International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources

Adebimpe Bolatito Ige [1,*], Eseoghene Kupa [2] and Oluwatosin Ilori [3]

[1] *Information Security Advisor, Corporate Security, City of Calgary, Canada.*
[2] *HSE Director - Frozen Hill Farms, Lagos State, Nigeria.*
[3] *Independent Researcher, Irving, TX, USA.*

International Journal of Science and Research Archive, 2024, 12(01), 2978–2995

Publication history: Received on 20 May 2024; revised on 25 June 2024; accepted on 28 June 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.12.1.1186

Abstract

This study investigates the cybersecurity challenges and strategies within the renewable energy sector, emphasizing the need for robust defense mechanisms against escalating cyber risks. Employing a systematic literature review and content analysis, the research scrutinizes peer-reviewed articles, industry reports, and international standards documents published between 2014 and 2024. The methodology focuses on identifying effective cybersecurity measures, innovative approaches, and the role of international cooperation in enhancing the security of renewable energy sources. Key findings reveal that the integration of renewable energy into the power grid introduces unique cybersecurity vulnerabilities, necessitating tailored defense strategies. Technological solutions, particularly artificial intelligence (AI) and machine learning (ML), emerge as promising tools for bridging existing security gaps. Moreover, international cooperation and adherence to global standards are identified as pivotal in bolstering cybersecurity resilience across the sector. The study proposes strategic recommendations for industry stakeholders, including the prioritization of comprehensive cybersecurity strategies, investment in advanced technologies, and fostering a culture of cybersecurity awareness. It also highlights the importance of developing robust cybersecurity frameworks through policy interventions and public-private partnerships. Finally, enhancing the cybersecurity of renewable energy sources requires a multifaceted approach that integrates innovative technologies, human factors, policy interventions, and international cooperation. Future research should explore the potential of emerging technologies and investigate the human and policy dimensions influencing cybersecurity in the renewable energy sector.

Keywords: Cyber Risks; Renewable Energy; Security; Defense Strategies; Energy Sector

1. Introduction

1.1. The Critical Importance of Cybersecurity in the Energy Sector

The critical importance of cybersecurity within the energy sector, particularly in the context of renewable energy sources, cannot be overstated. As the global community increasingly leans towards renewable energy to combat climate change and ensure sustainable development, the cybersecurity of these energy systems becomes paramount. The integration of renewable energy sources into the existing grid introduces a complex web of technological innovations and, consequently, new vulnerabilities to cyber threats (Shrobe, Shrier, & Pentland). The reliance on smart grids, which are essential for the efficient distribution of renewable energy, exemplifies this complexity. These grids, characterized by their advanced computing and communication technologies, are inherently more connected to the Internet and to each other, increasing their exposure to potential cyber-attacks (Shrobe, Shrier, & Pentland).

* Corresponding author: Adebimpe Bolatito Ige

The case of Moroccan energy companies, as explored by Raissouni et al. (2023), highlights the varying levels of cybersecurity maturity across the sector. Their findings underscore the significant challenges faced by energy companies in implementing effective cybersecurity measures. Factors such as the scarcity of qualified personnel, the high costs associated with security technologies, and the financial burden of training and awareness programs are notable obstacles. This situation is not unique to Morocco; it reflects a global challenge within the energy sector, emphasizing the need for a comprehensive approach to cybersecurity that addresses both technological and organizational aspects.

The systematic literature review conducted by Aarland and Gjøsæter (2022) on digital supply chain vulnerabilities in critical infrastructure, including the energy sector, reveals a significant gap in research on supply chain risks. Their work identifies the need for frameworks and methods that can enhance the resilience of supply chains against cybersecurity risks. This is particularly relevant for the energy sector, where the supply chain's complexity is magnified by the integration of renewable energy sources and the reliance on digital technologies.

In summary, the energy sector's shift towards renewable sources, while essential for sustainable development, introduces new cybersecurity challenges that must be addressed through a multidisciplinary approach. The experiences of Moroccan energy companies and the incidents in the wind energy sector illustrate the multifaceted nature of these challenges, encompassing technological, organizational, and supply chain vulnerabilities. As such, enhancing the cybersecurity of renewable energy sources requires not only technological solutions but also strategic investments in human resources, organizational resilience, and international cooperation to develop robust cybersecurity frameworks.

1.2. Defining the Scope: Cyber Risks and Renewable Energy Security

Defining the scope of cyber risks and renewable energy security involves understanding the multifaceted nature of threats that the energy sector faces in the digital age. The transition towards renewable energy sources, while essential for sustainable development, introduces new vulnerabilities and challenges in cybersecurity. Chobanov and Doychev (2022) highlight the importance of cybersecurity in the context of energy systems, emphasizing that the digital transformation of the energy sector, including the adoption of renewable sources, increases the potential for cyber-attacks. This transformation, driven by the need for efficient asset management and the prevention of vulnerabilities, underscores the critical role of cybersecurity in safeguarding energy systems against various forms of cyber threats.

Furthermore, the intersection of financial technology (FinTech) and renewable energy presents unique cybersecurity considerations. Rahardja et al. (2022) explore the impact of FinTech on the adoption of renewable energy in Asian Cooperation Dialogue (ACD) countries, emphasizing the role of cybersecurity in protecting systems and networks in the era of digital transformation. The study illustrates how FinTech innovations, such as cryptocurrencies and blockchain-based certifications, can support the renewable energy sector while also introducing new cybersecurity challenges that require careful management and protection strategies.

In summary, the scope of cyber risks and renewable energy security encompasses a broad range of threats and vulnerabilities, from technological to organizational and strategic dimensions. The integration of renewable energy sources into the energy sector's digital transformation amplifies these challenges, necessitating a multidisciplinary approach to cybersecurity. This approach should combine technological solutions with strategic planning, organizational resilience, and legal frameworks to effectively protect energy systems against cyber threats. The experiences and methodologies discussed in the literature provide a foundation for developing robust cybersecurity measures tailored to the unique needs of the renewable energy sector.

1.3. Historical Overview: Cybersecurity Challenges in the Energy Sector

The historical overview of cybersecurity challenges in the energy sector reveals a complex landscape marked by evolving threats and the sector's increasing reliance on digital technologies. Markopoulou (2022) provides a comprehensive analysis of the cybersecurity and sectoral regulatory frameworks, focusing on the energy and water sectors. The study highlights the critical role of smart metering systems in the new digitalized environment, underscoring the need for robust cybersecurity measures to protect these critical infrastructures. The deployment of smart technologies and devices introduces new vulnerabilities, making the energy sector a prime target for cyber-attacks. Markopoulou (2023) emphasizes the importance of a regulatory framework that can adapt to the dynamic nature of cyber threats, ensuring the resilience of critical energy and water infrastructures.

