastructure that showed how multiple vulnerabilities of the system could be exploited by cyber threats. In order to be able to successfully defend the energy infrastructure, it is important to fully understand correlations between cyber threats and vulnerabilities of the system.

This paper conducted a systematic literature review in order to investigate whether particular vulnerabilities enable particular cyberattacks. As the research emphasises, weak protocols and poor communication are primary weaknesses of the Smart Grid. Insecure or weak protocols and inadequate communication are major cyber threat vulnerabilities across nearly all types of cyber threats. Firmware, insider threats, and phishing threats do not directly use insecure protocols [6, 43, 51, 52]. Malware and DoS attacks are the most common threats in the literature and they rely on these vulnerable protocols and communication mechanisms [7, 8, 35–39]. Malware and DoS attacks also target weak authentication, access control, old systems, poor network design, and vulnerable IoT devices [7, 8, 35–39]. These elements, along with the most typical vulnerability, weak or unsecure communication protocols, make Smart Grid systems ideal for cyberattacks. Insecure protocols and communication methods are a typical vulnerability for cyber threats, such as spoofing, Sybil attacks, and jamming [6, 43, 51, 52]. These cyber risks are also vulnerable to lack of or poor encryption [6, 8, 37, 48, 50, 59, 68]. Lack of encryption and bad encryption methods affect spoofing, Sybil attacks, and jamming [45, 47, 65, 67]. Other cyber threats include cross-site, blockchain, and sabotage originating from old software, human errors, or inadequate training [44, 48–50]. Additionally, chip-level hardware vulnerabilities pose danger. APTs are linked to weak authentication, access control, legacy systems, outdated software, SCADA system exposure, and protocol issues. Human mistakes, poor training and poor awareness, unstandardised processes, and governance gaps cause insider threats and phishing. Device and firmware vulnerabilities cause firmware threats [6, 43, 51, 52]. Insecure protocols, inadequate communication, lack of encryption, weak authentication, poor access control, firmware, and device vulnerabilities cause data breaches, data fabrication, unauthorised access, and zero-day attacks [8, 35, 38, 46]. MitM attacks and ransomware are caused by insecure protocols, poor communication, weak authentication, inadequate policies, strategic gaps, insufficient planning, human

mistake, and lack of training [41, 54, 59]. Insecure protocols and communication mechanisms cause botnets.

It is vital to point out that some of the weaknesses are the same for different kinds of cyber threats. This is because, in real life, different forms of energy infrastructure and system vulnerabilities depend on one another, which means that vulnerabilities cannot be completely separated from one another. Malware, APTs, ransomware, and botnets exploit weak authentication and insecure protocols. Legacy systems and bad segmentation, on the other hand, are to blame for both cyber-physical sabotage and data breaches. Mapping the vulnerabilities and cyber threats in Smart Grid and energy infrastructure shows that a small number of important vulnerabilities can lead to many cyber threats. This shows again, why we need integrated and systemic defence methods. The Stuxnet attack on Iran's Natanz facility in 2010, for instance, showed how malware might use firmware and SCADA system weaknesses to physically damage important parts of the infrastructure [11–13, 37, 47]. The 2015 and 2016 blackouts in Ukraine and the BlackEnergy and Industroyer viruses that took advantage of weak authentication and protocols are further examples. These events caused power outages on a national level [18, 21, 25]. In 2017, Triton/Trisis attacked safety instrumented systems (SIS) at a petrochemical plant in Saudi Arabia and took advantage of a weak control mechanism. The Colonial Pipeline ransomware attack caused a fuel scarcity on the East Coast because of a flaw in how weak VPN credentials were handled. Saudi Aramco erased 30,000 hard drives because of hacked internal accounts and the misuse of access permissions. All of the weaknesses that cyber threats took advantage of show how vital it is to understand the negative cause-and-effect link between vulnerabilities that cyber threats in the Smart Grid. If the weakness is there, it will be used against the system.

The findings of this paper align closely with the requirements of the NIS2 Directive as well as NERC CIP standards, such as CIP-005 on access control, CIP-007 on patch management, and CIP-008 on incident reporting. The practical implications of the findings extend to multiple domains: regulatory alignment, risk assessment frameworks, improvement of defence strategy, and incident response and forensics.

