Malaysian Journal of Sustainable Environment
Special issue, June (2025), 103-126
doi: 10.24191/myse.v12i2.7072

SWOT ANALYSIS OF CYBERSECURITY VULNERABILITIES AND STRATEGIES IN RENEWABLE ENERGY SYSTEM: A CASE STUDY ON EUROPEAN WIND POWER SYSTEM

Nor Nashrah Azmi[1,2], Fiza Abdul Rahim*[3], Noor Hafizah Hassan[4] & Nur Azfahani Ahmad[5]
***Corresponding Author**
[1,3,4]Faculty of Artificial Intelligence, Universiti Teknologi Malaysia (UTM), Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia.
[2]College of Computing and Informatics, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia
[5]Green Safe Cities (GreSafe) Research Group, Department of Built Environment Studies and Technology, College of Built Environment, Universiti Teknologi Mara, Perak Branch, Malaysia

nornashrah@graduate.utm.my, *fiza.abdulrahim@utm.my, noorhafizah.kl@utm.my, nuraz020@uitm.edu.my
Received: 15 September 2024
Accepted: 09 March 2025
Published: 30 June 2025

ABSTRACT

As smart cities increasingly incorporate renewable energy systems to achieve sustainability objectives, ensuring strong cyber security measures is crucial. The susceptibility of these infrastructures, such as smart grids and solar panels, to diverse cyber threats poses significant risks to energy supply and data integrity. This paper examines cyber resilience in the context of the renewable energy industry, using a SWOT analysis of a European wind energy case study to assess the sector's cybersecurity posture and identify key vulnerabilities. This paper aims to identify the industry's current cyber defense mechanisms and the critical need to protect energy systems from increasingly sophisticated cyber threats that pose operational and safety risks, particularly in smart city infrastructures. The findings highlight the urgent need to bolster existing cyber defenses, develop comprehensive incident response plans, and foster a culture of collaborative information sharing among stakeholders. In the future, the paper suggests researching emergent technologies such as artificial intelligence and machine learning

for real-time threat detection and adaptive cybersecurity in wind energy systems to strengthen adaptive cyber defensive capabilities and investigating quantum computing for its promise of superior encryption security. By addressing these research gaps, this study provides several recommendations for cyber resilience strategies that may be used to strengthen the cyber resilience of renewable energy systems, ensuring a secure and renewable energy supply for smart cities in the future.

Keywords: *Cyber security, Renewable energy, Smart grids, Incident response planning*

INTRODUCTION

Projections indicate that by 2050, 70% of the world's population will reside in urban areas (Konstantinou, 2022). The increasing number of people living in urban areas puts an enormous demand on the resources and infrastructure already in place, demanding innovative strategies for sustainable growth. This challenge has spurred the development of 'smart cities' - urban centres that leverage digital technologies and data-driven approaches to enhance cities' efficiency, sustainability, and liveability.

Increasing urban populations energy demands highlight the need for smart city solutions. Tokyo, a megacity home to nearly 37 million people, anticipates adding an additional 5 million by 2050, placing an enormous burden on its energy infrastructure (Chaisson, 2022). Therefore, cities need to adopt smart energy management strategies to accommodate such development sustainably, and integrate renewable energy systems. Besides, a critical component of smart city infrastructure is the integration of renewable energy systems, such as solar panels, wind turbines, and smart grids, to reduce carbon emissions and achieve environmental goals (Toli & Murtagh, 2020).

For example, consider Copenhagen, which plans to achieve zero carbon emissions by 2025 (Damsø et al., 2017). The city offers an example of how smart grids that can efficiently balance energy supply and demand and renewable energy sources like wind power can be integrated to create a more sustainable urban future. Likewise, Barcelona adoption of smart lamps,

which adjust their brightness according to current conditions, highlights how even small technological improvements can result in significant energy conservation (Paradells et al., 2018).

The rapid dependence on digital infrastructure in the renewable energy sector has proved that new leading sectors will also be at considerable risk from cyber-attacks. One lone cyber-attack can disrupt operations, lead to reputational loss, and cause massive financial losses. In a report, Ponemon Institute (2021) estimated that the average cost of a cyber incident in the energy sector is around $4.65 million (Kiganda, 2022). Moreover, the expenses incurred transcend the immediate recovery expenditures, often including long-term damages that range from investors to regulatory fines. This has shown how vital proactive and robust cybersecurity is to the industry.

However, incorporating these renewable energy systems into the smart city ecosystem introduces new cyber security challenges that must be addressed appropriately. According to recent studies, renewable energy infrastructures, particularly smart grids and other related components, are vulnerable to a range of cyber threats, such as data breaches (Zografopoulos et al., 2021), system disruptions that are caused by various factors , but not limited to natural disasters or human-made errors, and malicious attacks from external sources (Cao et al., 2023).

