Assessing Cyber Vulnerabilities and Defence Strategies in Renewable Energy for Critical Sectors

MORAES JOSE, SATYA R SHAH
Engineering Management
Royal Holloway University of London
UNITED KINGDOM

Abstract: - Renewable energy (RE) sources such as wind farms and solar power plants are now widely seen as symbols of optimism and environmental responsibility as the global community tackles climate change. The adoption of digital technology in energy systems, such as smart grids, Internet of Things (IoT), and industrial control systems (ICS), has introduced new risks in terms of cybersecurity. This study investigates the weaknesses of RE infrastructure and emphasizes the pressing requirement for strong cybersecurity measures to safeguard these vital assets. The research focuses on different types of cyber threats that have targeted RE projects, such as ransomware, phishing, distributed denial of service (DDoS), supply chain (SC) attacks. To counter these threats, the study proposes a counter-strategy that includes advanced threat detection, regular updates, secure remote access, and thorough incident response plans. The study also emphasizes the significance of providing training for employees and strengthening security throughout the supply chain to reduce the risks posed by internal threats and mistakes made by humans. The research shows the importance of stakeholders in the RE sector considering cybersecurity as more than just a technical requirement but a crucial strategic decision-making.

Key-Words: - Cybersecurity, Renewable Energy (RE), Supply Chain Security, Defense, Energy Systems, Response Planning, Cyber Risks, Risk Management (RM)

Received: August 19, 2025. Revised: November 9, 2025. Accepted: March 13, 2026. Published: June 10, 2026.

1 Introduction

The use of Renewable Energy (RE) in electricity production, by using wind and solar power, is improving worldwide to greenhouse gases emission and the use of fossil energies. Thus, as the power systems change, the threats skyrocket because of increased interconnectedness and reliance on software and IoT. The following, therefore, are some striking reasons why there is a need for better protection of wind and solar projects supporting important operations. Globally it has committed to increasing renewable energy production (Jayaram, 2024). The EU has set a target to have 42.5% per cent of renewable energy by the year, 2030. Therefore, as more wind farms and solar parks are developed to achieve these targets, the exposed cyber surfaces increase as well. At the same time, digitalisation helps in the monitoring and management of distributed and remote energy assets with the help of sensors incorporated with IoT and industrial control (Jaffe, 2023). Although it allows collaboration more effective, it creates new opportunities for hackers to enter the firm's network. The cyber threats themselves are exemplified in recent occurrences. Sources are also targeting too-well, over a dozen wind farms suffered attempts at cyber intrusion in Germany in 2021 (Dauchy, 2021).

1.1 Research Problem

The protection requirements of medical centres, crisis reaction systems, financial markets, and other highly dependence organisations are still unidentified from the technical side. Features of vulnerabilities that may indicate how they may be expressed in these contexts are unknown, thus the direction of how to introduce the details is uncertain (Aliero, et.al., 2021). The complex cyber threats already depicted against conventional ICSs are issues of concern when it comes to newer energy systems. It is still necessary to discuss how TD practices and OCs might contribute to intrusions or disruptions accidentally (Stoddart, 2022). Evolving attack sophistication defines strategies proven effective formerly may no longer sufficiently address emerging renewable-specific risks to dependent critical services (Rodríguez, 2023). Unlike, energy providers and infrastructure operators currently have limited guidance for systematically assessing cybersecurity risks unique to their renewable energy portfolios and interdependencies (Culler, et.al., 2022).

1.2 Research Aim and Objectives

The study aims to identify and analyse vulnerabilities, threats, and risk mitigation strategies to enhance the cybersecurity posture of RE systems, focusing on Supervisory control and data acquisition (SCADA) vulnerabilities, effective threat detection, incident response plans, and securing remote access against cyber-attacks. On focus on identifying and analysing vulnerabilities and threats unique to renewable energy systems within these vital sectors.

RO1. To identify and analyse vulnerabilities and threats unique to RE systems in vital sectors.

RO2. To interconnected systems and SCADA vulnerabilities impact the cybersecurity posture of renewable energy projects.

RO3. Evaluate threat detection and risk mitigation tailored to wind and solar energy systems.

RO4. To implement comprehensive incident response plans to address cyber threats targeting renewable energy assets.

RO5. To secure remote access play in protecting renewable energy systems from cyber-attacks.

The key **research questions** to be addressed are:

Q1. What are the unique cybersecurity challenges faced by wind and solar infrastructure in critical sectors such as healthcare, finance, government, and critical infrastructure?

Q2. How do interconnected systems and SCADA vulnerabilities impact the cybersecurity posture of RE projects?

Q3. What strategies can be developed for effective threat detection and risk mitigation specifically tailored to wind and solar energy systems?

Q4. How can firms in critical sectors implement comprehensive incident response plans to address cyber threats targeting RE assets?

Q5. What role do SC security and secure remote access play in protecting RE systems from cyber-attacks?

1.3 Rationale and Research Significance

This study aims to advance understanding and strengthened practical definitions against evolving cyber threats targeting wind and solar infrastructure powering critical sectors. As renewable assets increasingly underpin essential national services, protecting their security and resilience was a strategic priority (Franza, et.al., 2022). The elaborate identification of technical vulnerabilities that pertain to these specialised energy environments would offer a very sound foundation for risk evaluation and definition (Haber and Haber, 2020). To apply deeper solutions in parallel with overarching approaches, adjusting strategies tailored to the distinct characteristics of a sector to detect the emergence of new cyber threats before they can disrupt industries was important (Topor, 2024). The recommended steps would assist organisations in identifying their cybersecurity maturity level, which would relate to the organisations' renewable portfolios and contain critical integrated functions (Zheng, et.al., 2022). The research proposal objectives sought to balance the environmental sustainability of buildings with improved security of renewable resources from cyber risks (Taplin, 2020). This research has significant practical implications for increasing the level of security of the renewable energy assets which are vital for the countries' critical infrastructure protection. Given that sector vulnerabilities can first be adequately recognised along with strategies for countering the risks involved in disrupting the sector's stable functioning, the general level of cyber risks can be notably minimised (Kabeyi, et.al., 2022).

As the share of wind and solar energy rises, their protection becomes more critical for public safety and quality of life. The study also has management implications for organisations that oversee crucial renewable energy remote urges (Whittaker, 2024). Recommendations on how to conduct risk analysis and deploy defence measures allow the operators of infrastructures to approach systematically the problem of improving protection against threats (Chairopoulou, 2024). This directly supports the business continuity, protection of company reputations and regulation in areas inherent to their work. In turn, the research helps to fill important gaps in the literature, which hinders thorough risk management (RM) (Council, 2021). The specific issues related to technical aspects in particular operating environments might be deepened to the point of pushing the development of optimal solutions (Duguay, 2020).

2 Literature Studies

This literature review examines some important issues regarding the cybersecurity of RE infrastructure. Technologies like solar panels and wind turbines have become more digitally networked and integrated with industrial control systems, they have become vulnerable to cyber-attacks. The study explores common vulnerabilities in these systems, previous cyber incidents that have already occurred, and strategies that can help bolster defences. The literature reviews SC security challenges and the need for comprehensive incident response planning.

2.1 Cybersecurity in Renewable Energy (RE)

Studies have argued that RE technologies, including solar PV and wind turbines, have expanded over recent years owing to the rise in awareness of climate change and the consequent shift to clean energy worldwide (Hassan, et.al., 2024). Research highlighted renewable infrastructure has increased its relational dependence on digitalization and connection to industrial control systems it has become increasingly exposed to cyber threats (Hou, et.al., 2024; Shah & Kaphantengo, 2025). Research on the cybersecurity challenges of RE has only recently started emerging (Nadir and Ghalib, 2022)

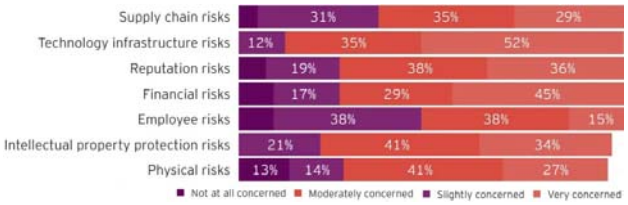

Fig. 1: Cyber Risks in Energy Firms (EY, 2024)

It is evident that many devices deployed in solar PV and wind power systems include active connectivity to the internet via sensors, inverters, and Supervisory Control and Data Acquisition systems, which makes them vulnerable to attackers' exploitation. Notably, there are open and familiar threats affecting device firmware, network, authentication, and security zones in the organization. The renewable portion has long durability but receives less frequent program patches once integrated, allowing adversarial subroutines to reign for years (Liu, et.al., 2024).

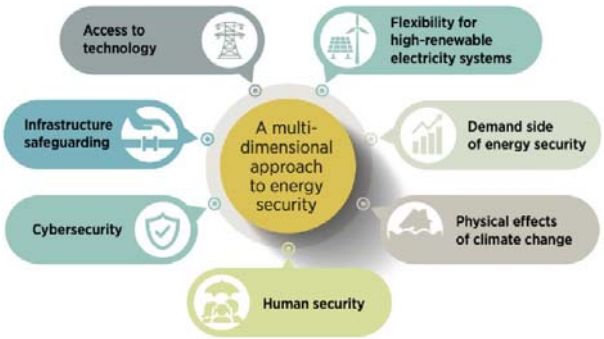

Fig. 2: Multidimensional Approach to Energy Security (PV Mag, 2024)

As stated, with the ongoing addition of renewable energy capacities all over the world, the capacity and intricacy of solar and wind-based projects have also stepped up (Birte & Hannele, 2022). Big solar power stations and wind power plants contain numerous more internet-connected checking points, correspondence systems, and contacts with the electricity network than a rooftop solar panel or small wind generator from the past. This trend towards more extensive and interconnected renewable infrastructure has aggravated cyber threats as the usable attack area increases (Khalaf, et.al., 2024). Some notable cyber incidents involving renewable technologies have already occurred. In 2016, the Ukrainian electricity grid was successfully compromised through industrial control systems, resulting in a blackout. While the origins are still being debated, renewable infrastructure could have represented an initial infiltration point or propagation channel (Vetrivel, et.al., 2023). More directly, the US Department of Energy has reported hacking attempts against wind turbines and other energy control systems (Plėta, et.al., 2020). According to (Henry, 2024) going forward, emerging technologies such as integrated renewable-grid platforms, distributed energy resources, and renewable microgrids are expected to introduce even greater interconnectivity and complexity. Without adequate safeguards, these systems risk becoming highly appealing cyber targets that could endanger public safety and critical national infrastructure functions. Coordinated efforts are now needed to identify vulnerabilities, harden defences, and ensure the continued safe and reliable operation of renewable technologies powering vital sectors into the future (Tawfiq and Abdulaziz, 2024).

2.2 Vulnerabilities in Renewable Energy

Research shows certain common vulnerabilities present across the wind and solar energy infrastructure which threaten to compromise security (Ekechukwu & Simpa, 2024). Studies have highlighted how renewable technologies' increasing use of networked monitoring devices and control systems to optimize performance and integration with transmission grids can introduce new cyber vulnerabilities. Both wind and solar installations widely employ internet-connected sensors, monitoring tools and control systems as identified in academic literature, which seeks to maximize the amount of clean energy fed into national infrastructure networks.