References

[1] V. Mahor, R. Rawat, A. Kumar, M. Chouhan, R.N. Shaw, et al., "Cyber warfare threat categorization on CPS by Dark Web Terrorist," in P. Kumar, A. Kumar, and R.P. Goyal (eds.), *2021 IEEE 4th International Conference on Computing,*

Power and Communication Technologies, GUCON 2021. New York, NY: Institute of Electrical and Electronics Engineers (IEEE), Sep. 2021, doi: 10.1109/GUCON50781.2021.9573994.

[2] D. Musakhanov. (2023). "The international consequences of cyber warfare: A study of the 'Stuxnet' case." Acta of Turin Polytechnic University in Tashkent, *Technical Science and Engineering*, vol. 13, no. 3, pp. 47–50.

[3] A. Bagchi, T. Bandyopadhyay, "Role of intelligence inputs in defending against cyber warfare and cyberterrorism," *Decision Analysis*, vol. 15, no. 3, pp. 174–193, 2018, doi: 10.1287/deca.2018.0370.

[4] M.B.E. Saaida, "The use of cyber warfare and its impact on international security." [Online]. Available: https://zenodo.org/records/10841887. [Accessed 14.02.2025].

[5] T. Plėta, M. Tvaronavičienė, S. Della Casa, K. Agafonov, "Cyberattacks to critical energy infrastructure and management issues: Overview of selected cases," *Insights into Regional Development*, vol. 2, no. 3, pp. 703–715, 2020, doi: 10.9770/ird.2020.2.3(7).

[6] I. Priyadarshini, R. Kumar, R. Sharma, P.K. Singh, S.C. Satapathy, "Identifying cyber insecurities in trustworthy space and energy sector for smart grids," *Computers and Electrical Engineering*, vol. 93, no. C, 2021, doi: 10.1016/j.compeleceng.2021.107204.

[7] C.C. Sun, A. Hahn, C.C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018, doi: 10.1016/j.ijepes.2017.12.020.

[8] A.B. Ige, E. Kupa, O. Ilori, "Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources," *International Journal of Science and Research Archive*, vol. 12, no. 1, pp. 2978–2995, 2024, doi: 10.30574/ijsra.2024.12.1.1186.

[9] I.-E. Ene, D. Savu, "Cybersecurity – A permanent challenge for the energy sector," *Romanian Cyber Security Journal*, vol. 5, no. 1, pp. 107–119, May 2023, doi: 10.54851/v5i1y202310.

[10] S.K. Venkatachary, J. Prasad, R. Samikannu, "Cybersecurity and cyber terrorism – in energy sector – A review," *Journal of Cyber Security Technology*, vol. 2, no. 3–4, pp. 111–130, 2018, doi: 10.1080/23742917.2018.1518057.

[11] G. Selján, "The remarkable 10th anniversary of Stuxnet," *Academic and Applied Research in Military and Public Management Science*, vol. 19, no. 3, pp. 85–98, 2020, doi: 10.32565/aarms.2020.3.6.

[12] B. Bakić, M. Milić, I. Antović, D. Savić, T. Stojanović, "10 years since Stuxnet: What have we learned from this mysterious computer software worm?," in V. Devedžić, V. Milutinović, and Z. Budimac, (eds.)., *25th International Conference on Information Technology, IT 2021*. New York, NY: Institute of Electrical and Electronics Engineers (IEEE), 2021, doi: 10.1109/IT51528.2021.9390103.

[13] C. Stevens, "Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet," *Contemporary Security Policy*, vol. 41, no. 1, pp. 129–152, Jan. 2020, doi: 10.1080/13523260.2019.1675258.

[14] S. Alelyani, H. Kumar G R, "Overview of cyberattack on Saudi organizations," *Journal of Information Security and Cybercrimes Research*, vol. 1, no. 1, pp. 32–39, 2018, doi: 10.26735/16587790.2018.004.