Although renewable energy has many advantages, knowing the potential consequences of malicious cyber activity targeted at these systems is crucial. For example, an intentionally planned attack on the Supervisory Control and Data Acquisition (SCADA), system of a wind farm could disrupt power production, resulting in blackouts and losses (Ara, 2022). In the same manner, breaching a smart grid communication networks could enable attackers to control the flow of electricity, destroying critical systems or disrupting services (Solar Energy Technologies Office, 2020). This necessitates comprehensive security measures and robust defence mechanisms to safeguard these critical assets.

Several research studies by Alotaibi et al. (2020) and Fursov et al. (2022) emphasize the critical role of cyber security in ensuring the reliable and secure operation of renewable energy systems in smart cities. Both

studies highlighted the increasing frequency and sophistication of cyber threats targeting smart grid infrastructure and underscore the need for ongoing evaluation and enhancement of security measures. Another study by O'Dwyer et al. (2019) delved into the specific security challenges posed by integrating multi-station energy systems, which are central to the functioning of smart cities.

As we explore deeper into the complexities of cyber security in the context of renewable energy systems within smart cities, it becomes evident that a proactive and multi-faceted approach is essential to counter the evolving cyber threats (Saadat et al., 2020). The evolving cyber landscape posed many challenges to the security of smart grids and distributed energy resources. Recent incidents have demonstrated the potential impact of cyber threats on the reliable operation of these systems, with implications for both energy supply and data integrity (Sinha et al., 2021). For instance, the intrusion of a smart grid infrastructure could result in widespread power disruptions, leading to significant economic and social ramifications (Saadat et al., 2020). Similarly, unauthorized access to sensitive data within the renewable energy systems can compromise confidentiality and erode trust in the overall smart city ecosystem (Dhara et al., 2021).

To address these concerns, this paper aims to explore and analyze the various cyber security challenges faced by renewable energy systems within smart cities. By identifying and understanding the vulnerabilities and threats, the objective is to devise effective strategies and recommendations to enhance the security posture of these critical infrastructures. The main purpose of this paper is to provide a comprehensive framework for implementing robust cyber security measures that can mitigate the risks posed by cyber threats and ensure the reliable and secure operation of renewable energy systems in smart cities. Through an in-depth examination of the existing security landscape and the potential ramifications of cyber incidents, this paper seeks to contribute to the ongoing efforts to strengthen the resilience of smart city infrastructure in the face of evolving cyber threats.

This work used SWOT analysis methodology to appraise the present landscape of cybersecurity in renewable energy systems, focusing on recent European wind energy companies that have been the subject of cyberattacks. The SWOT framework helped to systematically understand

both the challenges and the opportunities at hand for securing the infrastructure of renewable energy by critically analyzing existing strengths and vulnerabilities of the security measures. The most important result of this analysis pointed to critical weaknesses in the construction of remote-control systems and identified the need for improvements at an industrial level. Such results are central in the manuscript and point to the urgent need for adequate cybersecurity strategies.

LITERATURE REVIEW

This section investigated 1) current security practices and limitations in renewable energy systems, 2) the vulnerabilities inherent in these advanced energy systems, and 3) the critical importance of safeguarding data integrity, confidentiality, and availability.

Vulnerabilities in Renewable Energy Systems within Smart Cities

Smart grids, which serve as the backbone of smart city infrastructure, are particularly vulnerable to cyber threats due to their reliance on interconnected digital technologies and communication networks. These systems often incorporate a wide range of devices, from smart meters and energy management systems to automated control systems, all of which can be potential entry points for malicious actors (Mrabet et al., 2018; World Energy Council, 2016). Weaknesses in the security protocols governing data transmission, access control, and system monitoring can lead to data breaches, unauthorized control of grid operations, and even widespread power outages.

Smart grids are also susceptible to targeted attacks on critical components, such as the SCADA systems that manage and monitor the grid's operations. Comprising these systems can enable adversaries to disrupt power generation, transmission, and distribution, with cascading effects on the wider smart city infrastructure (Ara, 2022).

These systems are designed to enhance energy efficiency and reliability by employing advanced data communication and control technologies. However, the complexity and interconnectedness that make these systems

so effective also render them vulnerable to significant cyber risks (Kumar et al., 2018). The complex network of devices and communication channels is necessary for the operation of smart grids to create multiple points of potential failure and opportunities for malicious actors to exploit.

In addition, smart grids rely on continuous data exchange to manage and distribute energy effectively. This reliance makes them particularly susceptible to cyber-attacks that can intercept, manipulate, or disrupt data. Such attacks can result in grid instability, leading to power outages or even widespread blackouts (Solar Energy Technologies Office, 2020). Integrating distributed energy resources (DERs), including solar panels and wind turbines, further complicates the security landscape. These systems often depend on Internet of Things (IoT) devices for monitoring and control. While IoT technology enhances the functionality and responsiveness of energy systems, it also introduces additional vulnerabilities. If these IoT devices are not properly secured, attackers can exploit them to gain unauthorized access, potentially disrupting energy distribution and compromising the integrity of the entire energy network (Li et al., 2023).