Fig. 3: SCADA Overview (Nixma, 2024)

However, this growing connectivity also exposes these systems to potential cyber threats, according to research exploring the CS challenges of industrial Internet of Things technologies, unfortunately, the security protocols and software powering these internet-connected elements have routinely proven porous (Shah, et.al., 2020). Common vulnerabilities involve outdated encryption algorithms, failure to promptly address known exploits, and lack of adequate authentication measures to restrict unauthorized access to control interfaces (Philip, et.al., 2021). Interconnectivity amplifies the degree of risk, as clever adversaries may infiltrate whole systems by targeting individual points of weakness (Sewall, 2024). Under current setups, any single compromised wind turbine or solar array could potentially be leveraged as a gateway to disrupt surrounding infrastructure through vulnerable industrial control, supervisory control and data acquisition protocols (Nyangon, 2020).

Supervisory control and data acquisition (SCADA) defined as the electronic central nervous system that remotely monitors renewable fleets (Abdelmotaleb & Shrestha, 2023). They are centralised hardware and software platforms ideally used to monitor, control and analyse industrial processes in real time. The convenience of SCADA results in the complication of functions with no fewer than single-point failures. For instance, SCADA master's system that supervises several hundred wind turbines or hundreds of megawatts of solar panels; the successful intrusion into that system could stop the production of energy across large areas using only a single blow. Also, the previous generation of SCADA was developed with no concerns about contemporary security principles and has inherency defects (Loshin, 2021). Implementing retrofit solutions has been difficult while minimizing interference with plant operations and electricity requirements. Today's renewable deployments of the crucial sectors consist of several complex networks with innumerable threats, known and unknown. It is necessary to realise defensive measures that open a systematic approach starting with individual assets at the lowest level and ending at the network level (Huang & Zhu, 2020).

2.3 Cyber Attacks on Renewable Energy

Studies gave an example of the high-level attacks on renewable structures some of which if attacked result in drastic consequential impacts (Aljundi, et.al., 2024). Threats are weaknesses that adversaries leverage and the interruption that can be caused, therefore. Studies noted that hackers were able to penetrate the turbines' control software to manipulate its parameters; for instance, by changing the braking systems and tilting the blades (Barker, 2020). There is a need to consider the cybersecurity risks that emerge as renewable energy technologies become increasingly digitized and integrated within industrial infrastructure (El-Taj, et.al., 2024). As the literature highlights, the growing use of networked control systems within the solar, wind and other renewable installations which feed power directly into national grids introduces vulnerabilities. These systems could potentially be targets for cyber-attacks aimed at disrupting electricity generation or distribution. While renewables offer benefits to the environment, their integration into large-scale energy production means they face challenges comparable to other critical national infrastructure. Therefore, further research is required to fully understand the cyber threats faced and identify appropriate mitigating strategies. This will help ensure renewable resources can reliably support sustainable energy provision long into the future (Shah & Li, 2024). Downtime for repairs represented lost generation and revenue while potentially endangering reliability commitments if outages persisted (Salite, et.al., 2021).

One of the most concerning events consists of the doubts about a cyber-attack on Ukraine's electricity infrastructure in late 2015 (Di Pietro, et.al., 2021). While causality is still unknown, specialists assume distribution management systems could have been initially breached through vulnerable industrial control points, allowing hackers to take over the distribution systems. It is difficult to articulate the exact planning, but it depicted a real-life worst-case approach to a cyber-strike that uses connectivity to cause first-degree physical consequences. Renewable energy systems are cyber-physical, which makes them susceptible (Aslam, et.al., 2024).

Case studies help contextualize cyberattacks targeted towards renewable infrastructure (Sonnenberg, et.al., 2022). The account of a wind turbine hacking altering braking and tilting mechanisms paints a concerning picture of the direct operational impact digital intrusions can achieve. While attribution for infrastructure events may be difficult to determine, the Ukraine blackout example discussed highlights how infiltrating control points initially could facilitate broader distribution takeovers. This indicates the interactive vulnerabilities between physical and networked aspects that adversaries may seek to manipulate (Gaur, et.al., 2023). Further exploration is required to deeply comprehend the full spectrum of threats in this sector. Especially with its rising contributions to electricity systems supporting vital national services

that necessitate robust protections as dependence grows (Mlilo, et.al., 2021).

2.4 Defensive Strategies for RE

Considering vulnerabilities and incidents affecting renewable technologies, the sector has started adopting a range of defensive practices and strategies (Halgamuge, 2024). Implementing a combination of foundational security hygiene alongside innovative protections offers the most rounded approach. All renewable infrastructure owners should ensure prompt patching of known software vulnerabilities, use of strong authentication for access to control interfaces, and segment sensitive networks containing generation and transmission equipment (Sudha, et.al., 2024). Independent security auditing can identify gaps needing attention. International standards like the ISO 27001 framework provide comprehensive blueprint guidance on implementing formal information security management protocols. Beyond the fundamentals, certain technologies hold promises in strengthening network defences (Steingartner, et.al., 2021). Applied correctly as an extra barrier, this can help confine any infiltration. Intrusion detection tools monitoring network traffic for anomalies may detect suspicious connections or Commands sent to equipment for halting before serious harm occurs (Kumar, et.al., 2022).

Addressing vulnerabilities inherited within the equipment itself also requires focus (Gonzalez, et.al., 2023). System designs incorporating 'Security by design' principles inherently build in safeguards rather than bolting them on later. Some turbine and solar panel manufacturers now offer security-featured firmware upgrades designed with today's threats in mind. However, retrofitting millions of existing assets poses difficulties and remains a work in progress (Alabid, et.al., 2022). As renewable infrastructure expands ever deeper into international critical infrastructure domains, coordination between technology providers, owners, and dependent vital sectors grows essential. Information sharing on evolving risks facilitates a collaborative approach to threat management (Dandurand & Serrano, 2013). Defenders require multifaceted solutions encompassing adaptive technologies, learning from past experiences and cooperative strategies suited to RE's diversity to ensure continued resilience in the face of adversary determination (Gautam, 2023).

2.5 Role of Supply Chain Security

The globalized and intricate nature of renewable technology SC introduces further vulnerabilities requiring attention (Nygard, 2024). Components and third parties involved in equipment design, manufacturing, maintenance each represent potential vectors for the introduction of harmful alterations. A single compromised link within vast and opaque sourcing networks could inadvertently undermine industry security (Accenture, 2020). Figure 4 shows categories of SC security (Oracle, 2024). Solar panels, wind turbine blades, key electronic control systems all depend upon geographically distributed production processes (Usman, et.al., 2024).

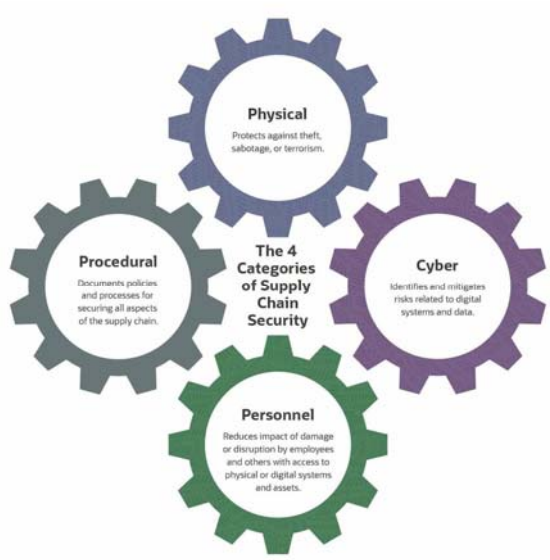

Fig. 4: Categories of SC Security (Oracle, 2024)

During manufacturing, untrusted suppliers either install hidden vulnerabilities or counterfeit authentic products with trojan functionality (Bhunia, et.al., 2014). Supplier relationships also evolve over the lifetime of multi-decade infrastructure assets, introducing continuous oversight challenges (Ratner, 2024). These risks are magnified when third-party maintenance roles because of the remote installation or the specialized nature of the renewable constructions (Meydani, et.al., 2024). Screening the background of temporary employees is challenging, and when many entities are involved in managing responsibilities, there is blurred ownership (Pipelines, 2022). To mitigate these risks, companies must conduct rigorous evaluations of their suppliers through audits, from the sourcing of raw materials to their internal security practices (Ventura, 2021). Legal requirements mandating transparency of security and governance procedures can clarify and manage relationships with high-risk suppliers (Shah & Lim, 2024). Additionally, "security by design" improves procurement regulations, such as: B. cryptographic authentication and tamper-proof design and protection (Udayakumar & Anandan, 2024). Anonymous information sharing platforms can also help industries

quickly identify compromised suppliers and address product security issues (Rantos, et.al., 2020).

2.6 Incident Response Planning

To effectively handle cyber incidents targeting renewable infrastructure when prevention fails, all owners must develop comprehensive response plans (Krause, et.al., 2021). Such strategies require consideration of technologies' unique attributes compared to traditional energy systems. The response also necessitates deep coordination between renewable operators and partners in supporting vital sectors (Abadi, 2023). Rapid incident detection and classification streams follow, with automatic alerts notifying key staff according to severity (Basheer, et.al., 2023). While in-depth analysis deals with the attack mechanisms, as soon as the first issue is contained it focuses on the prevention of the occurrence of similar issues (Kim, et.al., 2022). Feedback on lessons for teaching, learning and informed parenting of defences. Where criminal Behaviour takes place, acquired evidence preservation helps in any subsequent legal action (Tutay, et.al., 2023). Externally, the energy operators and the partner sectors must exchange information concerning potential threats and exercises. Studies conducted virtual exercises to assess the effectiveness of multiple-organisational incident management plans (Randall & Allen, 2021). Cooperative preparation for real occurrence enhances the effectivity of post disaster damage evaluation, critical load reduction and synchronous restoration. The only way in which such ongoing protection of the welfare of the public, which depends on infrastructure, is possible is through collaborative and integrated planning for the responses as well as the involvement of the technology providers and the various sectors (Rathnayaka, et.al., 2022).

Distinguishing characteristics of renewable technologies compared with the conventional grids strongly suggested that interdependencies between renewal technologies and other critical sectors are profound and complex; therefore, response strategies require internal coordination among different project sites and external collaboration between technology suppliers and infrastructure providers (Iweh, et.al., 2022). The literature provides some essentials that such plans should include, to then enable quick identification and categorisation of any events to enable the necessary alert the right personnel instantly. Once issues are on a steady decline, further research is possible to reveal specific tactics, which can be utilised to penetrate the system and avoid such occurrences in the future with lessons learned incorporated to improve defensive measures (Mehta, et.al., 2023). In cases where the participants engage in criminal conduct, then it is possible the evidence gathered form the digital artifacts will be useful to the legal processes that follow. Moreover, the exchange of information about new threats and regular, joint exercise training on how to prevent a supply disruption amongst the energy operators and the reliant sectors will be nearly mandatory to validate multi-party management procedures. This can only be achieved when individuals work hard and cooperate with others who can plan properly and ensure resilience and public welfare during adversity which is echoed by studies (Molakeng, 2020).

2.7 Cyber Insurance in Managing Cyber Risks

Since the dangers gradually shift towards the renewable energy infrastructure, thus the literature proves that cyber insurance has emerged as the other recognised RM solution to strengthen the industries (Bennagi, et.al., 2024). In renewable projects where the average online life is over a quarter of a century, insurance coverage helps compensate for deficiencies in conventional risk profiles by offering metrics for network connectivity and third-party and supply chain interactions made possible by digitalisation. The insurers are looking forward to developing bespoke solutions for renewable property that involves foremost the properties of the asset class and the need for response to both short-term and major events such as BI pay-outs for both small events and catastrophic ones (Hofmann, 2021). It also now captures the costs to address security incidents along with the related legal costs of the consequences of regulatory violations. It is stressed that premiums can contain such estimated risks concerning assets' significance, cyber checks, and SC risks' disclosure (Wai, 2022).