[15] R.A. Al-Mulhim, A. Al-Zamil, F.M. Al-Dossary, S. Arabia. (2020). "Cyber-attacks on Saudi Arabia environment." [Online]. Available: https://www.researchgate.net/publication/343497060_Cyber-attacks_on_Saudi_Arabia_Environment. [Accessed 15.04.2025].

[16] F. Alharbi, "Twelve years of cyber resilience: Analyzing cyberattacks in Saudi Arabia (2012–2024)," *TEM Journal*, vol. 14, no. 2, pp. 1791–1807, 2025, doi: 10.18421/TEM142-77.

[17] A. Alsaeed, "The cyber attack on Saudi Aramco in 2012," *Asian Journal of Engineering and Applied Technology*, vol. 10, no. 2, pp. 25–28, 2021, doi: 10.51983/ajeat-2021.10.2.3057.

[18] L. Pitman, W. Crosier, "On the scale from ransomware to cyberterrorism: The cases of JBS USA, Colonial Pipeline and the wiperware attacks against Ukraine," *Journal of Cyber Policy*, vol. 9, no. 2, pp. 179–199, 2024, doi: 10.1080/23738871.2024.2377670.

[19] M. Baezner, "Cyber and information warfare in the Ukrainian conflict," *CSS Cyberdefense Hotspot Analyses*, vol. 1, pp. 1–56, 2018, doi: 10.3929/ethz-b-000321570.

[20] S. Beska, Cyber Resilience in Ukraine: Measuring Response to Cyber Threats in the Context of Hybrid Warfare, M.S. thesis, Dept. of International Relations, Central European Univ., Vienna, Austria, 2025.

[21] V. Vanivska, J. Kuźniar, M. Kocik, A. Świrad, "Digital battleground: Analyzing cyber warfare between Russia and Ukraine since 2014," *Advances in Web Development Journal*, vol. 2 no. 1, pp. 1–17, 2024.

[22] S. Owusu, "The rising threat: Cybersecurity risks in critical energy infrastructure," *Global Energy Perspectives*, vol. 12, no. 3, pp. 45–67, 2023.

[23] Ministry of Defence Republic of North Macedonia. (2019). "Contemporary Macedonian Defence – Ministry of Defence, Republic of North Macedonia." [Online]. Available: http://www.morm.gov.mk/sovremena-makedonska-odbrana/. [Accessed 15.04.2025].

[24] J. Slowik, "Anatomy of an attack: Detecting and defeating CRASHOVERRIDE," in *Proc. Virus Bulletin Conf. (VB2018)*, Montreal, Canada, Oct. 2018. [Online]. Available: https://www.virusbulletin.com/conference/vb2018/abstracts/anatomy-attack-detecting-and-defeating-crashoverride/ [Accessed 09.05.20205].

[25] J. Slowik, *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*. Hanover, MD: Dragos, Inc., 2017. [Online]. Available: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE-01.pdf [Accessed 13.04.2025].

[26] S. Rector. (2024). "A case study of the CRASHOVERRIDE malware, its effects and possible countermeasures." [Online]. Available: https://digitalcommons.odu.edu/covacci-undergraduateresearch/2024spring/projects/5. [Accessed 15.04.2025].

[27] B. Jeffries. (2022). "Cyber risk to mission case study: Triton." [Online]. Available: https://attack.mitre.org/matrices/ics/. [Accessed 15.04.2025].

[28] J. Slowik. (2022). "Zeroing in on Xenotime: Analysis for the entities responsible for the Tirton event." [Online]. Available: https://www.virusbulletin.com/conference/vb2022/abstracts/zeroing-xenotime-analysis-entities-responsible-tri-ton-event/. [Accessed 11.05.2025].

[29] R. Kumar, R. Kela, S. Singh, R. Trujillo-Rasua, "APT attacks on industrial control systems: A tale of three incidents," *International Journal of Critical Infrastructure Protection*, vol. 37, no. C, p. 100521, 2022, doi: 10.1016/j.ijcip.2022.100521.

[30] T.J. Olorunlana, H. Mohammed, "Analysis of the Colonial Pipeline cybersecurity incident," *International Journal of Science, Architecture, Technology and Environment*, vol. 2, pp. 9–13, 2025, doi: 10.63680/jngh0767as.