Threats to Data Integrity, Confidentiality, and Availability

The extensive use of data-driven technologies and communication networks in renewable energy systems within smart cities underscores the critical importance of preserving data integrity, confidentiality, and availability. Cyber threats can compromise these fundamental security principles, leading to significant financial, operational, and reputational consequences for organizations, businesses, and individuals.

Furthermore, cyber-attacks targeting renewable energy systems can take various forms, including data breaches, network intrusions, and malware infections. Such attacks can enable adversaries to gain unauthorized access to sensitive information, manipulate control systems, and disrupt the overall functioning of the energy infrastructure (Ivanova, 2022; Jia et al., 2020). Incidents such as the 2015 cyber-attack on the Ukrainian power grid, which left hundreds of thousands of customers without electricity, demonstrate the potential scale and impact of such breaches (Cao et al., 2023).

Besides, data integrity ensures renewable energy systems are reliable

and efficient operation. However, cyber-attacks that manipulate or falsify data can have severe ramifications, such as causing imbalances in the energy grid, disrupting load management, and triggering instability in the power supply. For example, a hacker could infiltrate the SCADA system of a wind farm, altering sensor readings to make the system appear more or less productive than it is (Sinha et al., 2021). This could result in suboptimal energy generation and distribution, potentially leading to power outages in the smart city.

The confidentiality of sensitive data, such as customer information, grid operations, and energy trading data, is also a crucial concern (Eckhoff & Wagner, 2018; Ismagilova et al., 2022). Such breaches pose significant privacy concerns for consumers and can create competitive risks for energy providers. Unauthorized access to this data can lead to espionage, theft of intellectual property, or other malicious activities that undermine the security and economic stability of the energy sector.

Lastly, the availability of renewable energy systems is paramount to the resilience of smart cities. Moreover, cyber-attacks that disrupt the availability of these systems, such as through denial-of-service attacks, can have cascading effects on the entire smart city infrastructure, leading to widespread power outages and disruptions to critical services (Pour et al., 2017). In addition, distributed denial-of-service (DDoS) attacks, for example, aim to disrupt access to energy management systems by overwhelming them with traffic (Qi et al., 2016). This can result in delays or complete shutdowns of energy services, causing widespread disruptions and potentially endangering public safety.

The critical need for robust cyber security measures is underscored by the diverse threats targeting the vital data that underpins renewable energy systems. Securing this data is essential for operational reliability and trust and confidence in the renewable energy infrastructure. Addressing these challenges requires a comprehensive approach that integrates technical, operational, and organizational strategies to enhance the cyber resilience of renewable energy systems in smart cities.

METHODOLOGY

Research Design and Approach

This study adopted a qualitative approach by analyzing reported cyberattacks on European wind energy companies using secondary data. The analysis utilizes the SWOT matrix to assess the current state of cybersecurity in the renewable energy sector. The research explored industry vulnerabilities and strategic responses based on existing reports and data, which provide in-depth insights into the cybersecurity challenges faced by the sector.

The data for this research were obtained from expert reports, analysis of cybersecurity incidents, and case studies from the industry. These form the basis of the SWOT analysis to be presented within this manuscript. Such insights were integrated into an understanding of not only current instituted security measures but also those of emerging threats. This qualitative framework has been chosen because it allowed the investigation of complex, real-world cybersecurity challenges that cannot easily be quantified but are critical in devising effective strategies.

Data Collection Methods

Data were collected from various sources, ensuring a comprehensive analysis of the subject matter. The primary data sources included documented case studies of notable cyber security incidents involving renewable energy systems. The case study provided real-world examples of vulnerabilities, threats, and responses. In addition, reviews of existing literature, including academic papers, industry reports, and policy documents were conducted to supplement the case study data. This combination of sources ensured a robust dataset that captured the complexity and nuances of cyber security challenges in renewable energy systems.

Analytical Tools and Techniques

The collected data were analyzed using SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats). SWOT analysis is a strategic planning tool that helps identify the internal and external factors which

influence the cyber security posture of renewable energy systems. This structured approach allowed a comprehensive assessment of the strengths and weaknesses of existing cyber security strategies and the opportunities and threats posed by the evolving cyber threat landscape. Table 1 shows the detail description for each of the factors. By systematically evaluating these factors, the research aims to provide a balanced and thorough understanding of the cyber security challenges and potential solutions.

Table 1. SWOT Analysis Framework

Factor	Description
Strengths	Internal attributes of renewable energy systems that contribute to their cyber security robustness
Weaknesses	Internal attributes of renewable energy systems that make them vulnerable to cyber threats
Opportunities	External factors that could enhance the cyber security of renewable energy systems
Threats	External factors that could compromise the cyber security of renewable energy systems

Source: Author (2025)

The SWOT analysis provides a framework for evaluating cybersecurity strategies based on effectiveness, feasibility, and scalability criteria. Additionally, effectiveness measures how well a strategy mitigates identified cybersecurity risks, while, feasibility assesses the practicality of implementing the strategy within existing operational and technological constraints. Next, scalability evaluates whether the strategy can be expanded and adapted to different contexts and scales of operation. By applying this framework, the research aims to provide actionable recommendations for enhancing the cyber security of renewable energy systems.