The market take-up for cyber insurance relating to renewable power is rising gradually across markets as the owners of these assets realise risks are not limited to property (Eling, et.al., 2023). They also have an option of providing the policyholder risk consulting that will help in strengthening the base security while at the same time helping in minimising the future claim. From the literature, it has been ascertained that there exists a problem regarding how model uncertainties look for new system-like shocks. The policy conditions and exemptions also include appreciation concerning matters as quickly as the evolution of technologies (Shah, et.al., 2024). It is also necessary to introduce cyber insurance premia as it allows renewable project stakeholders to attain reasonable risk distribution for enhancing organisational CS readiness for more goals during projects' life cycles, as well as in the context of the planning and responding to better practices during

project implementation (Svensson-Hoglund, et.al., 2021).

2.8 Literature Gaps

While ongoing research into renewable energy cybersecurity risks and defences has provided valuable insights, significant gaps remain within the existing literature that require addressing (Ghiasi, et.al., 2023). A focused examination of these deficiencies can help prioritize future studies seeking to strengthen understanding and protections for this vital developing sector. The most notable is the lack of in-depth empirical analysis of cyber-physical impacts and how specific technical compromises translate to real-world consequences (Ofte & Katsikas, 2024). Case reports of past breaches describe disruptive outcomes at a high level without a thorough exploration of engineering and operational dynamics. Closing this gap demands detailed forensic post-mortems of notable incidents to elucidate attack pathways and quantify effects across generation, transmission and supported infrastructure domains (Costigan, 2023). Similarly, literature assessing renewable technologies' unique attributes compared to traditional energy systems remains limited. Distinct attributes like remote and distributed deployment, longevity timescales and specialized maintenance processes shape differing vulnerabilities (Blasi, 2020).

Testing and evaluation of industrial equipment also presents a major deficiency (Doh & Wood, 2021). While frameworks exist to 'pressure test' IT systems, renewable component manufacturers currently face no obligations to independently verify suppliers' security claims or rigorously validate designs' resilience through tailored evaluation regimes. Research literature systematically investigating potential product weaknesses is thus sparse. Integration of renewable assets within multi-vendor environments forms another gap (Majumder, et.al., 2023). Interdependence introduces complex interactive risks seldom addressed at a practical technical level. The literature neglects the evaluation of common system interfaces and emergence effects, potentially magnifying individual component issues (Windemer and Cowell, 2021). Focus on the human aspects of cybersecurity represents an overall deficiency across energy sector literature. Organizational processes, personnel risk factors, and human error vulnerabilities intrinsic to industrial cyber-physical systems warrant dedicated research attention regardless of the technological solutions applied (Alvarez-Alvarado, et.al., 2024). A socio-technical research perspective remains largely unexplored to date. Addressing these gaps promises significant rewards for strengthening infrastructure resilience (Attanasio and Battistella, 2023).

2.9 Theoretical Perspective

Richard Clarke and Robert Knake's Theory: Studies shown that nation-states and other actors will continue to perceive cyber operations as a source of strategic competition and conflict (Goldman, 2020). The renewable systems are critical national infrastructure and at times impacted in some serious cases, such as 2015 power outage in Ukraine, people still wonder whether hostile cyber operations impacted the blackout (Maschmeyer, 2021). This is mainly because renewable technologies are increasingly becoming embedded in energy systems of the world's economies and militaries, and therefore, any adversaries may seek to neutralize their opponents using cyber-attacks targeting them. Therefore, the theory which was developed by Clarke and Knake offers a solution to how the geopolitical environment influences state-sponsored threats on renewable systems (Montaña, 2022).

Cyber-Physical Systems: Explaining that renewable technologies incorporate information technologies with operational technologies because of digitalized features (Banales, 2020). The Stuxnet attack revealed that targeting industrial control systems will allow disruption of cyber-kinetic action effects (Stoddart, 2022). This is a perfect definition of cyber-physical systems as components of a cyber and physical network and can be well applied to denote renewable energy assets. Attacks have compelled changes to the settings of wind turbines or even encrypted files essential for the functioning of wind farms (McCarty, et.al., 2023).

Mancur Olson's Collective Action Theory: Challenges in coordinating effective strategic responses due to distributed ownership models and opaque global supply chains involved in renewable technologies (González, & Rendon, 2022). There are current gaps in collective activities such as integration risk assessment, testing of components, and supply chain security management (Emrouznejad & Abbasi, 2023). Furthermore, with renewable systems integrating into consolidated regional electricity networks, adversaries can more efficiently target multiple stakeholders simultaneously, requiring coordinated defensive strategies that collective action theory suggests will be difficult to achieve (Juozaitis, 2021). Considering the cybersecurity challenges facing renewable infrastructure through the lenses of Clarke and Knake's cyber war theory, the cyber-physical systems conceptualization, and Olson's

collective action theory provides a theoretically informed analysis of both the drivers of threats and barriers to developing comprehensive defensive solutions (Craig, 2018). In conclusion, cybersecurity issues facing renewable infrastructure as technologies like solar panels and wind turbines have become more networked. It examines common vulnerabilities, previous cyber incidents, and supply chain risks. Coordination is important for incident response given renewables' integration into consolidated power grids.

3 Research Methodology

This details the research methods used to investigate the unique CS challenges facing renewable energy projects in critical sectors. A mixed methods approach was employed consisting of qualitative and quantitative components. Semi-structured interviews with industry experts explored cyber risk perceptions and defence strategies. An online survey of renewable energy organisations in healthcare, finance and government quantified cyber incident trends and mitigation practices. Case studies of past cyber-attacks supplemented the data. Thematic analysis and descriptive statistics were utilised. The research design aimed to provide comprehensive and actionable insights through methodological triangulation.

3.1 Research Design

A mixed methods research design was adopted to address the objectives. This combined qualitative and quantitative data collection to provide a deeper and more nuanced understanding of the cybersecurity challenges, beyond what a single method could reveal. A concurrent triangulation design was employed where both qualitative and quantitative data were collected and analysed separately, then merged (Jayaram, 2024). Qualitatively, semi-structured interviews and case studies were used. Interviews gathered rich insights from 15 cybersecurity experts on unique risks, defences, and organisational impacts. An interview guide with open-ended questions was developed and aligned to the objectives. Semi-structured interviews were anticipated to take 60 minutes each and conducted face-to-face or remotely using video calls where it was possible. Sources which contained information were reports on incidents provided by cybersecurity companies, technical overviews of the incidents by energy organisations, and press articles in reputable periodicals. The online survey was designed to achieve a 20% response rate from the sample of 100 respondents, the targeted population being professionals from the renewable energy as well as cybersecurity industries of the critical infrastructure sectors. Power analyses estimated the number of interviewees and surveyed people required to sufficiently answer the research question given a desired effect size. The self-reporting bias that exists in survey data could be eliminated by guaranteeing the subjects' anonymity and giving them more open-ended questions where the answers could be expanded upon. Case studies of 5 past cyber incidents targeting renewable infrastructure explored technical vulnerabilities exploited and lessons learned. Quantitatively, an online survey targeted renewable energy organisations in the defined critical sectors. Questions measured cyber incident trends, defence strategies employed, and barriers to resilience using 5-point Likert scales. Organisational demographics helped analyse differences. The survey was piloted with 5 experts and distributed via industry associations to reach a target sample of 20 responses. Data analysis included thematic analysis of interview transcripts and case study reports to identify key themes. Descriptive statistics summarised survey responses, while inferential analysis tested relationships between variables. NVivo and SPSS software supported systematic and rigorous qualitative and quantitative analysis respectively. Bringing both strands together through triangulation validated and reinforced the findings. The concurrent timing allowed each component to inform the other for increasingly meaningful insights. This design empowered comprehensive exploration of research problem from multiple perspectives (Jaffe, 2023).

3.2 Research Approach and Sampling

The research approach employed a deductive methodology to investigate the cybersecurity challenges facing renewable energy projects in critical sectors. An in-depth review of existing literature and industry reports was conducted first to establish the body of knowledge and identify gaps (Dauchy, 2021). This informed the formulation of specific research objectives and questions aimed at addressing the gaps. Based on the objectives and literature, a mixed methods concurrent triangulation research design was developed using qualitative and quantitative data collection methods. The qualitative component involved semi-structured interviews with 15 cybersecurity experts from the energy sector to gather rich insights into unique risks, defences used, and organisational impacts of cyber incidents (Sherman, 2021). Five past cyber incident case studies were also compiled through documentation analysis to provide tangible examples. Meanwhile, a quantitative online survey targeted renewable energy organisations in critical healthcare, finance and government sectors to

quantify cyber incident trends, mitigation practices employed, and barriers to resilience. Ethical approval was obtained from the institutional review board before data collection commenced. Informed consent and confidentiality procedures protected participant identities and responses. Interviews were then conducted following the developed interview guide. At the same time, case study documentation was analysed (Aliero, et.al., 2021). The survey was also distributed using targeted sampling via industry associations. In the data analysis phase, a thematic analysis of interview transcripts and case study reports was conducted to identify key themes. Descriptive statistics summarised survey findings, while regression and correlation tested relationships between variables. Results across the qualitative and quantitative strands were integrated through joint display tables and narratives. Findings were then interpreted based on the initial literature and research questions. Conclusions regarding the research objectives were drawn and recommendations were provided to strengthen industry resilience. Suggestions for future research avenues were also outlined. Rigorous proofreading ensured a robust research process and reporting of high quality (Stoddart, 2022).For the qualitative component, semi-structured interviews were conducted with 15 cybersecurity professionals across various roles and levels of experience within renewable energy organisations. A pilot survey with 5 experts validated question wording and format before full distribution.

3.3 Data Collection & Analysis

Both qualitative and quantitative data were collected to gain a comprehensive understanding of the cybersecurity challenges for renewable energy projects. An interview guide was used consisting of open-ended questions linked to the research objectives. The interviews were scheduled for one hour via video conferencing and with permission, recordings were transcribed for later thematic analysis. Meanwhile, five recent cyber incident case studies involving renewable infrastructure breaches were compiled through an in-depth review of documentation from incident reports, technical analyses and media articles. Quantitative data was collected through an online survey distributed via targeted sampling to renewable energy organisations in critical healthcare, finance and government sectors. The survey questions focused on measuring trends in cyber incidents experienced, defence strategies employed, barriers to resilience, and organisational demographics.. Thematic analysis was used to analyse data from semi-structured interviews and case studies. Transcriptions and documentation were carefully reviewed to develop initial codes summarising key insights. These codes underwent several rounds of refinement as patterns emerged, before sorting into overarching themes (Rodríguez, 2023). NVivo software supported efficient data organisation and coding, responses were exported from the online platform into SPSS for analysis. Descriptive statistics characterised the sample and summarised responses. Frequencies represented trends while measures of central tendency captured average agreement levels with statements.

4 Results and Discussions

This chapter synthesises quantitative and qualitative outcomes with prior research, allowing us to discuss the studied phenomena in detail. The findings are then expounded, and interesting trends and analysis patterns are extracted from the data gathered to meet the aim and objectives. On the other hand, the quantitative data provided the consistency of the results and qualitative results summarised the link of the research question with existing literature.

4.1 Quantitative Results

The chart utilises different colours to illustrate the ratio of the visitors' responses. **Figure 5** shows research's basic findings regarding role distribution among 22 respondents.