The digitalization of the power energy system introduces both opportunities and challenges. Timčenko et al. (2023) explore the principles of cybersecurity in the context of the digitalization of the power energy sector, highlighting the introduction of future internet technologies such as the Internet of Things, cloud, and fog computing. This digital

transformation, while offering significant benefits in terms of efficiency and flexibility, also exposes the energy sector to a range of cybersecurity issues. The paper discusses the role of intrusion detection systems and digital twin technologies in mitigating these risks, illustrating the need for advanced cybersecurity solutions to protect the increasingly digitalized energy infrastructure.

Venkatachary et al. (2021) delve into the specific challenges associated with securing virtual power plants, a key component of the modern energy sector. The paper proposes an edge-based security architecture to address the vulnerabilities inherent in distributed generators and virtual power plants. This approach aims to enhance the security of physical systems, ensure data protection, and maintain information privacy. The study acknowledges the persistent threat posed by cybercriminals and the ongoing challenge of mitigating risks and vulnerabilities within the energy sector. The proposed edge computing principles offer a promising solution to enhance the cybersecurity of virtual power plants, demonstrating the potential for innovative technologies to safeguard the energy sector against cyber threats.

In summary, the historical overview of cybersecurity challenges in the energy sector underscores the critical importance of adapting to the evolving threat landscape. The integration of digital technologies into the energy infrastructure, while offering numerous benefits, also introduces new vulnerabilities that must be addressed through comprehensive cybersecurity measures. The studies by Markopoulou, Timčenko et al., and Venkatachary et al. highlight the multifaceted nature of these challenges and the need for a collaborative approach involving regulatory frameworks, advanced cybersecurity technologies, and sector-specific solutions to ensure the resilience and security of the energy sector in the face of cyber threats.

1.4. Aim and Objectives of the Review

The aim of this study is to analyze and evaluate the effectiveness of current cybersecurity measures and strategies within the renewable energy sector, identifying challenges, barriers, and innovative approaches to enhance the security and resilience of renewable energy sources against cyber threats. The study seeks to understand the impact of cybersecurity on renewable energy security, explore the role of international cooperation and standards, and propose strategic recommendations for industry stakeholders, policymakers, and researchers.

The objectives are;

- To assess the critical importance of cybersecurity in the energy sector.
- To provide a historical overview of cybersecurity challenges in the energy sector.
- To analyze defense strategies against cyber risks in the energy sector.

2. Methodology

This study employs a systematic literature review and content analysis to evaluate the effectiveness of cybersecurity measures in the renewable energy sector, identify challenges and barriers, and explore innovative approaches to enhance security.

2.1. Data Sources

The primary data sources for this study include peer-reviewed academic journals, conference proceedings, industry reports, and white papers. Key databases such as IEEE Xplore, ScienceDirect, SpringerLink, Wiley Online Library, and the Web of Science were systematically searched to gather relevant literature. Government and industry standards documents, as well as publications from international cybersecurity and energy organizations, were also reviewed.

2.2. Search Strategy

A comprehensive search strategy was developed using a combination of keywords and phrases related to cybersecurity, renewable energy, defense mechanisms, and cyber threats. The search terms included "cybersecurity AND renewable energy," "cyber defense strategies in energy sector," "cyber risks in renewable energy," and "innovative cybersecurity technologies in energy." Boolean operators (AND, OR) were used to refine the search. The search was limited to documents published between 2014 and 2024 to ensure the relevance and timeliness of the data.

2.3. Inclusion and Exclusion Criteria for Relevant Literature

Inclusion criteria were established to select studies that specifically address cybersecurity challenges, strategies, and technologies within the renewable energy sector. Studies were included if they provided insights into the effectiveness of current cybersecurity measures, discussed innovative approaches to cyber defense, or analyzed the impact of cybersecurity on renewable energy security. Exclusion criteria were applied to omit studies that did not focus on the renewable energy sector, were not related to cybersecurity, or did not provide empirical data or comprehensive reviews of cybersecurity practices. Articles not published in English were also excluded.

2.4. Selection Criteria

The selection process involved screening titles and abstracts based on the inclusion and exclusion criteria, followed by a full-text review of the shortlisted articles. The relevance of each study was assessed by examining its contribution to understanding cybersecurity in the renewable energy sector. Reference lists of selected articles were also reviewed to identify additional relevant studies.

2.5. Data Analysis

Content analysis was conducted on the selected literature to extract data related to cybersecurity challenges, defense mechanisms, innovative approaches, and the impact of cybersecurity measures on renewable energy security. The analysis involved coding the content into thematic categories and identifying patterns and trends in the data. This approach facilitated a comprehensive understanding of the current state of cybersecurity in the renewable energy sector and the identification of gaps in knowledge and practice.

The findings from the systematic literature review and content analysis were synthesized to provide insights into the effectiveness of existing cybersecurity strategies, highlight innovative approaches to enhancing cybersecurity, and offer recommendations for future research and practice in the renewable energy sector.

3. The Landscape of Cyber Risks in the Energy Sector

3.1. Understanding Cyber Risks: Types and Implications

Understanding the landscape of cyber risks in the energy sector involves dissecting the types of threats and their implications for national security, infrastructure stability, and economic vitality. The energy sector, being pivotal to the functioning of modern societies, presents a lucrative target for cyber adversaries. The synthesis of threats and risks, as discussed by Mujević (2022), underscores the vulnerability of information communication infrastructure to cyber-attacks. This vulnerability is not isolated to specific regions but is a global concern, as evidenced by the hacker attack on the Government of Montenegro, which, while not compromising confidential data, highlighted the potential for serious breaches in state security. Such incidents underscore the necessity for a critical examination of existing information and communication infrastructure to anticipate and mitigate cyber threats effectively.

The digital transformation of the energy sector, as explored by Chobanov and Doychev (2022), brings forth both opportunities and challenges. The integration of renewable sources and the adoption of smart technologies improve asset management but also introduce vulnerabilities to cyber-attacks. The authors emphasize the shared responsibility for cybersecurity and the application of knowledge to reduce the damage from cyber incidents. This perspective is crucial in understanding that cybersecurity in the energy sector is not solely a technical issue but also a matter of organizational and societal concern.