By adopting this methodological approach, the research ensured a detailed and systematic exploration of cyber security challenges and strategies in renewable energy systems. SWOT analysis provides a structured framework for assessing the internal and external factors that impact cyber security, contributing valuable insights to the field and informing future policy and practice.

Limitations

As with any qualitative research approach utilizing case studies, some inherent limitations and assumptions should be considered. Firstly, the findings from individual case studies may not be broadly generalizable to all renewable energy systems (Miller et al., 2023). Each case study represents a specific context, and while valuable insights can be drawn from them, caution must be exercised in applying them universally.

Additionally, the qualitative method relies on the availability and quality of the case study data (Dahal, 2023). Comprehensive and detailed case studies may be limited in accessibility, leading to potential gaps in the analysis. Moreover, the researchers' subjective interpretation and the potential for biases in selecting and analyzing case studies can influence the findings.

Another inherent assumption is that the identified patterns and conclusions drawn from the case studies accurately reflect the broader cyber security challenges and strategies for renewable energy systems (Pollock, 2020). While valuable insights can be gained, it is crucial to recognize the potential for oversimplification or overlooking certain complexities in the cyber threat landscape.

Furthermore, the qualitative approach assumes that the identified factors, such as strengths, weaknesses, opportunities, and threats, adequately capture the multifaceted nature of cyber security challenges. However, subjective judgments and perspectives may influence the interpretation of these factors and their implications for cyber security strategies, potentially limiting the comprehensiveness of the analysis.

RESULTS AND DISCUSSION

This study investigated one case study employing SWOT analysis to evaluate the cyber security of renewable energy systems. By scrutinizing recent cyber assaults on European wind energy companies, we acquire insights into the susceptibilities of renewable energy infrastructure and the approaches necessary for enhancing its cyber resilience. These case studies

emphasize the critical of robust cyber security measures in safeguarding crucial data and operations that support renewable energy systems' reliability and integrity amidst evolving cyber threats.

While this study underlined the need for strong security measures of renewable systems and gave an idea of several of the major vulnerabilities through a European case study in wind energy cyberattacks, it falls short of offering a comprehensive overview of the main security practices that exist and their limitations. Situating the current state of practice in security, its effectiveness, and related limitations would have put the challenge into a larger perspective. Further analysis would put into perspective what has been proposed in the form of improvements and strategies and, finally, guide more resilient cyber security measures for the sector.

Case Study: European Wind Energy Cyber Attack

In 2022, three European wind energy companies faced a cyberattack that disabled the remote-control systems of approximately 7,800 wind turbines for about a day (Greig, 2022). This attack exposed the weaknesses in digital management systems and the heavy reliance on remote-control technologies in the renewable energy sector. The incident prompted a re-evaluation of real-time monitoring capabilities and the need for comprehensive cyber security protocols. It also highlighted the growing threat landscape for renewable energy assets and the necessity for industry-wide standards and best practices to protect these critical systems.

Strengths

One key strength of the wind energy industry's current cyber security efforts is the implementation of access controls and firewalls, which have helped limit the initial spread of attacks. However, these measures alone are insufficient to address the evolving threat landscape. Regularly updating and auditing these security controls is crucial to ensure they remain effective against new and emerging threats.

As recommended by industry experts, wind energy companies should also implement multi-factor authentication (MFA) to strengthen their access control security further (Fursov et al., 2022). This approach requires users

to provide additional verification beyond a username and password, which can significantly reduce the risk of unauthorized access and help prevent successful cyber-attacks.

In addition, maintaining a comprehensive and continuously evolving cybersecurity protocol is essential for the wind energy industry. By building upon their existing measures, such as access controls and firewalls, and implementing additional security controls like multi-factor authentication, wind energy companies can bolster their defences against the growing threat of cyber attacks (Bai et al., 2020; Fursov et al., 2022).

Weaknesses

The remote-control systems within an organization play a crucial role in facilitating efficient operations; however, the weaknesses identified, such as inadequate security measures, weak password policies, and outdated software, have left these systems vulnerable to potential cyber exploits (Gao, 2015). To address these concerns and enhance the overall security posture, a comprehensive approach is necessary, encompassing the following key recommendations:

•Update and Patch Management

A robust update and patch management strategy is essential to ensure that all remote-control systems are running the latest software versions with the most up-to-date security patches (Ge et al., 2021). This proactive approach not only addresses known vulnerabilities, but also helps mitigate the risk of cyber threats that may exploit outdated software. Additionally, regular review and password policy updates should be implemented to enforce strong, unique passwords across all systems, thereby reducing the likelihood of unauthorized access.