Fig. 5: Q2: Role in the Organisation

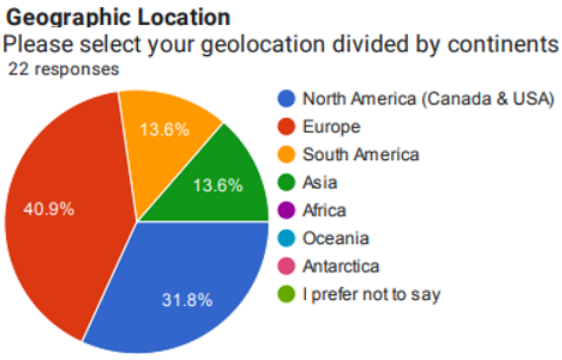

Fig. 6: Q3 Result: Geographical Location

There are 13 subfields for every role (IT Security Specialist, Project Manager), indicating a percentage of 13.6 for each field, whereas 9.1% indicated Cyber Security Consultant and Cyber Security Manager. **Figure 6** provides the geographic distribution of the 22 respondents by continent. The highest is with Europe, which accounted for 40 per cent. 7%, Europe at 40.9%, Asia at 28%, and North America at 31.8%. Asia and South America each make up 13.6%. The chart reveals a good geographical distribution among the world's population in the sample of respondents. **Figure 7** shows the distribution of the respondents within different sectors, which are considered the most critical in the region. It revealed that the Energy Infrastructure Services sector as most prominent sector among the respondents (63.6% working).

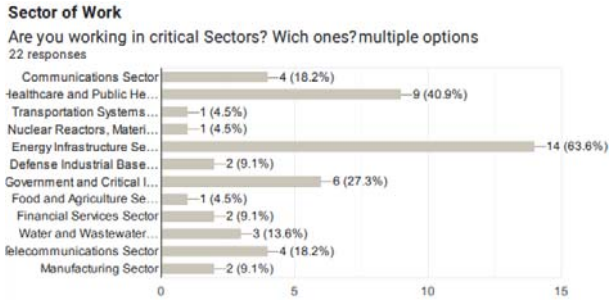

Fig. 7: Q3 Results – Work Sectors

Healthcare and Public Health come second with 40.9% of the respondent population. The government and critical infrastructure sector accounts for 27.3%, and the communications and telecommunications sector accounts for 18.2% each.

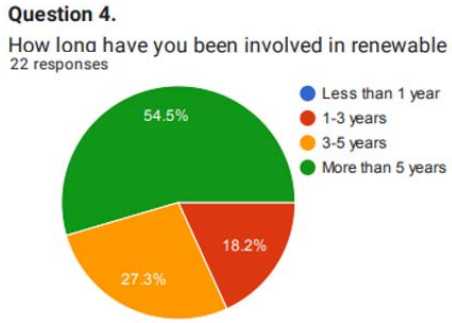

Fig. 8: Q4 Results – Involved in Renewable Energy

Other sectors, though, are also present, albeit not as popular as IT; water and wastewater have a 13.6% share, and financial services have 9.1%. This diversified spread suggests that the respondents are in multiple sectors crucial to the economy's functioning. **Figure 8** summarises the responses of 22 respondents who were asked questions related to their experience of involvement in renewable energy projects and the length of time it takes them. 54.5% of those involved, have done for 5+ years; 27.3% have experience ranging from 3-5 years, 18.2% have experience of 1-3 years.

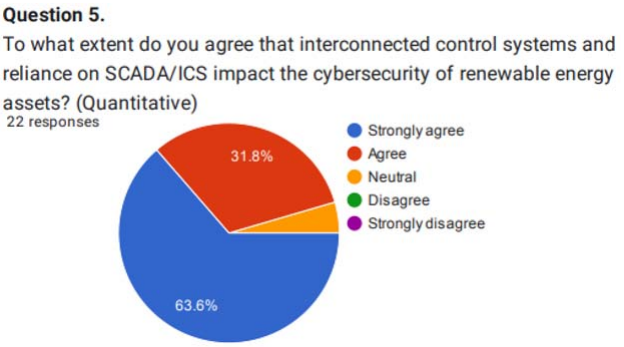

Fig. 9: Q6 Result – Impacts to Cybersecurity

According to the survey results presented (**figure 9**), as many as 63.6% of the interviewees strongly agree with the relationship between the integrated control systems and the dependence on SCADA/ICS regarding cybersecurity threats for renewable energy assets. 31.8% (agree) and 4.5% (neutral).

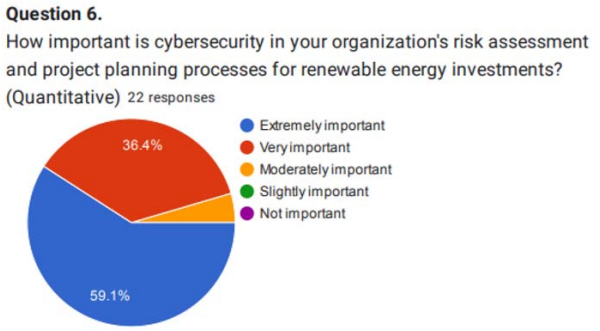

Fig. 10: Q6 Result – Importance of Cybersecurity

There is also no agreeing or strongly agreeing, and there is no disagreeing or strongly disagreeing; hence, the respondents provided overwhelming agreement towards the topical issue. Results (**figure 10)** that 59.1% of participants consider cybersecurity in their organisations very important. Overall, 59.1% of respondents strongly agree that cybersecurity is highly relevant when identifying their organisation's risks and, particularly, when planning investments in renewable energy projects.

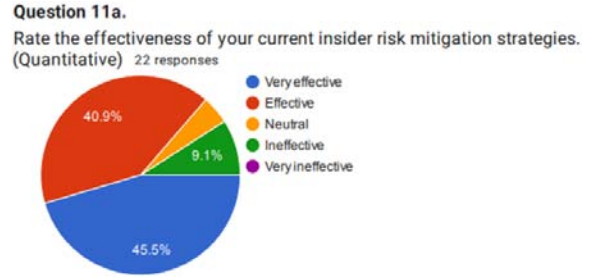

Fig. 11: Q11(a) Results – Effectiveness

Another 36.4% indicated that it is very important and related to cybersecurity; 4.5% rate it as moderate, thus highlighting the central position of cybersecurity in the mentioned processes. Results (**figure 11**) shows that 54.5% of respondents found "Threat detection strategies" to be moderately effective, and 36.4% as very effective. Only 4.5% of the respondents are indifferent to these strategies, and 4.5% claim they do not work. The share of optimistic respondents who believe have efficient measures to detect threats constitutes a relative majority.

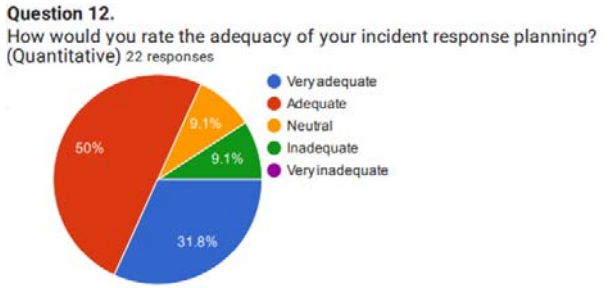

Fig. 12: Q12 Results – Incident Response Planning

As shown in **figure 12**, the responses to the questions are 50% adequate and 31.8% very adequate in terms of planning. Another 9.1% consider it adequate, while another 9.1% consider it inadequate. The worst score was 'very inadequate', which no respondent selected, which gives a positive impression of their confidence in their incident response planning.

Fig. 13: Q14 Results – Current Practices

According to the results (**figure 13)**, 50% of the respondents stated that their organisation usually meets the regulations & standards, 31.8% partially.

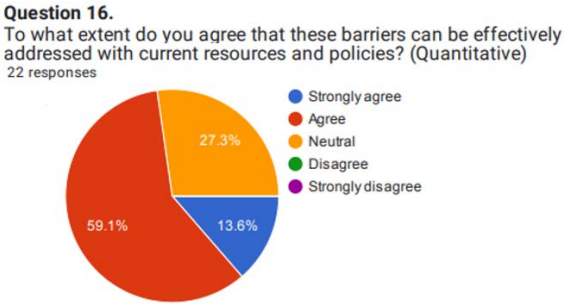

Fig. 14: Q16 Results – Barrier Effects

The rest of the respondents, 13.6%, are partially compliant, while 4.5% are slightly compliant. None of the respondents pointed out non-compliance, meaning that, generally, there is a high level of compliance with regulatory requirements. Results (**figure 14)** reveals that 59.1% of the respondents endorsed that barriers can be dealt with using current resources and policies. While 27.3% are indifferent; 13.6% very much in support. None of the respondents expressed a 'disagree' or 'strongly disagree' attitude, suggesting that most respondents felt sufficient existing resources and policies to tackle barriers.

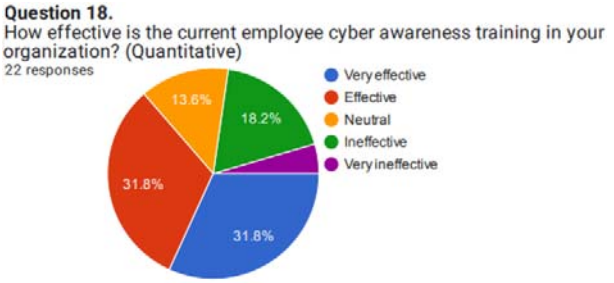

Fig. 15: Q18 Results – Cyber Awareness Training

Results shown in Figure 15 and Figure 31.8% of the respondents said that their organisation's employee cyber awareness training is effective, whereas another 31.8% said that it is very effective. However, 18.2% consider it ineffective, 13.6% are neutral, and 4.5% find it very ineffective. This implies that there are divergent views on the adequacy of training programmes in today's institutions.

4.3 Qualitative Results

Cybersecurity Challenges and Vulnerabilities in Renewable Energy Infrastructure

Some of the most significant cybersecurity issues affecting renewable energy infrastructure are as follows (1) SCADA systems used for operational control remain largely unprotected; (2) integration with 3rd parties introduces numerous susceptibilities to extrusion-like attacks; (3) insufficient attention is paid to cybersecurity awareness among workers, and that

causes numerous inside threats and careless human errors. One respondent suggested:

"The most critical challenges are (1) inadequate security measures for SCADA systems, (2) vulnerabilities in third-party vendor integrations, (3) insufficient cybersecurity training for employees."

Similarly, another participant suggested:

"Lack of standardised cybersecurity policies., Dependence on external consultants for critical cybersecurity functions."

This results in weak protection for cybersecurity due to the absence of standard protection policies across organisations and departments and delays in response times due to dependence on consultants for core functions of an organisation. The aspects linked to the information security issues include evaluations of risks connected with monetary operations and interactions with third parties, as the problems arising in these fields can result in notable losses and breaches. Similarly, another participant stated:

"Cybersecurity is a key consideration, particularly in evaluating the risks associated with financial transactions and third-party interactions."

Cyber-security is crucial and mandatory and entails targeted risk assessments on new projects, comprehensive constant checks, and the evolution of security measures, especially the SCADA/ICS, to seal off potential vulnerabilities in the system and ensure compliance with the industry. Similarly, another participant stated:

"Cybersecurity is a core component, with dedicated risk assessments for all new projects. It involves continuously monitoring and updating security measures, especially for SCADA/ICS systems, to prevent breaches and ensure compliance with industry standards."