[31] S. Bellamkonda, "Ransomware attacks on critical infrastructure: A study of the Colonial Pipeline incident," *International Journal of Research in Computer Applications and Information Technology (IJRCAIT)*, vol. 7, no. 2, pp. 1423–1433, 2024, doi: 10.5281/zenodo.14191113.

[32] L. Gawazah, A. Rondla, and M.S.A. Balhareth, "To pay or not to pay: The US Colonial Pipeline ransomware attack," *Global Journal of Engineering and Technology Advances*, vol. 22, no. 3, pp. 9–16, 2025, doi: 10.30574/gjeta.2025.22.3.0038.

[33] R. Dudley, D. Golden. (2021). "The Colonial Pipeline ransomware hackers had a secret weapon: Self-promoting cybersecurity firms the extortion." [Online]. Available: https://www.propublica.org/article/the-colonial-pipeline-ransomware-hac. [Accessed 11.05.2025].

[34] M.J. Page, J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ Journal,* vol. 372, p. 71, 2021, doi: 10.1136/bmj.n71.

[35] I.-E. Ene, D. Savu, "Cybersecurity – A permanent challenge for the energy sector," *Romanian Cyber Security Journal*, vol. 5, no. 1, pp. 107–119, 2023, doi: 10.54851/v5i1y202310.

[36] M. Alghassab, "Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector," *Energies*, vol. 15, no. 1, 2022, doi: 10.3390/en15010218.

[37] H. Zhang, B. Liu, H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021, doi: 10.1109/ACCESS.2021.3058628.

[38] I. Alotaibi, M.A. Abido, M. Khalid, A.V. Savkin, "A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources," *Energies*, vol. 13, no. 23, 6269, 2020, doi: 10.3390/en13236269.

[39] K. Kimani, V. Oduol, K. Langat, "Cyber security challenges for IoT-based smart grid networks," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, 2019, doi: 10.1016/j.ijcip.2019.01.001.

[40] S.J. Pinto, P. Siano, M. Parente, "Review of cybersecurity analysis in smart distribution systems and future directions for using unsupervised learning methods for cyber detection," *Energies*, vol. 16, p. 1651, 2023, doi: 10.3390/en16041651.

[41] R. Leszczyna, "A review of standards with cybersecurity requirements for smart grid," *Computers and Security*, vol. 156, no. C, 2018, doi: 10.1016/j.cose.2018.03.011.

[42] A. Ibrahim, C. Valli, I. McAteer, J. Chaudhry, "A security review of local government using NIST CSF: A case study," *Journal of Supercomputing*, vol. 74, no. 10, pp. 5171–5186, 2018, doi: 10.1007/s11227-018-2479-2.

[43] N. Mohamed, A. Oubelaid, S.K. Almazrouei, "Staying ahead of threats: A review of AI and cyber security in power generation and distribution," *International Journal of Electrical and Electronics Research (IJEER)*, vol. 11, no. 1, pp. 143–147, 2023, doi: 10.37391/ijeer.110120.

[44] P.I. Radoglou-Grammatikis, P.G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *IEEE Access*, vol. 7, pp. 46595–46620, 2019, doi: 10.1109/ACCESS.2019.2909807.

[45] M.Z. Gunduz, R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol. 169, p. 107094, 2020, doi: 10.1016/j.comnet.2019.107094.

[46] T.D. Le, A. Anwar, S.W. Loke, R. Beuran, Y. Tan, "Grid attacksim: A cyber attack simulation framework for smart grids," *Electronics*, vol. 9, no. 8, pp. 1–21, 2020, doi: 10.3390/electronics9081218.

[47] C. Peng, H. Sun, M. Yang, Y.L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554–1569, 2019, doi: 10.1109/TSMC.2018.2884952.

[48] M. Dawson, R. Bacius, L.B. Gouveia, A. Vassilakos, "Understanding the challenge of cybersecurity in critical infrastructure sectors," *Land Forces Academy Review*, vol. 26, no. 1, pp. 69–75, 2021, doi: 10.2478/raft-2021-0011.