•Segmentation and Isolation

These measures can significantly improve the security of remote-control systems. By isolating these systems from other critical networks, the potential for the spread of an attack is greatly diminished. In addition, network segmentation, which creates secure zones within the network, further reduces the attack surface and enhances the overall security posture (Manson & Anderson, 2019).

•Regular Vulnerability Assessments

Regular vulnerability assessments and penetration testing are crucial to

identify and address potential security gaps in remote-control systems. These assessments, performed by security professionals, can uncover vulnerabilities that may have been overlooked or not yet addressed, enabling the organization to proactively mitigate these risks and strengthen the security of its remote-control infrastructure.

Opportunities

The incident in the renewable energy sector has underscored the critical need for the industry to prioritize cyber security as a crucial component of its digital transformation. To address this challenge, the industry should focus on developing robust security standards, implementing advanced threat detection and response capabilities, and enhancing employee cyber security awareness.

- The renewable energy industry should collaborate with key stakeholders to develop and adopt comprehensive cyber security standards and best practices tailored to the unique requirements of the sector (McIntyre, 2018). By participating in industry forums and working groups, organizations can stay updated on the latest security trends and standards, ensuring their security measures remain effective and up to date.
- Renewable energy companies should invest in advanced threat detection and response technologies, such as Security Information and Event Management (SIEM) systems and Endpoint Detection and Response (EDR) solutions (Rubio et al., 2019). These technologies provide real-time monitoring and analysis, enabling swift detection and response to potential threats and thereby mitigating the impact of cyber-attacks.
- Organizations should implement comprehensive cyber security training programs for employees at all levels, raising awareness about common cyber threats and best practices for mitigating risks. Ensuring that all staff are equipped to recognize and respond to potential attacks is crucial in strengthening the renewable energy industry's overall cyber security posture.

Threats

Renewable energy systems have become increasingly vulnerable to sophisticated cyber-attacks, which can have far-reaching consequences,

including disruptions to power supply, financial losses, and potential safety hazards in smart cities (Syrmakesis et al., 2022). To mitigate these risks, a comprehensive approach to cyber security, encompassing continuous improvement and adaptation, incident response planning, and collaboration and information sharing, is essential.

- Continuous improvement and adaptation are crucial for maintaining effective cyber security measures in an evolving threat landscape. Researchers suggest adopting a proactive approach, continuously reviewing and updating defenses based on the latest intelligence and threat reports to keep pace with emerging cyber threats. Regular drills and simulations can also help ensure stakeholders are prepared to respond effectively during an attack.
- Incident Response Planning (IRP) is another key component of a robust cyber security strategy for renewable energy systems. Developing and maintaining a comprehensive incident response plan that outlines procedures for detecting, responding to, and recovering from cyber incidents is critical. Regular exercises and simulations can help ensure that all stakeholders are ready to implement the plan in the event of a cyber-attack.
- Collaboration and information sharing among industry peers, cyber security experts, and government agencies is essential for addressing the complex and rapidly evolving threats facing renewable energy systems. Joining collaborative forums can enable the exchange of threat intelligence and best practices, empowering organizations to strengthen their defenses (Hussain et al., 2018; Nejabatkhah et al., 2021).

Renewable energy systems are vital to a sustainable future but must be protected from the growing threat of sophisticated cyber-attacks. The good thing is that the renewable energy sector can improve its security outlook and reduce the economic impact caused by these cyber-attacks. According to a report by Accenture (2020), organizations with advanced threat detection and response capabilities reduced the average cyber incident cost by 18% (Teichmann & Boticiu, 2024). Technologies like Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) might promise substantial long-term cost savings, which is very important to ensure competitive advantages and operational efficiency (Κουνταρδάς & Kountardas, 2017). Also, by implementing a multifaceted approach

that emphasizes continuous improvement, incident response planning, and collaboration, stakeholders can enhance the resilience of these critical infrastructure systems and safeguard the transition to a clean energy future. Figure 1 summarizes the analysis and recommendations for European Wind Energy Cyber Attack:

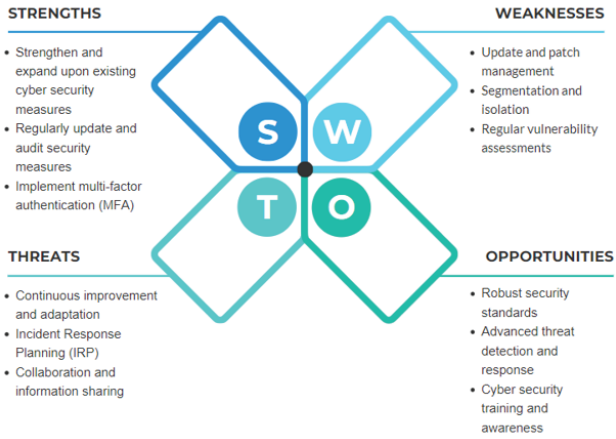

Figure 1. SWOT Analysis Framework for European Wind Energy Cyber Attack

These results show that it requires industry-wide collaboration among its stakeholders. Several past works have demonstrated how effective different industry-wide collaborations can function effectively to mitigate cybersecurity threats. For instance, the Energy Sector Cybersecurity Framework collaboration led by the United States Department of Energy and the Cyber Security Organisation of the European Union provided comprehensive frameworks to share threat intelligence (Florian Skopik, 2017). These enable companies to share information on vulnerabilities, incidents, and best practices in real-time and have remarkably enhanced their response and recovery to cyberattacks.