Cybersecurity Strategies, RM, and Best Practices

They employ threat identification tools for prompt threat detection, ongoing monitoring of system activity to identify threats, and auditing from time to time to confirm the security of all financial systems. One participant said,

"We employ advanced threat detection platforms, continuous monitoring, and regular audits of all financial systems."

Individuals use multiple layers of security measures, which include independent audits, security threat detection mechanisms and others, that ensure the overall security of their infrastructure as they seek to identify and deal with security threats as and when they are observed. Similarly, one participant claimed,

"We utilise multi-layered security protocols, including regular audits and automated threat detection systems."

They use role-based access controls, and the organisations have developed good remote access policies such as multi-factor authentications for only specified employees to gain access to certain highly secured systems or data. One participant also shared,

"We employ role-based access controls and have established protocols for remote access, including multi-factor authentication."

Behavioural monitoring is the constant capturing and analysis of user behaviour to flag any abnormal behaviour, which could indicate potential insider threats, to help prevent further insider threats, manipulation and unauthorised access, as stated:

"Behavioural Monitoring: Continuous monitoring of user behaviour to detect any deviations from the norm that could indicate an insider threat."

The section analysed research results quantitatively and qualitatively to synthesise the study's results. This approach allowed the procedure of defining general patterns and associations in the data. The qualitative study further developed the topic by employing detailed and descriptive data to give important insight into participants' experiences, beliefs, and reasons. Furthermore, the research has also discovered that new technologies and innovations entail some weaknesses that need to be discovered and fixed when the technologies and innovations are being implemented.

5 Discussions

The discussion section compares these findings with the research objectives and theoretical underpinnings and how findings support the literature and theoretical frameworks.

5.1 CS Challenges and Vulnerabilities in RE

The study noted that protecting renewable energy infrastructures from cyber risks has become relevant since green energy systems are popular. The change from fossil fuels to clean power like solar, wind, and hydroelectric power comes with new cyberspace threats and vulnerabilities that must be dealt with effectively if power delivery is safe and efficient. The two are the large number of entries points that IoTs, and smart grid networks offer and the challenge of controlling such entry points (Dienna, et.al., 2021). Solar energy systems, for example, consist of several

devices, including sensors, controllers, and interaction complexities, that are integrated to enhance the performance of the energy systems and monitor the occurrence of events. However, the research also established that despite the efficiency, it is appreciated that the ability to transfer information from one business area to another in a proactive and real-time manner offers so many points that harbour entries for criminals in the cyber world. Similarly, studies have shown that these devices might be vulnerable to hacker attacks if the security is unsound or if the equipment involved is old-fashioned (Riggs, et.al., 2023). For example, a 'hacked' sensor might feed the operational team bad information, leading them to make undesirable decisions, including calling for power off or damaging equipment. The other major weakness established from the research findings is that most renewable energy facilities involve the installation of remote access and control systems. Several current world renewable-powered electrical installations incorporate remote control and monitoring equipment to execute equipment control from a distance. Further, another capability is increased adaptability and operating effectiveness (Faquir, et al., 2021); however, this capability is linked to certain dangers if online login credentials are inadequately protected. Any malicious user who gains access to these systems can manipulate or delete certain sections, hence bringing about blackouts or destructions.

The research also highlights that these risks mean wherever remote access is permitted, strong authentication mechanisms and encryption algorithms are a necessity, but the implementation of such security mechanisms may turn out to be extremely costly. Similarly (Alotaibi, et al., 2020) also pointed out that integrating RE sources into the existing power system also brings an extra dimension to cybersecurity challenges. The original centralised grids used by electrical utilities were not designed to be highly secure, and their extension to incorporate new renewable distributed services only complicates the matter further. Furthermore, the research has also discussed that most renewable energy systems are off-grid or not fully integrated with the main network, and as such, it is challenging to protect all the components and substations. Moreover, (Tang, et.al., 2023) found that the modern prosumer is in touch with distributed generation and available for electrical grid use, thus making it possible to have a significantly higher number of interfaces points that hackers can penetrate easily. Certain new challenges have been the growth of larger and more diverse grids, besides CS, which needs better monitoring systems and integrated response measures. Another CS issue concerns the fast and continuous advancement of renewable energy technologies. For example, applying AI and ML in smart management systems in the energy sector raises efficiency and creates additional risks if protected. Managing technological change and ensuring security measures are up to date among main concerns of energy providers (Zografopoulos, et.al., 2023).

The research has also highlighted that legal factors also affect cybersecurity threats and risks since compliance is a significant problem at the company. The rules related to cybersecurity in the energy sector are evolving, and there can be discrepancies in the expectations of a region and a country. Studies (Tufail, et.al., 2021) also identified that stakeholders in the energy field face many codes, regulations, standards, and practices; it takes much work to align all the policies. Weak protective legislation may provide some loopholes for attackers to launch attacks. Improving the cybersecurity of renewable energy appliances requires improving and unifying regulations in the mentioned field (Krause et al., 2021). Additionally, the research has underlined that the social dimension is crucial in organisations' cybersecurity threats.

Moreover, poor training and awareness may lead to a high risk of disclosing secrets to unauthorised people or having weak passwords without their knowledge (Plėta, et.al., 2020). The research also discussed that to avoid such dangers; it is necessary to guarantee that every worker involved in renewable energy activities knows information protection measures. Security awareness programs, training sessions, and periodic exercises assist in reminding personnel of security issues, communicating current threats, and recommending security measures to them. (Venkatachary, et.al., 2020) also found that outsourced equipment and services bring more cybersecurity risks to the organisation. Many Performance Evaluation Reports (PER) require purchasing components, software, and services from different vendors, and their security policies may be distinct.

Holes in any of these third-party systems are disastrous since they cause vulnerability in the general framework. Hence, the research has highlighted that valid systems assessments and insurance that the vendors stick to high levels of security are effective procedures for minimising such risks. In addition, the research has discussed that the adversity and weak linkages associated with CS in renewable energy facilities are complex and comprise various aspects including the prevention form ransomware and any phishing attacks. Previous studies also identified that including the number of newly connected IoT devices, smart grid applications, contractors and third parties,

remote access, integration of renewable energy systems into traditional grids, the growing rate of technology innovation, legal and regulatory challenges, people-related risks, and third-party risks are covering the area of cybersecurity (Djenna, et.al., 2021). The research has highlighted that to overcome these challenges, there must be integrated technological solutions, sound security measures in practice, continuous training, and appropriate changes to relevant legislation. In this way, stakeholders can enhance the dependability of renewable energy sources in the face of changing cyber threats to address the mentioned weaknesses.

5.2 CS Strategies, RM, and Best Practices

The results derived from the research have supported the observations made in the literature review, regarding the significance of cybersecurity policies and RM in the modern context of a highly technological society. Since threats in cyberspace are constantly increasing in terms of their sophistication and incidence, organisations need to apply integrated strategies to protect their digital resources. The place to start any strong cybersecurity policy framework is to describe what that means and what is needed for any organisation (Ogbanufe, et.al., 2021). This encompasses risk assessment, critical asset identification, and developing a security regime that complements organisational objectives (Lee, 2020). The research has also highlighted that an essential component of the strategic approach is formulating an firm's CS policy that defines postholders' expectations, authorities, and procedures for responding to cyber threats.

Therefore, it has been evident from the research that this policy should be backed by governance that should comprise cybersecurity (Benz & Chatterjee, 2020). Another significant component identified from the research is using the technique known as defence-in-depth or multi-tiered security (Fraser, et al., 2021). This approach means employing multiple safeguards to protect information and systems against various threats. In the same way, a multilayered security approach may contain physical security like a firewall, IDS or IPS at the network level, antivirus, encryption at the operating system level, code review, and vulnerability assessment at the application level. Thus, the layered approach makes sense as it allows firms to induce dispersion to various potential threats that can occur and achieve better security resilience. Moreover, the research has also underlined that RM is a key aspect of any CS strategy in any firm.

It entails risk evaluation and ranking processes as much as resources can be adequately channelled towards threatening factors that pose maximum dangers. Similarly, research also identified that RM can be initiated with the risk evaluation procedure, which consists of identifying assets, risks, and threats and assessing the consequences in case of threat implementation and their probability (Benz & Chatterjee, 2020). This assessment assists an organisation in understanding the areas of a business that are most vulnerable and how they are likely to affect it (Lee, 2021). Moreover, the research has also discovered that organisations could formulate a RM plan comprising risk control measures after risk assessment. There are other aspects which need to be incorporated into risk logs like vulnerability, risk rating, threats, and protective measures. Integrating those aspects would help firms consider such risks in a much more effective manner and cover all aspects of CS threats. This should be done to identify the risks that firms should deal with first, according to the extent of their impact and the probability of occurrence. Some management control measures may involve security measures like access control and encryption, and others may include developing responses that prevent incidents and recoveries in case of an incident (Fraser, et.al., 2021). Likewise, the current research has also identified that one reason for a RM plan's regular update is the appearance of new threats or changes in the threat probability. Hence, studies also recommend that organisations incorporate ways by which the systems and networks of an organisation can be continuously scanned for security threats (Alahmari & Duncan, 2020). Further, RM means to display the flow and evolution of security controls and processes. This allows the auditor to recognise areas where specific controls have been substituted or missed and, therefore, guarantee they remain effective all the time. This way, the threat keeps changing, and a strong security plan is always safer for an organisation (Cheng and Wang, 2022).

Moreover, the research has also highlighted that following CS best practices is crucial if one would like to risk being exposed or wanting secureness. The first of these best practices is the requirement of sound access controls in any system. It entails using Multi-factor authentication (MFA) techniques to ensure the user's identity and limit their access to confidential data. MFA makes it even harder for the attacker to penetrate the user's account by insisting on two or more kinds of verification, such as a password and biometric scan or token (Cheng and Wang, 2022). Furthermore, the research found that the second practice includes the principle of least privilege, which should be used so that users get only the access required by their responsibilities in the organisation. Other fundamental matters are also called best practices; they include the regularity of software

updates and the management of software patches (Lee, 2021). Studies found that hackers can easily target likely weak points in software and get unauthorised access or pull off an attack (Alahmari & Duncan, 2020). This means an organisation is safe from being attacked again by a virus or a hacker since all software and systems contain updated security patches. Therefore, the research has discussed that this can be challenging, which is why integrating automated patch management solutions can assist in the proper execution of the process of patch management. Another important practice identified from research findings is the training and awareness undertaken with the employees in the organisation. Employees can often be the weakest link to cyber-security, and as such, should be trained in security risks and methods. Studies shown some topics that must be presented in the training sessions include scams, passwords, and policies (Benz & Chatterjee, 2020). Moreover, the research has also indicated that data encryption is important to enhance data and information security in motion or storage. Encryption is a process that transforms data into unintelligible data, which can only be transformed back into intelligible data using cyphers (Hubbard & Siersen, 2023). Using encryption, firms can protect data in a way that if the data is intercepted or pirated, it cannot be read. Encryption of certain data, including personal or financial information, is a must to ensure that data is safe from breach (Syafrizal, et.al., 2020)

In addition, the research has also discovered that programs should have response and recovery plans tested periodically or immediately when an incident occurs. As much as one may employ strict security measures, there might still be a security incident. An incident response plan defines measures for detecting, reporting, and combating security threats and plans for restoring the systems (Fraser, et.al., 2021). Still, periodic revisions and updates of the plan help adapt it to new threats and risks that may appear. It also reduces organisations' vulnerability should a security breach occur and assists firms in getting back onto their feet in the event of disruptions. It also brings the point closer to firms, pointing out the importance of implementing good CS practices, managing risks, and following industry standards to be safe and protect from threats and risks. Furthermore, the research has also found that firms must establish long-term systematic CS plans, adopt effective RM frameworks, and adhere to secure themes that can ensure better security posture and protect the valuables. This means that firms can be more prepared for the challenges and dynamics of CS threats to the technology and information they own; by making a regular assessment, adaptations can be made to these measures to counter these threats (Shah, et.al., 2024; Lee, 2021).