Furthermore, the classification of cyber threats and the development of countermeasures, as detailed by Darem et al. (2023), provide a framework for understanding the complexity of cyber risks. While their study focuses on the banking and financial sector, the principles of threat classification and risk management are applicable to the energy sector. Identifying common threats and their characteristics helps in developing appropriate countermeasures, underscoring the importance of both technical and organizational strategies in mitigating cyber risks.

From the study, the energy sector's cybersecurity landscape is marked by a diverse array of threats, from sophisticated cyber-attacks targeting critical infrastructure to the vulnerabilities introduced by digital transformation and the integration of renewable energy sources. The studies by Mujević, Chobanov and Doychev, and Darem et al. highlight the multifaceted nature of these challenges, emphasizing the need for a comprehensive approach to cybersecurity. This approach should combine technological solutions with strategic planning, organizational resilience, and international cooperation to safeguard the energy sector against the evolving threat landscape.

3.2. The Architecture of Cybersecurity in Renewable Energy Systems

The architecture of cybersecurity in renewable energy systems is a critical area of focus as the sector increasingly relies on digital technologies for efficient operation and management. The integration of artificial intelligence (AI) into cybersecurity strategies for renewable energy systems presents a promising avenue for enhancing security measures against cyber threats. Mohamed et al. (2023) provide a comprehensive review of the applications of AI in this domain, highlighting the significant potential of AI in improving the security of renewable energy systems. The study notes that machine learning, a subset of AI, is particularly effective, demonstrating an impressive detection rate of 85% and a false positive rate below 5%. However, challenges such as the limited availability of relevant data and concerns regarding the interpretability of AI models persist, underscoring the need for further research to optimize the use of AI in cybersecurity for renewable energy.

The cybersecurity resiliency of marine renewable energy systems (MRE) is another critical aspect of the cybersecurity architecture in the renewable energy sector. de Peralta (2020) discusses the identification of cybersecurity vulnerabilities and determining risk in MRE systems, emphasizing the importance of a risk-based approach to cybersecurity. This approach involves assessing potential cyber threats, identifying vulnerabilities (including people, processes, technology, physical, and operational environment), and evaluating the consequences of cyberattacks on the operation of MRE systems and the impact on end users' mission and business objectives. The development of cybersecurity guidance based on standards from the National Institute of Standards and Technology (NIST) aims to enhance the resiliency of MRE systems against cyber threats.

Furthermore, de Peralta et al. (2021) delve into cybersecurity best practices and risk management for MRE systems in the second part of their series. This publication outlines an approach to select appropriate cybersecurity measures commensurate with the MRE system's cybersecurity risk. The guidance includes 86 cybersecurity best practices across 36 cybersecurity domains, grouped into nine categories, following the core functions of the NIST Cybersecurity Framework. This comprehensive framework provides a robust foundation for protecting information and operational technology assets prevalent in MRE systems, highlighting the importance of incorporating cybersecurity measures from the inception, development, operation, to decommissioning of MRE systems.

From the foregoing, the architecture of cybersecurity in renewable energy systems is complex and multifaceted, requiring a comprehensive approach that integrates advanced technologies like AI and adheres to established cybersecurity frameworks. The research by Mohamed et al. (2023) and de Peralta (2020, 2021) underscores the critical need for innovative solutions to address the unique cybersecurity challenges faced by the renewable energy sector. As the sector continues to evolve, so too must its cybersecurity strategies, ensuring the protection of critical infrastructure and the reliability of renewable energy sources.

3.3. Case Studies: Significant Cyber Attacks on Energy Systems

The energy sector's reliance on Supervisory Control and Data Acquisition (SCADA) systems for critical infrastructure management has exposed it to significant cyber risks. Ismail, Sitnikova, and Slay (2020) delve into the vulnerabilities of SCADA systems through an examination of nine case studies across multiple utility sectors, including transport, energy, and water. These case studies reveal how past cyber-attacks have compromised SCADA systems, leading to financial, economic, and, in some instances, physical harm to the public. The study underscores the importance of understanding cyber-terrorist decision-making theories and capabilities to better prepare for future cybersecurity threats against SCADA systems.

The transition to smart grids in the United States exemplifies the sector's increasing digital vulnerability. Huang, Majidi, and Baldick (2018) present a case study of the cyber-attack on the Ukrainian power grid, highlighting the vulnerabilities introduced by the digitalization of power systems. This attack, which disrupted electricity supply and demonstrated the potential for significant impacts on national security and economic stability, serves as a critical lesson in the importance of securing energy systems against cyber threats. The study emphasizes the need for a comprehensive approach to cybersecurity, incorporating both technological solutions and strategic planning to mitigate the risks of cyber-attacks on power systems.

Hossain et al. (2023) explore the threat of coordinated cyber-attacks on active distribution systems with high penetration of distributed energy resources (DERs) from an attacker's perspective. By developing a multi-stage attack algorithm and formulating an optimization problem to compromise voltage control, the study provides insights into the sophistication of modern cyber-attacks against energy systems. The research highlights the importance of understanding the attacker's perspective to develop effective countermeasures and improve the resilience of energy systems against cyber threats.

In summary, the case studies presented by Ismail, Sitnikova, and Slay (2020), Huang, Majidi, and Baldick (2018), and Hossain et al. (2023) illustrate the complex landscape of cyber threats facing the energy sector. These studies underscore the critical need for robust cybersecurity measures that address both the technological vulnerabilities of energy systems and the strategic aspects of cyber defense. As the energy sector continues to evolve and integrate digital technologies, the importance of safeguarding against cyber-attacks remains paramount to ensure the reliability, safety, and security of critical energy infrastructure.

3.4. Technological Innovations in Cybersecurity for Renewable Energy

The integration of renewable energy sources into urban microgrids presents a unique set of challenges and opportunities for cybersecurity. Xiong et al. (2023) provide a comprehensive analysis of the economic viability, technological innovations, and the probabilistic analysis of renewable adoption in urban microgrids. Their study highlights the critical role of technological innovations in ensuring the sustainability and reliability of these energy solutions. The research underscores the importance of adopting advanced cybersecurity measures to protect the increasingly complex and interconnected energy systems that characterize modern urban microgrids.

Lamnatou, Cristofari, and Chemisana (2023) explore the role of renewable energy sources in the energy transition, with a focus on technological innovations and a case study of the energy transition in France. Their research emphasizes the transformative potential of renewable energy technologies in achieving energy sustainability. However, the study also points to the cybersecurity challenges that accompany these technological innovations, particularly as energy systems become more distributed and reliant on digital technologies. The authors argue for the need to integrate robust cybersecurity strategies from the outset of renewable energy projects to safeguard against potential cyber threats.