[49] S.S. Baggott, J.R. Santos, "A risk analysis framework for cyber security and critical infrastructure protection of the US electric power grid," *Risk Analysis*, vol. 40, no. 9, pp. 1744–1761, 2020, doi: 10.1111/risa.13511.

[50] Stoyanov, Evstatiev, Iliev, *Analysis of the cybersecurity threats in smart grid*. IEEE, 2018.

[51] S. K. Venkatachary, J. Prasad, and R. Samikannu, "Cybersecurity and cyber terrorism in the energy sector: A review," *J. Cyber Secur. Technol.*, vol. 2, no. 3–4, pp. 111–130, 2018, doi: 10.1080/23742917.2018.1518057.

[52] T.R. Vance, A. Vance, "Cybersecurity in the blockchain era: A survey on examining critical infrastructure protection with blockchain-based technology," in *2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology (PIC S & T) 2019. Proceedings of the IEEE*, Corpus ID 215738455, pp. 107–112, 2019, doi: 10.1109/PICST47496.2019.9061242.

[53] A. Vernotte, M. Välja, M. Korman, G. Björkman, M. Ekstedt, R. Lagerström, "Load balancing of renewable energy: A cyber security analysis," *Energy Informatics*, vol. 1, article no. 5, 2018, doi: 10.1186/s42162-018-0010-x.

[54] T. Krause, R. Ernst, B. Klaer, I. Hacker, M. Henze, "Cybersecurity in power grids: Challenges and opportunities," *Sensors*, vol. 21, no. 18, 2021, doi: 10.3390/s21186225.

[55] M. Alkhalifa, M. Aljaafari, S. Muzafar, "Top 5 deadly cybersecurity threats to Kingdom of Saudi Arabia," *Preprints*, 2024, doi: 10.20944/preprints202408.2244.v1.

[56] A. Akkad, G. Wills, A. Rezazadeh, "An information security model for an IoT-enabled smart grid in the Saudi energy sector," *Computers and Electrical Engineering*, vol. 105, p. 108491, 2023, doi: 10.1016/j.compeleceng.2022.108491.

[57] D,E. Ekechukwu, P. Simpa, "The future of cybersecurity in renewable energy systems: A review, identifying challenges and proposing strategic solutions," *Computer Science & IT Research Journal*, vol. 5, no. 6, pp. 1265–1299, 2024, doi: 10.51594/csitrj.v5i6.1197.

[58] Z. Aydın, "Detecting cybersecurity threats in digital energy systems using deep learning for imbalanced datasets," *International Journal of Energy Economics and Policy*, vol. 15, no. 3, pp. 614–628, 2025, doi: 10.32479/ijeep.19649.

[59] N. Tatipatri, S.L. Arun, "A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, cyber security," *IEEE Access*, vol. 12, pp. 18147–18167, 2024, doi: 10.1109/ACCESS.2024.3361039.

[60] O.D. Dovhan, T.Yu Tkachuk, A.V. Tarasiuk, "Counter forensics as a threat to the information security of Ukraine: The problem of forensic expertise of digital evidence in the realities of war," *Uzhhorod National University Herald. Series: Law*, vol. 2, no. 89, pp. 402–409, 2025, doi: 10.24144/2307-3322.2025.89.2.61.

[61] N.K. Singh, V. Mahajan, "Analysis and evaluation of cyber-attack impact on critical power system infrastructure," *Smart Science*, vol. 9, no. 1, pp. 1–13, 2021, doi: 10.1080/23080477.2020.1861502.

[62] S.K. Venkatachary, A. Alagappan, L.J.B. Andrews, "Cybersecurity challenges in energy sector (virtual power plants) – Can edge computing principles be applied to enhance security?," *Energy Informatics*, vol. 4, no. 1, 2021, doi: 10.1186/s42162-021-00139-7.

[63] D. Ghelani, "Cyber security in smart grids: Threats and possible solutions," preprint, 2022.

[64] A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, K. Salonitis, "Predicting cybersecurity threats in critical infrastructure for industry 4.0: A proactive approach based on attacker motivations," *Sensors*, vol. 23, no. 9, 2023, doi: 10.3390/s23094539.