Collaboration, mainly by participating in established cyber security forums and organizations, will also play a massive role in this strategy. Companies can join platforms like the Global Forum on Cyber Expertise (GFCE) or the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) that facilitate information sharing and build cyber resilience.

These interfaces allow energy companies to share their experiences, learn lessons from past incidents, and adopt best practices to reduce their exposure to cyber threats. These collaborative efforts can help the renewable energy sector develop a more coordinated and proactive cybersecurity posture.

Aside from that, to strengthen the proposed strategies, it is essential to outline a structured approach that includes specific, actionable steps for implementation. For instance, detailing the process for integrating advanced threat detection technologies, establishing comprehensive incident response plans, and fostering industry-wide collaboration will provide clearer guidance for practitioners and stakeholders (Hansen & Hansen, 2018). Such a framework will ensure that the strategies are theoretical but also practical and executable in real-world scenarios.

Future Directions in Renewable Energy Cyber Security

Continuous improvement and adaptation are crucial to stay ahead of evolving cyber threats and ensuring the long-term security of renewable energy systems. In addition, leveraging emerging technologies can significantly enhance cyber security measures, offering innovative solutions to protect and revolutionize the renewable energy sector.

Technologies such as artificial intelligence (AI) and machine learning (ML) can enhance threat detection and response capabilities by analyzing large volumes of data to identify patterns indicative of cyber threats. Quantum computing, though still in its emerging stages, promises to offer unprecedented levels of encryption and security, potentially rendering current cryptographic methods obsolete. Future research should focus on developing and refining these technologies to address specific challenges in renewable energy cyber security. Additionally, exploring the integration of AI and ML with existing security frameworks can provide more adaptive and proactive defense mechanisms.

In the future, the renewable energy sector must continue strengthening cooperation with other industries and government agencies as cyber threats become increasingly complex. These public-private partnerships, for instance, those facilitated by the Cybersecurity and Infrastructure Security Agency (CISA), can serve as models for future partnerships in Europe

and beyond. This will enable the companies to be better prepared against emerging threats and thus provide more robust, unified defenses. It would work out closer relations among industry participants and government regulators.

CONCLUSION

This study has pointed out an essential need for the renewable energy industry, and such a necessity is testified to in the case of the European wind energy cyber-attacks. The study also highlights the necessity for robust cyber resilience strategies within the renewable energy sector, particularly highlighted by the SWOT analysis of European wind energy cybersecurity. While proactive measures, including access controls and firewalls, have been somewhat effective, this paper identifies critical vulnerabilities due to inadequate security protocols for remote-control systems. The conclusion advocates for an iterative improvement process for cyber defenses, rigorous incident response planning, and the benefits of collaborative efforts within the industry to leverage shared knowledge and resources to address these challenges.

This paper would be more substantial if there were a detailed framework or steps that one could take in pursuit of these recommendations. Further work is needed to develop a comprehensive, structured approach, including specific activities to improve cyber resilience. This framework should address advanced technologies for integration, incident response mechanisms, and strategies on how stakeholders can cooperate to ensure the measures proposed are pragmatic and applicable.

The paper further suggests that future security of renewable energy infrastructure demands investment in innovative technologies such as AI and machine learning, which offer sophisticated threat detection and quantum computing for advanced encryption. By embracing these strategies and technologies, the renewable energy sector can significantly enhance its cyber resilience, ensuring reliable and secure energy provision crucial for advancing a sustainable future.

AUTHOR CONTRIBUTIONS

Nor Nashrah Azmi: This author was responsible for gathering relevant data and performing a detailed analysis. She collected information on cyber security incidents, industry standards, and current practices in renewable energy systems. Fiza Abdul Rahim: This author was responsible for the primary conceptualization of the research framework and the overall direction of the paper. She identified the key objectives and scope of the SWOT analysis, focusing on the cyber security evaluation of renewable energy systems in smart cities.Noor Hafizah Hassan: This author, an expert in cyber security, focused on writing and refining the paper's content. She ensures clarity, coherence, and academic rigor in presenting the research findings and proposed strategies.Nur Azfahani Ahmad: This author provided specialized knowledge and insights into the renewable energy industry. She validated the research's technical aspects and contributed expert opinions on the strategies proposed.

CONFLICT OF INTEREST

The authors declared there is no conflict of interest.