The section analysed research results quantitatively and qualitatively to synthesise the study's results. This approach allowed the procedure of defining general patterns and associations in the data. Furthermore, the research has also discovered that new technologies and innovations entail some weaknesses that need to be discovered and fixed when the technologies and innovations are being implemented.

6 Conclusions and Future Research

This study investigated the key cybersecurity challenges facing RE infrastructure and evaluated strategies to strengthen protection. Through a mixed methods approach, insights were gained from both quantitative and qualitative data collection and analysis. As the need for sustainable energy increases and technology plays a larger role in overseeing these systems, new risks start to surface. The vulnerabilities stem from the incorporation of industrial control systems (ICS), SCADA systems, and IoT into renewable energy infrastructure. The research emphasizes the importance of these systems in effectively managing energy but also reveals that they have several vulnerabilities that could be exploited by cyber attackers. As countries around the world increase all dedication to reaching renewable energy goals, the risk of cyber threats targeting this sector is also growing. Moreover, the continuous digitization in this field, enabled by IoT for remote monitoring and management, brings forth a mix of possibilities and obstacles. Enhancing operational effectiveness also makes these systems vulnerable to potential cyber threats.

The research highlights important issues, including the absence of thorough protection plans for important sectors as hospitals and banking systems that rely more on sustainable energy sources. It also emphasizes the necessity of efficient response strategies for incidents and the significance of secure remote access to prevent cyber-attacks. Furthermore, it highlights the increasing complexity of cyber-attacks, requiring consistent adjustment and enhancement of cybersecurity protocols. The study recommends a comprehensive cybersecurity strategy that includes strong defence measures, ongoing risk evaluations, and training for employees, based on these discoveries. Emphasizing the significance of creating a robust cybersecurity culture in organizations that oversee renewable energy assets is crucial. Consistently monitoring and updating cybersecurity protocols, along with utilizing advanced

threat detection technology, are essential for preserving a strong renewable energy network.

In general, this study adds to our knowledge of the cybersecurity threats linked to RE ventures and provides practical suggestions for improving their security. The protection of RE sources from cyber threats is crucial for both national security and the safety of the public as they play an increasing role in the global energy supply. With the ongoing growth and digital transformation of the renewable energy industry, it is becoming a more appealing target for cyber threats. Ensuring the security of renewable energy infrastructure involves implementing a variety of strategies, such as strong cybersecurity measures, ongoing employee education, and regular monitoring and updating of security protocols. Some of the **key recommendations** for **future research** derived from the study are:

- Adding renewable sources to traditional centralised systems also was deemed to amplify cyber threats because the older infrastructure does not have enough protection (Aliero, et.al., 2021). There was the recommendation of a multi-faceted approach with special emphasis being placed on increasing the security measures, reinforcing existing systems, and including the check-up on security systems as part of a frequent schedule.
- Network segmentation should split existing technology and renewable innovation until the entire network is updated; additional monitoring tools give some glimpse (Culler, et.al., 2022).
- New Cyber policy and reporting format for renewable sector-specific applications would mean a higher baseline being set across the renewable sector companies.
- Informed scrutiny of new and innovative social engineering and phishing techniques is crucial, fundamentally because insiders were initially involved in most breaches.
- It proposed that learning paths according to role that could be generalised from general threats down to system-specific risks might be an effective way of dealing with it.
- It was if implementation would need super-ordinate leadership commitment, but it was associated with long-term gains in managing business operations and catering to customer requirements (Franza, et.al., 2022).

Declaration of Generative AI and AI-assisted Technologies in the Writing Process

"The author(s) wrote, reviewed and edited the content as needed and She/He/They has/have not utilised artificial intelligence (AI) tools. The author(s) take(s) full responsibility for the content of the publication."

References:

[1] Jayaram, G., 2024. Guardians of the Grid: Enhancing Cybersecurity of Blockchain-Based Renewable Energy Marketplace.

[2] Jaffe, A.M. 2023. US Defence Strategy: forging an industrial orientation towards energy security and foreign policy. In: Handbook on the Geopolitics of the Energy Transition, ed. E. Dauchy, 388-403. Edward Elgar Publishing, November 10.

[3] Dauchy, E., 2021. Cyber Security Management in Energy Supply: Cyber Security Roadmap for Elenia. Available at: https://www.theseus.fi/handle/10024/501180 , [Accessed: 11/Aug/2024]

[4] Aliero, M.S., Qureshi, K.N., Pasha, M.F., Jeon, G. 2021. Smart Home Energy Management Systems in Internet of Things networks for green cities demands and services. Environmental Technology & Innovation, 22, 101443. Doi: https://doi.org/10.1016/j.eti.2021.101443

[5] Stoddart, K. (2022). On Cyberwar: Theorizing Cyberwarfare Through Attacks on Critical Infrastructure—Reality, Potential, and Debates. Springer eBooks, [online] pp.53–146. Doi https://doi.org/10.1007/978-3-030-97299-8_2 .

[6] Stoddart, K. (2022). Cyberwar: Attacking Critical Infrastructure. In: Cyberwarfare: Threats to Critical Infrastructure, ed. E. Dauchy, 147-225. Cham: Springer International Publishing, November 19.

[7] Rodríguez Peña, A.C., 2023. China's role in the global green energy transition: the geopolitical implications of China's dominance over rare metals and green technologies.

[8] Culler, M.J., Welch, J.J., Meng, J.P., Reen, D.W. and Myers, K.S., 2022. Cyber-Risk Management Feasibility Study.

[9] Franza, L., Bianchi, M., Bergamaschi, L. 2022. Geopolitics and Italian foreign policy in the age of renewable energy. Istituto Affari International (IAI).

[10] Haber, M.J. and Haber, M.J., 2020. Industrial control systems (ICS) and Internet

of Things (IoT). Privileged Attack Vectors: Building Effective Cyber-Défense Strategies to Protect Organizations, pp.203-214.

[11] Topor, L. 2024. Secure Cyber Domains (SCD): Mature Models. In: Cyber Sovereignty: International Security, Mass Communication, and the Future of the Internet, ed. E. Dauchy, 133-163. Cham: Springer Nature Switzerland, June 27.

[12] Zheng, T., Liu, M., Puthal, D., Yi, P., Wu, Y., He, X. 2022. Smart grid: Cyber-attacks, critical defence approaches, and digital twin. arXiv preprint arXiv:2205.11783, May 2

[13] Taplin, R. 2020. Cyber risk, intellectual property theft and cyberwarfare: Asia, Europe and the USA. Routledge, November 12.

[14] Kabeyi, M.J., Olanrewaju, O.A. 2022. Sustainable energy transition for renewable and low carbon grid electricity generation and supply. Frontiers in Energy Research 9: 743114, March 24.

[15] Whittaker, D.H. 2024. Building a New Economy: Japan's Digital and Green Transformation. Oxford University Press.

[16] Chairopoulou, S., 2024. Cybersecurity in industrial control systems: a roadmap for fortifying operations (master's thesis, Πανεπιστήμιο Πειραιώς).

[17] Council, A. 2021. The global energy agenda. Report, Washington, DC, January.

[18] Duguay, R. 2020. Small modular reactors and advanced reactor security: Regulatory perspectives on integrating physical and cyber security by design to protect against malicious acts and evolving threats. International Journal of Nuclear Security, 7(1), DoI: https://doi.org/10.7290/ijns070102

[19] Hassan, Q., Viktor, P., Al-Musawi, T. J., Ali, B. M., Algburi, S., Alzoubi, H. M., ... & Jaszczur, M. (2024). The renewable energy role in the global energy Transformations. Renewable Energy Focus, 48, 100545. Doi: https://doi.org/10.1016/j.ref.2024.100545

[20] Hou, J., Hu, C., Lei, S. and Hou, Y. (2024). Cyber resilience of power electronics-enabled power systems: A review. Renewable & sustainable energy reviews, 189, pp.114036. Doi: https://doi.org/10.1016/j.rser.2023.114036

[21] Shah, S., & Kaphantengo, T. (2025). Assessment of the Impact of Digitalisation on Improvement of Downstream Supply Chain Performance. WSEAS Transactions on Business and Economics, 22, 493-515. Article 45. https://doi.org/10.37394/23207.2025.22.45

[22] Nadir, I., Mahmood, H. and Ghalib Asadullah (2022). A taxonomy of IoT firmware security and principal firmware analysis techniques. International journal of critical infrastructure protection, 38, Doi https://doi.org/10.1016/j.ijcip.2022.100552 .

[23] EY. 2024. Cyber Security Risks in Energy Firms. Available: https://www.ey.com/en_au/insights/cybersecurity/how-cyber-security-can-keep-pace-with-the-energy-transition, Accessed: 18/9/2024

[24] Liu, M., Teng, F., Zhang, Z., Ge, P., Sun, M., Deng, R., Cheng, P. and Chen, J. (2024). Enhancing Cyber-Resiliency of DER-Based Smart Grid: A Survey. IEEE Transactions on smart grid, [online] pp.1–1. Doi: https://doi.org/10.1109/tsg.2024.3373008 .

[25] PV Magazine. 2024. Multidimensional Approach to Energy Security, Available: (https://www.pv-magazine.com/2024/05/24/energy-security-in-renewables-based-systems/), Accessed: 20/9/2024

[26] Birte Holst Jørgensen and Hannele Holttinen (2022). IEA Wind TCP Annual Report 2021. Welcome to DTU Research Database. Available at: https://orbit.dtu.dk/en/publications/iea-wind-tcp-annual-report-2021 [Accessed 30 Jul. 2024].

[27] Khalaf, M., Ayad, A., Hossain, M., Kassouf, M. and Deepa Kundur (2024). A Survey on Cyber-Physical Security of Active Distribution Networks in Smart Grids. IEEE Access, pp.1–1. Doi: https://doi.org/10.1109/access.2024.3364362 .

[28] Vetrivel Subramaniam Rajkumar, Alexandru Ştefanov, Alfan Presekal, Palensky, P. and Rueda, L. (2023). Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures. IEEE Access, 11, pp.103154–176. Doi: https://doi.org/10.1109/access.2023.3317695 .

[29] Plėta, T., Tvaronavičienė, M., Della Casa, S., & Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases. Insights into Regional Development, 2(3), 703-715. Available at:

https://cris.mruni.eu/cris/handle/007/17156 [Accessed 11 Jul. 2024] .

[30] Henry, T.J. (2024). Strategic Vulnerabilities of US Offshore Wind Assets: A New US Border Requires a Long-Term Security Plan. [online] Jhu.edu. Available at: https://jscholarship.library.jhu.edu/items/df28c125-0148-45ec-9f16-b62669df087a [Accessed 11 Jul. 2024].

[31] Tawfiq Aljohani and Abdulaziz Almutairi (2024). A comprehensive survey of cyberattacks on EVs: Research domains, attacks, defensive mechanisms, and verification methods. Defence technology. [online] Doi https://doi.org/10.1016/j.dt.2024.06.009

[32] Ekechukwu, D.E., & Simpa, P. (2024). The importance of cybersecurity in protecting renewable energy investment: A strategic analysis of threats and solutions. Engineering Science & Technology Journal, 5(6), 1845-83, Doi https://doi.org/10.51594/estj.v5i6.1186 .