[65] J. Ding, A. Qammar, Z. Zhang, A. Karim, H. Ning, "Cyber threats to smart grids: Review, taxonomy, potential solutions, future directions," *Energies*, vol. 15, no. 18, pp. 6799, Sep. 2022, doi: 10.3390/en15186799.

[66] R. Leszczyna, "Standards with cybersecurity controls for smart grid – A systematic analysis," *International Journal of Communication Systems*, vol. 32, no. 6, pp, e3910, 2019, doi: 10.1002/dac.3910.

[67] Z. El Mrabet, N. Kaabouch, H. El Ghazi, H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers and Electrical Engineering*, vol. 67, pp. 469–482, 2018, doi: 10.1016/j.compeleceng.2018.01.015.

[68] D.C. Smith, "Cybersecurity in the energy sector: Are we really prepared?," vol. 39, no. 3, pp. 265–270, 2021, doi: 10.1080/02646811.2021.1943935.

[69] M. Boeding, K. Boswell, M. Hempel, H. Sharif, J. Lopez, K. Perumalla, "Survey of cybersecurity governance, threats, and countermeasures for the power grid," *Energies*, vol. 15, no. 22, pp. 8692, 2022, doi: 10.3390/en15228692.

[70] O. Ajayi, C. Alozie, O. Abieba, "Enhancing cybersecurity in energy infrastructure: Strategies for safeguarding critical systems in the digital age," *Trends in Renewable Energy*, vol. 11, no. 2, pp. 201–212, 2025, doi: 10.17737/tre.2025.11.2.00192.

[71] T.D. Le, M. Ge, A. Anwar, S.W. Loke, R. Beuran, et al., "Grid attack analyzer: A cyber attack analysis framework for smart grids," *Sensors*, vol. 22, no. 13, p. 4795, 2022, doi: 10.3390/s22134795.

[72] F. Mohammadi, "Emerging challenges in smart grid cybersecurity enhancement: A review," *Energies*, vol. 14, article no. 1380, 2021, doi: 10.3390/en14051380.

[73] A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, K. Salonitis, "Predicting cybersecurity threats in critical infrastructure for Industry 4.0: A proactive approach based on attacker motivations," *Sensors*, vol. 23, no. 9, p. 4539, 2023, doi: 10.3390/s23094539.

Appendix

Table S1. Systematic literature review of primary literature.

No.	Title	Citations	Year	Authors	Focus area	Cyber threats (Q1)	Vulnerabilities (Q2)
1.	A comprehensive review of recent advances in Smart Grids: A sustainable future with renewable energy resources	[38]	2020	I. Alotaibi, M.A. Abido, M. Khalid, A.V. Savkin	Renewable energy	Malware, unauthorised access	Insufficient strategy, protocol gaps
2.	A comprehensive review on cyber-attacks in power systems: impact analysis, detection, and cyber security	[59]	2024	N. Tatipatri, S.L. Arun	Power systems	SCADA-targeted attacks	Protocol vulnerabilities (e.g., Modbus, DNP3)
3.	A review of standards with cybersecurity requirements for Smart Grid	[41]	2018	R. Leszczyna	Standards in Smart Grid	Injection attacks, sniffing	Standard gap in cybersecurity specs.
4.	A risk analysis framework for cyber security and critical infrastructure protection of the US Electric Power Grid	[49]	2020	S.S. Baggott, J.R. Santos	Risk analysis	Multi-stage attacks, APTs	Risk not quantitatively integrated in planning
5.	A security review of local government using NIST CSF: a case study	[42]	2018	A. Ibrahim, C. Valli, I. McAteer, J. Chaudhry	Framework	Generalised threats	Gaps in NIST CSF adoption
6.	A survey on security communication and control for Smart Grids under malicious cyber-attacks	[47]	2019	C. Peng, H. Sun, M. Yang, Y.L. Wang	Smart Grid communication	Packet injection, sniffing	Poor encryption, network vulnerabilities
7.	Analysis and evaluation of cyber-attack impact on critical power system infrastructure	[61]	2021	N.K. Singh, V. Mahajan	Power systems	Coordinated cyber-physical attacks	Weak control systems
8.	Analysis of the cybersecurity threats in Smart Grid	[50]	2018	Stoyanov, Evstatiev, Iliev	Design	Hardware-based vulnerabilities	Poor chip-level protections