Azevedo, Pellanda, and Campos (2020) address the cybersecurity challenges of future electrical power systems, including those powered by renewable energy sources. They examine the traditional structure of electrical power systems and the anticipated changes due to environmental concerns and technological evolution. The study highlights the cybersecurity implications of distributed renewable microgeneration, electric vehicles, distributed energy storage, the Internet of Things, smart grids, and software-defined operating devices. The authors propose that the cybersecurity of future power systems will require innovative approaches to mitigate risks associated with the increased complexity and interconnectedness of these systems.

In essence, the integration of renewable energy sources into urban microgrids and the broader energy transition presents both opportunities and challenges for cybersecurity. The studies collectively underscore the importance of technological innovations in enhancing the sustainability and reliability of renewable energy systems. However, they also highlight the critical need for advanced cybersecurity measures to protect against the evolving landscape of cyber threats. As renewable energy technologies continue to advance, so too must the cybersecurity strategies that safeguard these vital systems.

3.5. Current Trends and Future Directions in Cyber Risk Management

The landscape of cyber risk management in the renewable energy sector is undergoing significant transformation, driven by technological advancements and the evolving nature of cyber threats. Tsohou et al. (2023) delve into the role of cyber insurance as a pivotal strategy for managing cyber risks, highlighting its emergence as a crucial tool for organizations to protect against losses related to cyberattacks. The study provides a comprehensive review of the current state and future directions of cyber insurance, underscoring its importance in the broader context of cybersecurity strategies. This reflects a growing recognition of the need for financial risk transfer mechanisms in addition to technical cybersecurity measures.

Xue, Fan, and Yue (2020) explore the trends in risk management for renewable energy projects, emphasizing the shift from traditional risk management practices to technology-driven integration systems. Their analysis, based on a systematic review of research hotspots and frontiers in China, reveals an evolutionary trend towards integrating advanced technologies for risk assessment and mitigation in renewable energy projects. This trend underscores the importance of adopting innovative approaches to manage the complex uncertainties and long life cycles associated with renewable energy projects, highlighting the role of technology in enhancing the resilience of renewable energy systems against cyber threats.

Ricciardi and Valli (2023) report on the state of the art in control engineering and artificial intelligence (AI) for managing and controlling energy networks with improved efficiency and effectiveness. Their review focuses on recent trends in electric vehicle (EV) charging, cyber-physical security, and predictive maintenance, identified as key areas responsible for most of the business needs currently expressed by energy companies. The study provides a critical discussion of

methodological approaches and experimental setups, offering insights into how AI and control engineering can address the challenges of cyber-physical security in the energy sector. This highlights the potential of AI and related technologies to revolutionize energy management and cybersecurity practices, pointing towards future research directions in the integration of AI with cyber risk management strategies.

From the study, the current trends and future directions in cyber risk management for the renewable energy sector are characterized by a growing emphasis on integrating technological innovations with traditional risk management practices. The studies by Tsohou et al. (2023), Xue et al. (2020), and Ricciardi Celsi and Valli (2023) collectively highlight the pivotal role of cyber insurance, technology-driven risk management systems, and AI in addressing the cybersecurity challenges faced by the renewable energy sector. As the sector continues to evolve, these trends underscore the need for a multidisciplinary approach that combines technical, financial, and strategic elements to enhance the cybersecurity resilience of renewable energy systems.

4. Analyzing Defense Strategies

4.1. Comprehensive Review of Existing Defense Mechanisms

The integration of renewable energy sources into the power grid has necessitated the development of advanced cybersecurity measures to protect against the increasing threat of cyberattacks. Tuyen et al. (2022) provide a comprehensive review of cybersecurity in inverter-based smart power systems, highlighting the vulnerabilities introduced by the integration of distributed energy resources (DERs) and the smart inverters that are critical for the optimal operation of smart grids. The study discusses the nature of cyberattacks, state-of-the-art defense strategies, including detection and mitigation techniques, and offers an overview of testbed and simulation tools for cyber-physical research. This review underscores the importance of understanding system vulnerabilities and the need for continuous innovation in defense mechanisms to protect the burgeoning renewable energy infrastructure.

Sharma and Saraswat (2021) explore the cybersecurity challenges faced by the smart grid, particularly in the context of renewable energy integration. Their review outlines the efforts undertaken in the field of renewable energy cybersecurity, covering areas such as Power Control System (PCS) Risk, Proposed Smart Stability, Electric Grid Model Based Security, Distributed Generation Data Link Protection, and Smart Grid Simulations for Security Research. The paper emphasizes the complexity of the power system's infrastructure and the critical need for comprehensive cyber defense preparation to safeguard against potential threats.

Saleem et al. (2020) propose a multidimensional holistic framework for the security of distributed energy and control systems, addressing the gap left by traditional cybersecurity technologies. Their framework incorporates advanced technologies, intelligent algorithms, and continuous assessments to ensure security across all dimensions of the information assurance model required for a robust cybersecurity business process. By integrating the layered defense model into the National Renewable Energy Laboratory's Security and Resilience Testbed, the study evaluates the security and resilience of microgrid control systems, offering insights and best practices for utility cybersecurity analysts.

In summary, the comprehensive review of existing defense mechanisms in cybersecurity for renewable energy highlights the critical need for innovative and multidimensional approaches to safeguard the smart grid and its components. The studies by Tuyen et al. (2022), Sharma and Saraswat (2021), and Saleem et al. (2020) collectively emphasize the importance of understanding the specific vulnerabilities of renewable energy systems and the development of advanced defense strategies to mitigate the risks posed by cyber threats. As the renewable energy sector continues to evolve, so too must the cybersecurity measures designed to protect it, ensuring the resilience and reliability of the energy infrastructure in the face of increasingly sophisticated cyberattacks.

4.1.1. Technological Solutions: Firewalls, Encryption, and Beyond

The integration of renewable energy sources into the power grid has necessitated the development of advanced cybersecurity measures to protect against the increasing threat of cyberattacks. The adoption of artificial intelligence (AI) has emerged as a promising approach to enhance the security of renewable energy systems (Ohalete et al., 2023). Mohamed et al. (2023) provide a comprehensive review of the applications of AI in cybersecurity for renewable energy systems, highlighting the significant potential of AI in improving the security of these systems. The study notes that machine learning, a subset of AI, is particularly effective, demonstrating an impressive detection rate of 85% and a false positive rate below 5%. However, challenges such as the limited availability of relevant data and concerns regarding the

interpretability of AI models persist, underscoring the need for further research to optimize the use of AI in cybersecurity for renewable energy.