[33] Philip W.T. Pong, Annaswamy, A.M., Kroposki, B., Zhang, Y., Rajagopal, R., Zussman, G., and H. Vincent Poor (2021). Cyber-enabled grids: Shaping future energy systems. Advances in applied energy, [online] 1, pp.100003–100003. Doi: https://doi.org/10.1016/j.adapen.2020.100003.

[34] Sewall, A. (2024). Dumb Devices/Smart Adversaries: Real Threats in Critical Infrastructure. Signals and communication technology, [online] pp.85–111. doi: https://doi.org/10.1007/978-3-031-61117-9_5 .

[35] Nyangon, J. (2020). Smart Energy Frameworks for Smart Cities: The Need for Polycentrism. Springer eBooks, [online] pp.1–33. Doi https://doi.org/10.1007/978-3-030-15145-4_4-2.

[36] Nixma. (2024). What is SCADA. Available from: https://nixma.com/what-is-scada/ , Accessed: 18/7/24

[37] Shah, S., Rutherford, R., & Menon, S. (2020). Emerging technologies of IoT usage in global logistics. In Proc. of Int. Conf. on Computation, Automation and Knowledge Management, ICCAKM 2020 (pp. 251-257). https://doi.org/10.1109/ICCAKM46823.2020.9051530

[38] Abdelmotaleb, M., Shrestha, A. and Suhaila, A. (2023). Digital twin in power system research and development: Principle, scope, and challenges. Openarchive.usn.no. [online] doi https://doi.org/2772-9702 .

[39] Loshin, P. (2021). SCADA (supervisory control and data acquisition). [online] What Is. Available at: https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition [Accessed 11 Jul. 2024].

[40] Huang, L. and Zhu, Q. (2020). A dynamic games approach proactive defence strategies against Advanced Persistent Threats in cyber-physical systems. Computers & Security, [online] 89, pp.101660–101660. Doi: https://doi.org/10.1016/j.cose.2019.101660.

[41] Aljundi, I., Rawashdeh, M., Al-Fayoumi, M., Al-Badarneh, A., & Al-Haija, Q. A. (2023, August). Protecting critical national infrastructures: An overview of cyberattacks and countermeasures. In International conference on WorldS4 (pp. 295-317). Singapore: Springer Nature Singapore.

[42] Barker, N.V. (2020). Development of a Drone-Mounted Wireless Attack Platform. [online] AFIT Scholar. Available at: https://scholar.afit.edu/etd/3224/ [Accessed 11 Jul. 2024].

[43] El-Taj, H., Khoja, A., Kamal, D., Alammari, F., Alkhowaiter, J., Bogari, L., & Essa, R. (2024, December). Renewable energy and cyber threats: safeguarding solar power systems. In 2024 International Jordanian Cybersecurity Conference (IJCC) (pp. 118-123). IEEE. Doi: 10.1109/IJCC64742.2024.10847288.

[44] Shah, S., & Li, R. (2024). An Overview of Energy Conservation and Emission Reduction Policy for Conventional Boiler Power Sector. WSEAS Transactions on Power Systems, 19, 450-474. https://doi.org/10.37394/232016.2024.19.39

[45] Salite, D., Kirshner, J., Cotton, M., Howe, L., Cuamba, B., Feijó, J., & Macome, A. Z. (2021). Electricity access in Mozambique: A critical policy analysis of investment, service reliability and social sustainability. Energy Research & Social Science, 78, 102123. Doi: https://doi.org/10.1016/j.erss.2021.102123 .

[46] Di Pietro, R., Raponi, S., Caprolu, M., Cresci, S. (2021). Critical Infrastructure. In: New Dimensions of Information Warfare. Advances in Information Security, vol 84. Springer, Cham. https://doi.org/10.1007/978-3-030-60618-3_5

[47] Aslam, M. M., Tufail, A., Apong, R. A. A. H. M., De Silva, L. C., & Raza, M. T. (2024). Scrutinizing security in industrial control systems: An architectural vulnerabilities and communication network perspective. IEEE Access, 12, 67537-67573. doi: https://doi.org/10.1109/access.2024.3394848

[48] Sonnenberg, S., Mason, L., Lim, Y. and Reddi, T. (2022). Towards a Human Rights-Based Approach to New and Emerging Technologies: A Framework. [online] Ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4587332 [Accessed 30 Jul. 2024] .

[49] Gaur, V. S., Sharma, V., & McAllister, J. (2023). Abusive adversarial agents and attack strategies in cyber□physical systems. CAAI Transactions on Intelligence Technology, 8(1), 149-165. Doi: https://doi.org/10.1049/cit2.12171

[50] Mlilo, N., Brown, J., & Ahfock, T. (2021). Impact of intermittent renewable energy generation penetration on the power system networks–A review. Technology and Economics of Smart Grids and Sustainable Energy, 6(1), 25. Doi: https://doi.org/10.1007/s40866-021-00123-w

[51] Halgamuge, M.N. (2024). Leveraging Deep Learning to Strengthen the Cyber-Resilience of Renewable Energy Supply Chains: A Survey. IEEE Communications surveys and tutorials [online] pp.1–1. Doi: https://doi.org/10.1109/comst.2024.3365076

[52] Sudha, A., Sudha, C. N., & Shajina, A. (2024). Detecting and mitigating cyber-physical attacks in microgrids to ensure resilient and sustainable communities. In Next-Generation Cyber-Physical Microgrid Systems (pp. 215-231). Elsevier. eBooks, [online] pp.215–231. Doi https://doi.org/10.1016/b978-0-443-22187-3.00009-6

[53] Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat Defence: Cyber deception approach and education for resilience in hybrid threats model. Symmetry, 13(4), 597. Doi: https://doi.org/10.3390/sym13040597 .

[54] Kumar, A., K. Abhishek, M.R. Ghalib, Shankar, A. and Cheng, X. (2022). Intrusion detection and prevention system for an IoT environment. Digital communications and networks, [online] 8(4), pp.540–551. Doi: https://doi.org/10.1016/j.dcan.2022.05.027 .

[55] Gonzalez-Cortes, A., Burlet-Vienney, D., Chinniah, Y., Mosbah, A. B., Bahloul, A., & Ouellet, C. (2023). Development of a context-specific knowledge base for Inherently Safer Design (ISD) in confined spaces: A resource for designers and end users. Process Safety and Environmental Protection, 180, 1076-1093. Doi: https://doi.org/10.1016/j.psep.2023.10.068 .

[56] Alabid, J., Amar Bennadji and Seddiki, M. (2022). A review of the energy retrofit policies and improvements of the UK's existing buildings, challenges and benefits. Renewable & sustainable energy reviews, 159, pp.112161. Doi https://doi.org/10.1016/j.rser.2022.112161 .

[57] Dandurand, L., & Serrano, O. S. (2013, June). Towards improved cyber security information sharing. In 2013 5th international conference on cyber conflict (CYCON 2013) (pp. 1-16). IEEE.

[58] Gautam, M. (2023). Deep Reinforcement Learning for Resilient Power and Energy Systems: Progress, Prospects, and Future Avenues. Electricity, [online] 4(4), pp.336–380. Doi: https://doi.org/10.3390/electricity4040020 .

[59] Nygård, A. (2024). Commissioning and qualification of process equipment for the manufacturing of advanced therapy medicinal products. Doria. Fi. [online] https://www.doria.fi/handle/10024/189679 .

[60] Accenture. (2020). Securing the supply chain: Understanding and mitigating the security risks of modern enterprise supply networks. Accenture. https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-3/pdf/pdf-134/accenture-securing-the-supply-chain.pdf, Accessed: 12/8/24

[61] Oracle 2024. Categories of Supply Chain Security Available: https://www.netsuite.com/portal/resource/articles/erp/supply-chain-security.shtml, Accessed; 20/8/2024.

[62] Usman, F. O., Ani, E. C., Ebirim, W., Montero, D. J. P., Olu-lawal, K. A., & Ninduwezuor-Ehiobu, N. (2024). Integrating renewable energy solutions in the manufacturing industry: challenges and opportunities: a review. Engineering Science & Technology Journal, 5(3), 674-703. Doi: https://doi.org/10.51594/estj.v5i3.865

[63] Bhunia, S., Hsiao, M. S., Banga, M., & Narasimhan, S. (2014). Hardware Trojan attacks: Threat analysis and countermeasures. Proceedings of the IEEE, 102(8), 1229–1247.

https://doi.org/10.1109/JPROC.2014.2339391

[64] Ratner, S. (2024). Espionage, Secrecy, and Institutional Moral Reasoning. Criminal law and philosophy. [online] Doi https://doi.org/10.1007/s11572-024-09718-7.

[65] Meydani, A., Shahinzadeh, H., Ramezani, A., Nafisi, H., & Gharehpetian, G. B. (2024, April). A review and analysis of attack and countermeasure approaches for enhancing smart grid cybersecurity. In 2024 28th international electrical power distribution conference (EPDC) (pp. 1-19). IEEE. Doi https://doi.org/10.1109/epdc62178.2024.10571761

[66] Pipelines 2022. (2022). Pipelines 2022. [online] Doi: https://doi.org/10.1061/9780784484272.

[67] Ventura, L. (2021). Supply chain management and sustainability: the new boundaries of the firm. Uniform law review, [online] 26(3), pp.599–634. Doi: https://doi.org/10.1093/ulr/unab025.

[68] Shah, S., & Ling, M. (2024). An Exploratory Study for Performance Improvement through Supplier Client Services Framework. International Journal of Applied Sciences and Development, 3, 28-56. Article 3. https://doi.org/10.37394/232029.2024.3.4

[69] Udayakumar, P., & Anandan, R. (2024). Develop security strategy for IoT/OT with defender for IoT. In Design and Deploy Microsoft Defender for IoT: Leveraging Cloud-based Analytics and Machine Learning Capabilities (pp. 47-146). Berkeley, CA, Doi: https://doi.org/10.1007/979-8-8688-0239-3_2

[70] Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., & Katos, V. (2020). Interoperability challenges in the cybersecurity information sharing ecosystem. Computers, 9(1), 18. Doi: https://doi.org/10.3390/computers9010018

[71] Krause, T., Ernst, R., Klaer, B., Hacker, I. and Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. Sensors, 21(18), Doi: https://doi.org/10.3390/s21186225 .

[72] Abadi, A. (2023). Energy Transition through Business Model Innovation - Governance, Actors, and Partnerships Polito. [online] DOI https://webthesis.biblio.polito.it/secure/27285/1/tesi.pdf .

[73] Basheer Ahmed, M. I., Zaghdoud, R., Ahmed, M. S., Sendi, R., Alsharif, S., Alabdulkarim, J., ... & Krishnasamy, G. (2023). A real-time computer vision-based approach to detection and classification of traffic incidents. Big data and cognitive computing, 7(1), 22. Doi: https://doi.org/10.3390/bdcc7010022

[74] Kim, S., Park, K.-J. and Lu, C. (2022). A Survey on Network Security for Cyber-Physical Systems: From Threats to Resilient Design. IEEE Communications Surveys and tutorials, [online] 24(3), pp.1534–1573. Doi: https://doi.org/10.1109/comst.2022.3187531 .

[75] Tutay, G. T., Kutanoglu, E., & Hasenbein, J. (2023). Impact of Power Outages Depends on Who Loses It: Equity-Informed Grid Resilience Planning. Research Square, Doi: https://doi.org/10.21203/rs.3.rs-3408250/v1.