9.	Analysing defence strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources	[8]	2024	Adebimpe B. Ige, Eseoghene Kupa, Oluwatosin Ilori	Renewable energy Green buildings	Cyber-physical system threats Targeted system breach, control hijacking	Lack of resilience strategies Weak IoT integration, outdated firmware
10.	Analysing the impact of cybersecurity on monitoring and control systems in the energy sector	[36]	2022	M. Alghassab	Monitoring; control systems	Targeted ICS attacks	Weak authentication, system misconfigurations
11.	Cyber security challenges for IoT-based Smart Grid networks	[39]	2019	K. Kimani, V. Oduol, K. Langat	IoT in energy systems	IoT-targeted threats, botnets	Weak IoT integration, authentication flaws
12.	Cyber security in Smart Grids, threats, and possible solutions	[63]	2022	D. Ghelani	Cybersecurity overview	General threats, evolving malware	Future system adaptation needs
13.	Cyber security of a power grid: State-of-the-art	[7]	2018	C.C. Sun, A. Hahn, C.C. Liu	Power grid	APTs and DDoS	Legacy systems, poor segmentation
14.	Cyber threats to Smart Grids: Review, taxonomy, potential solutions, and future directions	[65]	2022	J. Ding, A. Qammar, Z. Zhang, A. Karim, H. Ning	Smart grids	Malware, DoS, data breaches	Lack of encryption, insecure protocols
15.	Cyberattacks to critical energy infrastructure and management issues: Overview of selected cases	[5]	2020	T. Plėta, M. Tvaronavičienė, S. Della Casa, K. Agafonov	Case studies	Stuxnet-like malware, data manipulation	SCADA system exposure
16.	Cybersecurity in Smart Grid: Survey and challenges	[67]	2018	Z. El Mrabet, N. Kaabouch, H. El Ghazi, H. El Ghazi	Smart grid	Eavesdropping, denial-of-service	Insecure protocols, poor encryption
17.	Cybersecurity on Smart Grid: Threats and potential solutions	[45]	2020	M.Z. Gunduz, R. Das	Smart grid	Spoofing, Sybil attacks, data falsification	Insecure communication protocols

(*continues*)

Table S1. Continued.

No.	Title	Citations	Year	Authors	Focus area	Cyber threats (Q1)	Vulnerabilities (Q2)
18.	Cybersecurity – A permanent challenge for the energy sector	[9]	2023	I.-E. Ene, D. Savu	Energy sector	Botnets, ransomware	Inadequate endpoint protection
19.	Cybersecurity and cyber terrorism - in energy sector – a review	[10]	2018	S.K. Venkatachary, J. Prasad, R. Samikannu	Cyber terrorism	Nation-state attacks	Interconnected system exposure
20.	Cybersecurity challenges in energy sector (virtual power plants) – can edge computing principles be applied to enhance security?	[62]	2021	S.K. Venkatachary, A. Alagappan, L.J.B. Andrews	Edge computing	Insider breaches, unauthorised access	Edge-device vulnerabilities
21.	Cybersecurity in power grids: Challenges and opportunities	[54]	2021	T. Krause, R. Ernst, B. Klaer, I. Hacker, M. Henze	Power grids	Remote access attacks, malware	Third-party software vulnerability
22.	Cybersecurity in the blockchain era: A survey on examining critical infrastructure protection with blockchain-based technology	[52]	2019	T.R. Vance, A. Vance	Blockchain for critical infrastructure	Blockchain hijack, smart contract abuse	Smart contract logic flaws, blockchain integration gaps
23.	Cybersecurity in the energy sector: Are we really prepared?	[68]	2021	D.C. Smith	Preparedness	Cross-site attacks, DDoS	Readiness gaps, legacy software
24.	Detecting cybersecurity threats in digital energy systems using deep learning for imbalanced datasets	[58]	2025	Z. Aydın	Digital energy systems	Imbalanced dataset-based threats	Bias in detection, insufficient training data
25.	Emerging challenges in Smart Grid cybersecurity enhancement: A review	[72]	2021	F. Mohammadi	Smart grid	Eavesdropping, malware	Lack of real-time threat response
26.	Enhancing cybersecurity in energy infrastructure: strategies for safeguarding critical systems in the digital age	[70]	2025	O. Ajayi, C. Alozie, O. Abieba	Energy infrastructure	Digital sabotage, SCADA breach	Insufficient strategy deployment, policy gaps
27.	Grid attacksim: A cyberattack simulation framework for Smart Grids	[46]	2020	T.D. Le, A. Anwar, S.W. Loke, R. Beuran, Y. Tan	Smart grid simulation	Penetration testing results (varied attacks)	Testing exposes weaknesses in grid simulation