REFERENCES

Alotaibi, I., Abido, M. A., Khalid, M., & Savkin, A. V. (2020). A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources. *Energies, 13*(23), 1–41. Retrieved from:https://doi.org/10.3390/en13236269.

Ara, A. (2022). Security in Supervisory Control and Data Acquisition (SCADA) based Industrial Control Systems: Challenges and Solutions. *IOP Conference Series: Earth and Environmental Science, 1026*(1). Retrieved from:https://doi.org/10.1088/1755-1315/1026/1/012030.

Bai, X., Liu, L., Wei, D., & Cao, J. (2020). Research on Security Threat and Evaluation Model of New Energy Plant and Station. *Proceedings - 2020 International Conference on Computer Communication and Network Security, CCNS 2020, 75–80.* Retrieved from: https://doi.org/10.1109/

CCNS50731.2020.00025.

Cao, Y., Li, S., Lv, C., Wang, D., Sun, H., Jiang, J., Meng, F., Xu, L., & Cheng, X. (2023). Towards cyber security for low-carbon transportation: Overview, challenges and future directions. *Renewable and Sustainable Energy Reviews, 183*, 113401. https://doi.org/10.1016/j.rser.2023.113401

Chaisson, E. J. (2022). Energy Budgets of Evolving Nations and Their Growing Cities. *Energies, 15*(21), 8212. Retrieved from: https://doi.org/10.3390/en15218212.

Dahal, N. (2023). Ensuring Quality in Qualitative Research: A Researcher's Reflections. *Qualitative Report, 28*(8), 2298–2317. Retrieved from: https://doi.org/10.46743/2160-3715/2023.6097.

Damsø, T., Kjær, T., & Christensen, T. B. (2017). Implementation of local climate action plans: Copenhagen – Towards a carbon-neutral capital. *Journal of Cleaner Production, 167*, 406–415. Retrieved from: https://doi.org/10.1016/j.jclepro.2017.08.156.

Dhara, S., Shrivastav, A. K., & Sadhu, P. K. (2021). Smart grid modernization: Opportunities and challenges. *In IntechOpen*. https://doi.org/10.5772/intechopen.97892

Eckhoff, D., & Wagner, I. (2018). Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys and Tutorials, 20*(1), 489–516. Retrieved from: https://doi.org/10.1109/COMST.2017.2748998.

Skopik, F. (2017). *Collaborative cyber threat intelligence: Detecting and responding to advanced cyber attacks at the national level*. CRC Press. Retrieved from https://books.google.com.my/books?hl=en&lr=&id=9EQPEAAAQBAJ

Fursov, I., Yamkovyi, K., & Shmatko, O. (2022). Smart Grid and Wind Generators: an Overview of Cyber Threats and Vulnerabilities of Power Supply Networks. *Radioelectronic and Computer Systems, 2022*(4), 50–63. Retrieved from: https://doi.org/10.32620/reks.2022.4.04.

Gao, Y. (2015). Computer remote control system of network security research. In *Proceedings of the 2015 International Conference on Intelligent Transportation, Big Data and Smart City (ICITBS)* (pp. 225–227). IEEE. https://doi.org/10.1109/ICITBS.2015.62

Ge, H., Yue, D., Xie, X., Deng, S., & Dou, C. (2021). A unified modeling of muti-sources cyber-attacks with uncertainties for CPS security control. *Journal of the Franklin Institute, 358*(1), 89–113. Retrieved from:https://doi.org/10.1016/j.jfranklin.2019.01.006.

Greig, J. (2022, April 4). German wind turbine maker shut down after cyberattack. *The Record.* https://therecord.media/german-wind-turbine-maker-shut-down-after-cyberattack

Hussain, S., Meraj, M., Abughalwa, M., & Shikfa, A. (2018). Smart grid cybersecurity: Standards and technical countermeasures. *2018 International Conference on Computer and Applications* (ICCA), 136–140. https://doi.org/10.1109/COMAPP.2018.8460390

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Information Systems Frontiers, 24*(2), 393–414. Retrieved from: https://doi.org/10.1007/s10796-020-10044-1.

Ivanova, A. (2022, April 14). *Deutsche Windtechnik hit by targeted cyberattack*. Renewables Now. https://renewablesnow.com/news/deutsche-windtechnik-hit-by-targeted-cyberattack-778949/

Jia, H., Shao, C., Liu, D., Singh, C., Ding, Y., & Li, Y. (2020). Operating reliability evaluation of power systems with demand-side resources considering cyber malfunctions. *IEEE Access, 8,* 87354–87366. https://doi.org/10.1109/ACCESS.2020.2992636

Kenya Kiganda, in. (2022). *An Assessment of the factors affecting cyber resilience in microfinance institutions* . Retrieved from: http://hdl.handle.net/11071/12982Followthisandadditionalworksat:http://hdl.handle.net/11071/12982

Konstantinou, C. (2022). Toward a Secure and Resilient All-Renewable Energy Grid for Smart Cities. *IEEE Consumer Electronics Magazine, 11*(1), 33–41. Retrieved from: https://doi.org/10.1109/MCE.2021.3055492.