[76] Randall, R.G. and Allen, S. (2021). Cybersecurity professionals' information sharing sources and networks in the US electrical power industry. International journal of critical infrastructure protection, 34, pp.100454–100454. Doi https://doi.org/10.1016/j.ijcip.2021.100454.

[77] Rathnayaka, B., Siriwardana, C., Robert, D., Amaratunga, D., & Setunge, S. (2022). Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. International Journal of Disaster Risk Reduction, 78, 103123. Doi https://doi.org/10.1016/j.ijdrr.2022.103123 .

[78] Iweh, C. D., Gyamfi, S., Tanyi, E., & Effah-Donyina, E. (2021). Distributed generation and renewable energy integration into the grid: Prerequisites, push factors, practical options, issues and merits. Energies, 14(17), 5375. Doi: https://doi.org/10.3390/en14175375

[79] Mehta, A.A., Padaria, A.A., Bavisi, DJ., Ukani, V., Thakkar, P., Geddam, R., ... & Abraham, A. (2023). Securing the future: A comprehensive review of security challenges and solutions in advanced driver assistance systems. IEEE Access, 12, 643-678. Doi: https://doi.org/10.1109/access.2023.3347200

[80] Molakeng, M. H. (2020). Workplace adversities and resilience in a group of designated social workers in the Free State. Nwu.ac.za. [online] Doi: https://orcid.org/0000-0003-3855-7712 .

[81] Bennagi, A., AlHousrya, O., Cotfas, D. T., & Cotfas, P. A. (2024). Comprehensive study of the artificial intelligence applied in renewable

energy. Energy Strategy Reviews, 54, 101446. Doi: https://doi.org/10.1016/j.esr.2024.101446 .

[82] Hofmann, (2021). Disaster recovery in urban communities. Uni-muenchen.de. [online] Doi: https://edoc.ub.uni-muenchen.de/29316/1/Hofmann_Sahar.pdf .

[83] Wai, W. (2022). Incentive model for managing cyber risk in the supply chain. fig share. [online] Doi: https://doi.org/10.25949/19444340.v1 .

[84] Eling, M., Kartasheva, A.V. and Ning, D. (2023). The Supply of Cyber Risk Insurance. SSRN Electronic Journal. Doi: https://doi.org/10.2139/ssrn.4497405.

[85] Shah, S., Chen, S., & Naghi Ganji, E. (2024). An Investigative Study to Examine Impact of Digitalisation on Manufacturing Supply Chains. Engineering World, 6, 61-89. Doi: https://doi.org/10.37394/232025.2024.6.8

[86] Svensson-Hoglund, S., Richter, J. L., Maitre-Ekern, E., Russell, J. D., Pihlajarinne, T., & Dalhammar, C. (2021). Barriers, enablers and market governance: A review of the policy landscape for repair of consumer electronics in the EU and the US. Journal of Cleaner Production, 288, 125488. Doi: https://doi.org/10.1016/j.jclepro.2020.125488

[87] Ghiasi, M., Niknam, T., Wang, Z., Mehran Mehrandezh, Dehghani, M. and Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defence mechanisms for improving Security in smart grid energy systems: Past, present and future. Electric power systems research, 215, pp.108975 Doi https://doi.org/10.1016/j.epsr.2022.108975

[88] Ofte, H. J., & Katsikas, S. (2024, June). Paralyzed or compromised: a case study of decisions in cyber-physical systems. In International Conference on Human-Computer Interaction (pp. 134-152). Cham: Springer Nature Switzerland. Doi: https://doi.org/10.1007/978-3-031-61382-1_9

[89] Costigan, S. (2023). Shifting the Boundaries: Conceptual and Practical Challenges of Cybersecurity Education, Definitions and Expectations. [online] Available at: https://pure.port.ac.uk/ws/portalfiles/portal/67986003/

[90] Blasi, D. (2020). Beyond the Hype: A Comparative Case Study of the Impact of Artificial Intelligence and Machine Learning on Cybersecurity. Cuni. CZ. [online] Doi http://hdl.handle.net/20.500.11956/177219.

[91] Doh, J., Budhwar, P., & Wood, G. (2021). Long-term energy transitions and international business: Concepts, theory, methods, and a research agenda. Journal of International Business Studies, 52(5), pp.951–70. DoI: https://doi.org/10.1057/s41267-021-00405-6 .

[92] Majumder, S., Vosughi, A., Mustafa, H. M., Warner, T. E., & Srivastava, A. K. (2023). On the cyber-physical needs of DER-based voltage control/optimization algorithms in active distribution network. IEEE Access, 11, 64397-64429. Doi: https://doi.org/10.1109/access.2023.3278281 .

[93] Windemer, R. and Cowell, R. (2021). Are the impacts of wind energy reversible? Critically reviewing the research literature, the governance challenges and presenting an agenda for social science. Energy research & social science, 79, pp.102162–102162. Doi: https://doi.org/10.1016/j.erss.2021.102162 .

[94] Alvarez-Alvarado, M. S., Apolo-Tinoco, C., Ramirez-Prado, M. J., Alban-Chacón, F. E., Pico, N., Aviles-Cedeno, J., ... & Rengifo, J. (2024). Cyber-physical power systems: A comprehensive review about technologies drivers, standards, and future perspectives. Computers and Electrical Engineering, 116, 109149. Doi https://doi.org/10.1016/j.compeleceng.2024.109149

[95] Attanasio, G., Battistella, C. and Chizzolini, E. (2023). The future of energy management: Results of a Delphi panel applied in the case of ports. Journal of cleaner production, 417, pp.137947–137947. Doi: https://doi.org/10.1016/j.jclepro.2023.137947 .

[96] Goldman, E.O. (2020). From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy (Fall 2020). [online] Utexas.edu. Available at: https://repositories.lib.utexas.edu/items/4036be3c-296e-4e1b-87f3-0df8a6175c4f [Accessed 11 Jul. 2024].

[97] Maschmeyer, L. (2021). The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. International Security, [online] 46(2), pp.51–90. Doi: https://doi.org/10.1162/isec_a_00418 .

[98] Montaña Seisdedos, E. (2022). Cyberattacks: A New Weapon in the Economic Warfare Toolkit? A Study of Russian Cyberattacks on the European Energy Sector in 2022. Cuni. [online] Doi http://hdl.handle.net/20.500.11956/187332 .

[99] Bañales, S. (2020). The enabling impact of digital technologies on distributed energy resources integration. Journal of renewable and sustainable energy, 12(4), Doi: https://doi.org/10.1063/5.0009282 .

[100] McCarty, M., Johnson, J., Richardson, B., Rieger, C., Cooley, R., Gentle, J., ... & Wright, B. (2023). Cybersecurity resilience demonstration for wind energy sites in co-simulation environment. IEEE Access, 11, 15297-15313. Doi: https://doi.org/10.1109/access.2023.3244778

[101] González, DML., & Rendon, J.G. (2022). Opportunities and challenges of mainstreaming distributed energy resources towards the transition to more efficient and resilient energy markets. Renewable and Sustainable Energy Reviews, 157, 112018. Doi: https://doi.org/10.1016/j.rser.2021.112018 .

[102] Emrouznejad, A., Abbasi, S. and Sıcakyüz, C., (2023). Supply Chain Risk Management: A content analysis-based review of existing and emerging topics. Supply chain analytics, 3, pp.100031. Doi: https://doi.org/10.1016/j.sca.2023.100031 .

[103] Juozaitis, J., (2021). Baltic States' Synchronisation with Continental European Network: Navigating the Hybrid Threat Landscape. NATO Energy Security Centre of Excellence Report. Available at: https://vb.lka.lt/object/elaba:114602905/ [Accessed 11 Jul. 2024].

[104] Craig, A. (2018). Realism and Cyber Conflict: Security in the Digital Age. [online] E-International Relations. Available at: https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/ [Accessed 11 Jul. 2024].

[105] Sherman, J. (2021). Cyber Defence across the Ocean Floor. Atlantic Council. Available: https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/, Accessed: 11/6/24

[106] Djenna, A., Harous, S. and Saidouni, D.E., 2021. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), p.4580. Doi: https://doi.org/10.3390/app11104580

[107] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors, 23(8), 4060. Doi: https://doi.org/10.3390/s23084060

[108] Faquir, D., Chouliaras, N., Sofia, V., Olga, K. and Maglaras, L., 2021. Cybersecurity in smart grids, challenges and solutions. AIMS Electronics and Electrical Engineering, 5(1), pp.24-37. DoI: 10.3934/electreng.2021002

[109] Alotaibi, I., Abido, M.A., Khalid, M. and Savkin, A.V., 2020. A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources. Energies, 13(23), p.6269. Doi: https://doi.org/10.3390/en13236269

[110] Tang, D., Fang, Y.P. and Zio, E., 2023. Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber-attacks and online detection methods. Reliability Engineering & System Safety, 235, p.109212. Doi: https://doi.org/10.1016/j.ress.2023.109212

[111] Zografopoulos, I., Hatziargyriou, N. D., & Konstantinou, C. (2023). Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. IEEE Systems Journal, 17(4), 6695-6709. Doi: https://doi.org/10.1109/JSYST.2023.3305757

[112] Tufail, S., Parvez, I., Batool, S. and Sarwat, A., 2021. A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. Energies, 14(18), p.5894. Doi: https://doi.org/10.3390/en14185894

[113] Venkatachary, S.K., Prasad, J., Samikannu, R., Alagappan, A. and Andrews, L.J.B., 2020. Cybersecurity infrastructure challenges in IoT-based virtual power plants. Journal of Statistics and Management Systems, 23(2), pp.263-276.

[114] Ogbanufe, O., Kim, D.J. and Jones, M.C., 2021. Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. Information & management, 58(7), p.103507. Doi: https://doi.org/10.1016/j.im.2021.103507

[115] Lee, I., 2020. Internet of Things (IoT) cybersecurity: Literature review and IoT

cyber risk management. Future internet, 12(9), p.157.
[116] Benz, M. and Chatterjee, D., 2020. Calculated risk? A cybersecurity evaluation tool for SMEs. Business horizons, 63(4), pp.531-540. Doi: https://doi.org/10.1016/j.bushor.2020.03.010
[117] Fraser, J.R., Quail, R. and Simkins, B. eds., 2021. Enterprise risk management: Today's leading research and best practices for tomorrow's executives. John Wiley & Sons.
[118] Lee, I., 2021. Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), pp.659-671.
[119] Alahmari, A. and Duncan, B., (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 international conference on cyber situational awareness, data analytics and assessment, pp. 1-5. IEEE. DoI: 10.1109/CyberSA49311.2020.9139638
[120] Cheng, E.C. and Wang, T., 2022. Institutional strategies for cybersecurity in higher education institutions. Information, 13(4), p.192. DoI: https://doi.org/10.3390/info13040192
[121] Hubbard, D.W. and Seiersen, R., 2023. How to measure anything in cybersecurity risk. John Wiley & Sons.
[122] Syafrizal, M., Selamat, S.R. and Zakaria, N.A., 2020. Analysis of cybersecurity standard and framework components. International Journal of Communication Networks and Information Security, 12(3), pp.417-432.
[123] Shah, S., Kuemmerer, S., & Hasan, S. (2024). Exploring the Role of Industry 4.0 on Global Logistics: Challenges in Big Data and IoT. Journal of Computing and Management Studies, 8(1). https://drive.google.com/file/d/1dpezQkCIm0xomOGVrlD9Ogq1AatC6z3c/view

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed to the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.