The rapid evolution of Smart Energy Communities (SECs) has introduced novel cybersecurity issues that require innovative solutions. Gaggero et al. (2023) analyze common architectures and protocols used to build SECs, evaluating the attack surfaces and possible vulnerabilities. The study discusses solutions that can be employed to mitigate risks and highlights current gaps in the state of the art. This research emphasizes the importance of evaluating cybersecurity risks from the beginning to develop "secure-by-design" systems and platforms for SECs.

Furthermore, the role of technological solutions such as automation, blockchain, and smart cities in renewable energy use has been explored by Tarasova et al. (2021) and Ohalete et al. (2023). The paper presents a comprehensive overview of how these technologies can be employed for smarter green energy use, enhancing efficiency and sustainability. The integration of blockchain technology, in particular, offers a decentralized and secure platform for energy transactions, which can significantly improve the cybersecurity posture of renewable energy systems.

In summary, the comprehensive review of existing technological solutions in cybersecurity for renewable energy highlights the critical need for innovative and multidimensional approaches to safeguard the smart grid and its components. The studies collectively emphasize the importance of understanding the specific vulnerabilities of renewable energy systems and the development of advanced defense strategies to mitigate the risks posed by cyber threats. As the renewable energy sector continues to evolve, so too must the cybersecurity measures designed to protect it, ensuring the resilience and reliability of the energy infrastructure in the face of increasingly sophisticated cyberattacks.

4.1.2. Policy and Regulatory Approaches: Standards and Frameworks

The renewable energy sector is increasingly facing the challenge of integrating cybersecurity measures within its operational and regulatory frameworks. D'Alpaos and Andreolli (2020) highlight the need for new policy and regulatory frameworks designed to address the unique challenges posed by renewable energy communities. These communities, characterized by their reliance on distributed energy resources, necessitate a reevaluation of traditional energy policies to ensure both the security and efficiency of renewable energy systems. The study underscores the importance of developing regulatory frameworks that can adapt to the evolving landscape of renewable energy, emphasizing the role of policy in fostering secure and sustainable energy communities.

Mudaliyar, Sharma, and Panja (2022) explore various governmental approaches to reducing greenhouse gas emissions and promoting renewable energy sources. Their research delves into the effectiveness of carbon pricing, emissions trading systems, and financial incentives in encouraging the adoption of renewable energy technologies. The study also examines the impact of regulatory support and policy initiatives on investment in distributed renewable energy systems, such as feed-in tariffs and net metering. The findings suggest that while there is significant diversity in national policies, shared experiences and strategies can inform the development of more effective policies aimed at combating climate change and advancing sustainable energy.

In summary, the integration of policy and regulatory approaches in cybersecurity for renewable energy is crucial for the development of secure, efficient, and sustainable energy systems. The studies by D'Alpaos and Andreolli (2020), Mudaliyar, Sharma, and Panja (2022), and Khydyntsev (2023) collectively emphasize the need for innovative policy frameworks that can accommodate the unique characteristics of renewable energy communities and the broader energy sector. As the renewable energy landscape continues to evolve, so too must the policies and regulations that govern its development, ensuring that cybersecurity remains a central consideration in the pursuit of a sustainable energy future.

4.1.3. Human Factors: Training and Awareness Programs

The integration of human factors in cybersecurity training and awareness programs is crucial for enhancing the security posture of organizations, especially those involved in the renewable energy sector. Giriraj, Haggag, and Haggag (2022) emphasize the importance of customizing cybersecurity training materials to address human factors effectively. Their study proposes a human-centric framework that suggests personalized cybersecurity training materials based on the end-user's knowledge about cybersecurity. This approach acknowledges the diversity in employees' cybersecurity awareness levels and aims to bridge the gap by providing tailored training that addresses specific needs and vulnerabilities.

Nasir (2023) delves into the effectiveness of cybersecurity training programs, highlighting the significance of addressing human vulnerability to foster a positive cybersecurity awareness culture within organizations. The research evaluates the mechanics influencing the success of cybersecurity training programs and presents best practices and success factors for their development. Nasir's findings propose a model examining the relationship between cybersecurity training and user behavior, emphasizing the interconnectedness of input, process, and output components in achieving effective cybersecurity awareness.

Flores et al. (2023) explore the human factors relevant to cybersecurity awareness in a remote work environment, a setting that has become increasingly common in the renewable energy sector. Through qualitative interviews, the study identifies trust in cybersecurity infrastructure, previous practices, training, security fatigue, and the potential improvements with gamification as core elements supporting the success of cybersecurity programs. This research underscores the need for cybersecurity training and awareness programs to consider the unique challenges and opportunities presented by remote work settings.

In summary, addressing human factors through training and awareness programs is essential for mitigating cybersecurity risks in the renewable energy sector. The studies by Giriraj, Haggag, and Haggag (2022), Nasir (2023), and Flores et al. (2023) collectively highlight the need for personalized, effective, and engaging cybersecurity training that accounts for the diverse needs and vulnerabilities of employees. As the renewable energy sector continues to evolve, so too must the approaches to cybersecurity training and awareness, ensuring that human factors are at the forefront of developing a secure and resilient energy infrastructure.

4.2. Effectiveness and Limitations of Current Strategies

The integration of renewable energy into the power grid presents both opportunities and challenges for cybersecurity. Oyekale et al. (2020) provide a succinct review of the impacts of renewable energy resources on the effectiveness of grid-integrated systems, highlighting the current challenges and potential solution strategies. The study emphasizes the need for innovative solutions to address the vulnerabilities introduced by the integration of renewable energy sources, such as solar, wind, biomass, and geothermal energy, into the power grid. The research underscores the importance of developing robust cybersecurity measures to protect against potential cyberattacks that could compromise the reliability and efficiency of renewable energy systems.

Halkos and Gkampoura (2020) delve into the usage, potentials, and limitations of renewable energy sources, examining their connection to climate change, economic growth, and human health. The paper reviews consumers' willingness to pay for renewables in different countries and analyzes policies and strategies recommended for fully integrating renewables as a sustainable energy source. This comprehensive review highlights the critical role of cybersecurity in ensuring the safe and efficient operation of renewable energy systems, pointing out the necessity for policies and strategies that address the unique cybersecurity challenges posed by renewable energy technologies.

Adegbite et al. (2023) analyze cybersecurity strategies in the USA, focusing on protecting national infrastructure, including the energy sector, from cyber threats. The review outlines key frameworks, policies, and initiatives implemented by the USA to safeguard its critical infrastructure against cyberattacks. The paper examines the strategic approaches adopted, including the National Infrastructure Protection Plan (NIPP) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The study assesses the effectiveness of these strategies in enhancing the resilience of national infrastructure against cyber threats, offering insights into the lessons and implications for global cybersecurity practices.