Kumar, V. S., Prasad, J., & Samikannu, R. (2018). A critical review of cyber security and cyber terrorism – threats to critical infrastructure in the energy sector. *International Journal of Critical Infrastructures, 14*(2), 101–119. Retrieved from: https://doi.org/10.1504/IJCIS.2018.091932.

Li, Y., Mandalari, A. M., & Straw, I. (2023). Who let the smart toaster hack the house? An investigation into the security vulnerabilities of consumer IoT devices. In *Proceedings of the 2nd Workshop on Security and Privacy in Connected Embedded Systems (SPICES).* https://doi.org/10.48550/arXiv.2306.0901

Manson, S., & Anderson, D. (2019). Cybersecurity for Protection and Control Systems: An Overview of Proven Design Solutions. *IEEE Industry Applications Magazine, 25*(4), 14–23. Retrieved from: https://doi.org/10.1109/MIAS.2018.2875175.

McIntyre, A. (2018). Developing a Cybersecurity Protocol for Your Operational Environment. *Natural Gas & Electricity, 34*(9), 23–27. Retrieved from: https://doi.org/10.1002/gas.22048.

Miller, E. M., Porter, J. E., & Barbagallo, M. S. (2023). Simplifying Qualitative Case Study Research Methodology: A Step-By-Step Guide Using a Palliative Care Example. *Qualitative Report, 28*(8), 2363–2379. Retrieved from: https://doi.org/10.46743/2160-3715/2023.6478.

Mrabet, Z. El, Kaabouch, N., Ghazi, H. El, & Ghazi, H. El. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering, 67*, 469–482. https://doi.org/10.1016/J.COMPELECENG.2018.01.015.

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

O'Dwyer, E., Pan, I., Acha, S., & Shah, N. (2019). Smart energy systems for sustainable smart cities: Current developments, trends and future directions. *Applied Energy, 237*(October 2018), 581–597. Retrieved from: https://doi.org/10.1016/j.apenergy.2019.01.024.

Paradells, J., Lindelöf, B., & Barcelona, C. F. (2018). *Smart city lighting in the city of Stockholm.*

Pollock, N. W. (2020). Managing Bias in Research. *Wilderness & Environmental Medicine, 31*(1), 1–2. Retrieved from: https://doi.org/10.1016/j.wem.2020.01.001.

Pour, M. M., Anzalchi, A., & Sarwat, A. (2017). A review on cyber security issues and mitigation methods in smart grid systems. *Conference Proceedings - IEEE SOUTHEASTCON*, 1–4. Retrieved from: https://doi.org/10.1109/SECON.2017.7925278.

Qi, J., Hahn, A., Lu, X., Wang, J., & Liu, C. (2016). Cybersecurity for distributed energy resources and smart inverters. *IET Cyber-Physical Systems: Theory & Applications, 1*(1), 28–39. Retrieved from: https://doi.org/10.1049/iet-cps.2016.0018.

Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers and Security, 87,* 101561. Retrieved from: https://doi.org/10.1016/j.cose.2019.06.015.

Saadat, S., Bahizad, S., Ahmed, T., & Maingot, S. (2020). Smart Grid and Cybersecurity Challenges. *2020 5th IEEE Workshop on the Electronic Grid, EGRID 2020*, 1–8. Retrieved from: https://doi.org/10.1109/eGRID48559.2020.9330660.

Sinha, A., Mohandas, M., Pandey, P., & Vyas, O. P. (2021). Cyber Physical Defense Framework for Distributed Smart Grid Applications. *Frontiers in Energy Research, 8*(2), 1–17. Retrieved from: https://doi.org/10.3389/fenrg.2020.621650.

Solar Energy Technologies Office. (2020). *Solar cybersecurity basics.* U.S. Department of Energy. Retrieved from https://www.energy.gov/eere/solar/solar-cybersecurity-basics

Syrmakesis, A. D., Alcaraz, C., & Hatziargyriou, N. D. (2022). Classifying resilience approaches for protecting smart grids against cyber threats. *International Journal of Information Security, 21*(5), 1189–1210. Retrieved from:https://doi.org/10.1007/s10207-022-00594-7

Teichmann, F. M., & Boticiu, S. R. (2024). Adequate responses to cyber-attacks. *International Cybersecurity Law Review, 5*(2), 337–345. Retrieved from:https://doi.org/10.1365/S43439-024-00116-2

Toli, A. M., & Murtagh, N. (2020). The concept of sustainability in smart city definitions. *Frontiers in Built Environment, 6*. https://doi.org/10.3389/fbuil.2020.00077.

World Energy Council. (2016). *World energy perspectives the road to resilience.*

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access, 9,* 29775–29818. Retrieved from: https://doi.org/10.1109/ACCESS.2021.3058403

Κουνταρδάς, N., & Kountardas, N. (2017). *Big data real-time security analytics.*