28.	Grid attack analyser: A cyberattack analysis framework for Smart Grids	[71]	2022	T.D. Le et al.	Smart Grid analysis tools	Simulation of DoS, MiTM	Poor real-time monitoring capabilities
29.	Identifying cyber insecurities in trustworthy space and energy sector for Smart Grids	[6]	2021	I. Priyadarshini, R. Kumar, R. Sharma, P.K. Singh, S.C. Satapathy	Trustworthy systems	ICS attacks, firmware-level threats	Insecure device firmware
30.	Load balancing of renewable energy: A cyber security analysis	[53]	2018	A. Vernotte, M. Välja, M. Korman, G. Björkman, M. Ekstedt, R. Lagerström	Renewable energy	Interference, overload attacks	Balancing system limitations, sensor vulnerabilities
31.	Predicting cybersecurity threats in critical infrastructure for Industry 4.0: A proactive approach based on attacker motivations	[73]	2023	A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, K. Salonitis	Industry 4.0 infrastructure	Motivation-driven attacks, targeted APTs	Predictive model gaps, attacker profiling challenges
32.	Review of cybersecurity analysis in smart distribution systems and future directions for using unsupervised learning methods for cyber detection	[40]	2023	S.J. Pinto, P. Siano, M. Parente	Smart distribution systems	Anomalous behaviour, zero-day attacks	Lack of unsupervised learning-based detection
33.	Securing the Smart Grid: A comprehensive compilation of intrusion detection and prevention systems	[44]	2019	P.I. Radoglou-Grammatikis, P.G. Sarigiannidis	Smart grid	Intrusion, malware	Insufficient detection, protocol vulnerabilities
34.	Smart Grid cyber-physical attack and defence: A review	[37]	2021	H. Zhang, B. Liu, H. Wu	Smart grid	Cyber-physical attacks, spoofing	Poor segmentation, legacy system exposure
35.	Standards with cybersecurity controls for Smart Grid – A systematic analysis	[66]	2019	R. Leszczyna	Standards in Smart Grid	Misconfiguration, attacks via third parties	Lack of standardised controls
36.	Staying ahead of threats: A review of artificial intelligence (AI) and cyber security in power generation and distribution	[43]	2023	N. Mohamed, A. Oubelaid, S.K. Almazrouei	Power generation; distribution	AI-driven attacks, deepfake intrusion	AI model exploitation, detection lag

(*continues*)

ACIG APPLIED CYBERSECURITY & INTERNET GOVERNANCE

Table S1. Continued.

No.	Title	Citations	Year	Authors	Focus area	Cyber threats (Q1)	Vulnerabilities (Q2)
37.	Survey of cybersecurity governance, threats, and countermeasures for the power grid	[69]	2022	M. Boeding, K. Boswell, M. Hempel, H. Sharif, J. Lopez, K. Perumalla	Governance	Insider threats, remote code injection	Governance policy gaps
38.	The future of cybersecurity in renewable energy systems: A review, identifying challenges and proposing strategic solutions	[57]	2024	D.E. Ekechukwu, P. Simpa	Renewable energy	Man-in-the-middle (MitM), insider threats	Insecure network topology
39.	Understanding the challenge of cybersecurity in critical infrastructure sectors	[48]	2021	M. Dawson, R. Bacius, L.B. Gouveia, A. Vassilakos	Critical infrastructure	Phishing, DDoS, ransomware	Human error, legacy protocols

ACIG APPLIED CYBERSECURITY & INTERNET GOVERNANCE