From the foregoing, the effectiveness and limitations of current strategies in cybersecurity for renewable energy are multifaceted, requiring a comprehensive approach that encompasses technical, policy, and strategic dimensions. The studies highlight the importance of developing and implementing robust cybersecurity measures to protect renewable energy systems. As the renewable energy sector continues to grow, so too must the cybersecurity strategies designed to safeguard it, ensuring the resilience and sustainability of the energy infrastructure in the face of evolving cyber threats.

4.3. Innovative Approaches in Cyber Defense for the Energy Sector

The energy sector's transition towards decentralization, incorporating numerous smaller energy producers alongside traditional large-scale projects, has underscored the critical need for robust cybersecurity measures. Mladenov et al. (2020) discuss the development of tailored cybersecurity solutions for various actors within the energy sector, highlighting the SPEAR consortium's initiative to secure the energy system against cyber-attacks. This initiative is particularly significant for small energy plants, which often lack the resources for expensive cybersecurity systems and

are thus left vulnerable. The study presents a case of a hydro power plant in Bulgaria, which had previously experienced a cyber-attack, underscoring the real and present danger of such threats to the energy sector's stability and security.

The expansion of digital management services within the energy sector introduces new cybersecurity challenges, particularly in the context of cyber-physical systems. Bugaev et al. (2023) propose the formation of an Integrated Digital Data Management Platform to create a secure information structure for intercorporate exchange of data and electronic documents within the energy sector. This initiative aims to enhance the security of cyber-physical systems across various forms of ownership and government bodies, highlighting the importance of a unified approach to cybersecurity in the face of digital transformation.

Davydiuk and Zubok (2023) provide an analytical review of the resilience of Ukraine's critical energy infrastructure to cyber threats amid ongoing conflict. The study identifies cyber resilience factors and their dependencies, analyzing the causes of vulnerabilities within the energy sector. The research emphasizes the importance of enhancing the resilience of the energy sector through processes such as big data analysis, public-private cooperation, and cyber training. This approach aims to increase the level of cybersecurity for critical infrastructure, demonstrating the need for proactive and comprehensive strategies to mitigate cyber threats.

In summary, innovative approaches in cyber defense for the energy sector are essential for protecting critical infrastructure against the evolving landscape of cyber threats. The studies by Mladenov et al. (2020), Bugaev et al. (2023), and Davydiuk and Zubok (2023) collectively highlight the need for tailored cybersecurity solutions, integrated digital platforms, and resilience-enhancing strategies to safeguard the energy sector. As the sector continues to evolve towards decentralization and digitalization, so too must the cybersecurity measures designed to protect it, ensuring the stability and security of energy systems worldwide.

4.4. Integrating Cybersecurity with Renewable Energy Development

The integration of cybersecurity within the development of renewable energy systems is becoming increasingly crucial as the sector evolves towards more interconnected and intelligent infrastructures. Rekeraho et al. (2023) delve into the cybersecurity challenges faced by IoT-based smart renewable energy systems, highlighting the vulnerabilities that these systems are exposed to due to their reliance on internet connectivity. The study identifies false data injection, replay, denial of service, and brute force credential attacks as primary threats, emphasizing the need for secure communication protocols, robust encryption techniques, and effective access control measures to safeguard smart renewable energy systems.

Rambabu et al. (2023) explore the intersection of renewable energy and computer science, underscoring the role of computer science in enhancing the efficiency, integration, and management of renewable energy systems. The paper discusses the potential of smart grid technology, energy storage solutions, demand-side management, and predictive analytics in optimizing renewable energy consumption and system stability. However, it also points out the challenges associated with integrating renewable energy sources and computer science, such as technical complications, interoperability issues, and cybersecurity concerns, advocating for comprehensive solutions to address these hurdles.

de Peralta (2020) focuses on the cybersecurity resiliency of marine renewable energy systems, presenting a framework for identifying cybersecurity vulnerabilities and assessing risks. The study is based on standards developed by the National Institute of Standards and Technology (NIST) and aims to guide marine renewable energy developers and stakeholders in assessing their cybersecurity risk posture. By incorporating appropriate cybersecurity controls, the approach seeks to reduce the consequences and impacts of cyberattacks on marine renewable energy systems, highlighting the importance of cybersecurity measures from the inception to the decommissioning of these systems.

From the study, integrating cybersecurity with renewable energy development is essential for ensuring the security and resilience of the energy sector in the face of evolving cyber threats. The studies emphasize the need for innovative cybersecurity solutions that address the unique challenges posed by smart renewable energy systems. As the renewable energy sector continues to grow and integrate with advanced technologies, so too must the cybersecurity strategies designed to protect it, ensuring a sustainable and secure energy future.

5. Case Studies and Practical Applications

5.1. Successful Implementations of Cyber Defense Strategies

The energy sector's cybersecurity landscape is evolving rapidly, necessitating innovative defense strategies to protect critical infrastructure. Mukherjee (2019) discusses the implementation of cybersecurity in the energy sector, highlighting the increasing number of successful cyber-attacks and the critical role of cybersecurity in ensuring energy security. The study emphasizes the need for energy companies, primarily operated by private corporations, to prioritize cybersecurity to protect their systems from threats posed by malicious actors. The research underscores the importance of establishing dedicated cybersecurity cells within organizations and enhancing board-level understanding of cybersecurity issues to ensure effective protection of the energy infrastructure.

Davydiuk and Zubok (2023) provide an analytical review of the resilience of Ukraine's critical energy infrastructure to cyber threats amid ongoing conflict. The study identifies cyber resilience factors and their dependencies, emphasizing the need for comprehensive strategies to enhance the resilience of the energy sector. The research proposes implementing processes for collecting and processing big data on cyber statistics, optimizing public-private cooperation, and organizing cyber training to increase the level of cybersecurity for critical infrastructure. This approach aims to improve the effectiveness of responding to cybersecurity crises, highlighting the unique experience of Ukraine in conducting such research and its potential to serve as a model for other countries.

Tobar Rosero et al. (2023) explore the role of digital substations in the transformation of the electricity sector, focusing on the cybersecurity challenges associated with the adoption of information and communication technologies (ICTs). The study presents a simulated substation environment to demonstrate successful spoofing attacks and highlights the importance of managing cyber risks in digital systems. The research reveals vulnerabilities within communication protocols and proposes attributes for early attack detection, providing valuable guidance for implementing innovative applications and advancing human capital knowledge in the energy sector.

In summary, the successful implementation of cyber defense strategies in the energy sector is crucial for protecting critical infrastructure against evolving cyber threats. The studies emphasize the need for innovative cybersecurity solutions, comprehensive strategies to enhance resilience, and the importance of public-private cooperation in safeguarding the energy sector. As the sector continues to integrate advanced technologies, so too must the cybersecurity measures designed to protect it, ensuring the security and reliability of energy systems worldwide.

5.2. Lessons Learned from Cybersecurity Breaches

The energy sector's cybersecurity landscape is continuously evolving, necessitating a proactive and informed approach to safeguarding critical infrastructure. Freier (2021) explores the impact of digitalization and flexibility trading in the energy sector, focusing on lessons learned from Northeastern Germany. The study highlights the transformative potential of digital technologies in enhancing the efficiency and resilience of energy systems. However, it also points out the cybersecurity challenges that accompany digitalization, underscoring the importance of developing robust cybersecurity measures to protect against potential threats. The lessons learned from the German experience provide valuable insights into the integration of digital technologies in the energy sector, emphasizing the need for a balanced approach that considers both the benefits and risks of digitalization.

Funabashi and Dickson (2023) delve into the Fukushima disaster, offering critical lessons learned from this devastating "near-miss" in the energy sector. The study examines the failure to adequately address known vulnerabilities and the consequences of inadequate regulatory oversight. The Fukushima incident serves as a stark reminder of the potential risks associated with energy production and the importance of maintaining rigorous safety and security standards. The lessons learned from Fukushima are applicable beyond the nuclear industry, highlighting the need for continuous improvement in cybersecurity practices across all segments of the energy sector to prevent future disasters.

In summary, the successful implementation of cybersecurity measures in the energy sector requires learning from past incidents and leveraging insights from other domains. The studies emphasize the importance of adopting a holistic and informed approach to cybersecurity. By integrating lessons learned from various sectors and incidents, the energy sector can enhance its resilience against cyber threats, ensuring the security and reliability of critical energy infrastructure.

5.3. Comparative Analysis of Cybersecurity Practices across Different Regions

The cybersecurity practices in the energy sector vary significantly across different regions, influenced by social, cultural, and economic factors. Creese, Dutton, and Esteve-González (2021) conducted an empirical study exploring the social and cultural aspects of cybersecurity capacity building in 78 nations. Their findings suggest that while geographical regions might share similar attitudes and practices around cybersecurity, the primary differences are largely explained by cross-national differences in development and the scale of Internet use. This study highlights the importance of considering national development and Internet usage levels when assessing cybersecurity capacity, rather than relying solely on regional categorizations.

Ersoy and Taslak (2022) provide a multidimensional framework to measure corporate sustainability in the energy sector, comparing the sustainability performance of energy companies operating in Asia and Europe. Their analysis, utilizing hybrid multiple-criteria decision-making (MCDM) methods, reveals that energy companies in the Asian region are more sustainable than those in the European region. This comparative analysis underscores the varying approaches to sustainability and, by extension, cybersecurity practices within the energy sector across different regions, emphasizing the role of corporate sustainability in shaping cybersecurity strategies.

Lu et al. (2019) focus on the corporate social responsibility (CSR) of energy utilities in the Baltic States and its link to sustainable energy development achievements. Their comparative analysis of CSR reports and sustainable energy development trends in Lithuania, Latvia, and Estonia provides insights into how energy utilities' CSR practices can impact the achievement of sustainable energy development targets. The study suggests that the CSR practices of energy utilities, which include cybersecurity measures, play a significant role in advancing sustainable energy development, highlighting the interconnection between CSR, cybersecurity, and sustainable energy goals.

From the study, the comparative analysis of cybersecurity practices across different regions in the energy sector reveals significant variations influenced by development levels, Internet usage, corporate sustainability, and CSR practices. These studies collectively emphasize the need for a nuanced understanding of regional differences in cybersecurity practices within the energy sector. As the sector continues to evolve, recognizing and addressing these variations will be crucial in developing effective cybersecurity strategies that cater to the specific needs and challenges of different regions.

6. Discussion

6.1. Analyzing the Impact of Cybersecurity Measures on Renewable Energy Security

The integration of renewable energy sources into the electricity market presents both opportunities and challenges for energy security, particularly in the context of cybersecurity. Ríos-Ocampo, Arango-Aramburo, and Larsen (2021) explore the impact of renewable energy penetration on energy security, highlighting the vulnerabilities introduced by the dependency on weather conditions for energy generation. The study emphasizes the importance of developing robust cybersecurity measures to protect against potential cyberattacks that could exploit these vulnerabilities, potentially compromising the reliability, reserve margin, resilience, and vulnerability of the energy system.

Nazaré, Nardo, Arias-Garcia, and Nepomuceno (2023) focus on the cybersecurity challenges associated with Ocean Energy Power Plants, a promising solution to address climate change and fossil fuel depletion. The study underscores the critical need for cybersecurity measures to protect the networks connecting devices in these systems, emphasizing the importance of reducing vulnerability and increasing resilience to prevent attacks and minimize cyber threats to suppliers and customers. The European Commission's objective of reducing critical infrastructure vulnerability and increasing its resilience highlights the significance of cybersecurity in ensuring the security and reliability of renewable energy sources.

Rahardja et al. (2022) examine the role of financial technology (FinTech) in promoting the use of renewable energy across the Asian Cooperation Dialogue (ACD) countries, emphasizing the cybersecurity implications of digital technologies in the renewable energy sector. The study highlights the potential of cryptocurrencies, blockchain-based certifications, and crowdsourcing for renewable energy projects to enhance the security and efficiency of renewable energy systems. However, it also points out the need for comprehensive cybersecurity measures to protect systems and networks in the era of digital transformation.

In summary, the impact of cybersecurity measures on renewable energy security is significant, with the potential to enhance or compromise the reliability and resilience of renewable energy systems. The studies by Ríos-Ocampo et al.

(2021), Nazaré et al. (2023), and Rahardja et al. (2022) collectively emphasize the need for innovative and effective cybersecurity strategies to safeguard renewable energy infrastructure against cyber threats. As the renewable energy sector continues to grow and integrate with digital technologies, the importance of cybersecurity in ensuring the security and sustainability of energy systems cannot be overstated.

6.2. Challenges and Barriers in Enhancing Cybersecurity in the Energy Sector

The energy sector's cybersecurity landscape is fraught with challenges and barriers that hinder the enhancement of security measures. Smith (2018) highlights the growing concern among U.S. policymakers regarding cyberattacks on the nation's energy infrastructure, emphasizing the critical need for enhanced cybersecurity measures. The establishment of the National Risk Management Center (NRMC) by the U.S. Department of Homeland Security (DHS) underscores the federal government's commitment to defending critical infrastructure, including the energy sector, against worsening threats. Smith's analysis points to the geopolitical complexities and the urgent need for robust cybersecurity frameworks to protect the energy sector from potential adversaries.

Markopoulou (2022) delves into the applicability of the EU cybersecurity regulatory framework in the energy and water sectors, focusing on the challenges posed by the expansive deployment of smart technologies and devices. The paper examines the regulatory regime of smart meters and the privacy and security complications associated with their installation and use. Markopoulou (2022) sheds light on the shortcomings of the existing legal framework and suggests further steps to enhance the cyber resilience of the energy and water sectors in the face of evolving cyber threats.

Venkatachary, Alagappan, and Andrews (2021) explore the cybersecurity challenges associated with virtual power plants and the potential application of edge computing principles to enhance security. The paper presents a comprehensive edge-based security architecture aimed at reducing risks and securing physical systems while ensuring privacy and data protection. This study underscores the technological advancements and the persistent challenge of mitigating risks and vulnerabilities in the energy sector, highlighting the importance of innovative solutions to bolster cybersecurity.

In summary, the challenges and barriers in enhancing cybersecurity in the energy sector are multifaceted, encompassing geopolitical, regulatory, technological, and privacy concerns. The studies collectively emphasize the critical need for a comprehensive approach to cybersecurity, integrating robust regulatory frameworks, innovative technological solutions, and collaborative efforts to safeguard the energy sector against cyber threats. As the sector continues to evolve and integrate advanced technologies, addressing these challenges will be paramount in ensuring the security and resilience of critical energy infrastructure.

6.3. Future Trends in Cyber Defense Technologies and Strategies

The energy sector is at a critical juncture, facing the dual challenge of ensuring security while embracing digital transformation. Simonovich (2020) discusses the paramount importance of protecting endpoint operating technologies (OT) in the utility sector, emphasizing the escalating frequency and sophistication of cyberattacks. The paper highlights the structural mismatches between the life cycles of OT and the maintenance cycles, which complicate the defense of assets. Simonovich advocates for future cybersecurity solutions that function while isolated, remain potent between updates, and provide flexibility for deployment in varied OT configurations. Artificial intelligence (AI) and machine learning (ML) solutions are posited as capable of meeting these requirements, offering a path forward for the energy sector to navigate the cybersecurity landscape.

Yeremyan and Yeremyan (2022) delve into the international law issues surrounding cyber defense, particularly in the context of the defense sector's rapid technological development. The paper examines whether current legal regulations at international and national levels are sufficient to address the challenges posed by cyber warfare and the advancement of cyber weapons. The authors suggest that cyber means of warfare, which have been increasingly used in recent decades, necessitate a reevaluation of legal and strategic solutions to ensure adequate defense capabilities.

Trifunović and Bjelica (2021) explore the evolving nature of cyber warfare, emphasizing its implications for civilian infrastructure and military readiness. The paper discusses the role of special war and the unlimited number of potential adversaries in cyber warfare, highlighting the importance of intelligence in planning future defense scenarios against hybrid or other cyber threats. The authors argue for the need to consider the rapid deployment of problematic cyber technology and the trends in cyber-attack and defense technologies.

In summary, the future trends in cyber defense technologies and strategies in the energy sector underscore the need for innovative solutions that can adapt to the rapidly evolving threat landscape. The studies highlight the importance of

AI and ML solutions, the reevaluation of legal frameworks, and the strategic consideration of intelligence in planning defense against cyber threats. As the sector continues to integrate digital technologies, these insights will be crucial in developing effective cyber defense strategies to protect critical energy infrastructure.

7. Conclusions and Recommendations

The systematic literature review and content analysis revealed several key findings crucial for strengthening the security of renewable energy sources against cyber risks. Firstly, the integration of renewable energy into the power grid introduces unique cybersecurity challenges, necessitating tailored defense mechanisms. Secondly, the effectiveness of current cybersecurity measures varies widely, with technological solutions like AI and ML showing promise in bridging existing gaps. Thirdly, international cooperation and adherence to global standards play a pivotal role in enhancing cybersecurity resilience across the energy sector. Lastly, there is a critical need for continuous innovation in cybersecurity strategies to keep pace with the evolving threat landscape.

To mitigate cyber risks effectively, industry stakeholders should prioritize the development and implementation of comprehensive cybersecurity strategies that encompass technological, human, and policy dimensions. Investing in advanced cybersecurity technologies, such as AI and ML, can provide proactive defense mechanisms. Additionally, fostering a culture of cybersecurity awareness and training among employees is essential. Stakeholders should also engage in international collaborations to share best practices and leverage global standards for cybersecurity in the renewable energy sector.

The findings underscore the importance of developing robust cybersecurity frameworks that can adapt to the specific needs of the renewable energy sector. Policymakers should consider enacting regulations that encourage the adoption of best practices in cybersecurity, including the use of standardized protocols and technologies. Furthermore, policies should facilitate public-private partnerships to enhance the sharing of cybersecurity intelligence and resources. Establishing clear guidelines for responding to cyber incidents and promoting resilience in renewable energy infrastructure is also crucial.

Future research should focus on exploring the potential of emerging technologies to enhance cybersecurity in the renewable energy sector. Studies on the effectiveness of AI and ML in detecting and mitigating cyber threats in real-time can provide valuable insights. Additionally, research on the human factors influencing cybersecurity, such as behavior, culture, and training, can help in developing more effective awareness programs. Investigating the impact of international cooperation and standards on improving cybersecurity practices across different regions can also contribute to the development of a more secure global energy infrastructure.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Aarland, M., & Gjøsæter, T. (2022). Digital Supply Chain Vulnerabilities in Critical Infrastructure: A Systematic Literature Review on Cybersecurity in the Energy Sector. Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP), 1, pp. 326-333. https://doi.org/10.5220/0010803800003120

[2] Adegbite, A. O., Akinwolemiwa, D. I., Uwaoma, P. U., Kaggwa, S., Akindote, O. J., & Dawodu, S. O. (2023). Review of Cybersecurity Strategies in Protecting National Infrastructure: Perspectives from the USA. Computer Science and Information Technology Research Journal, 4(3), 200-219. https://doi.org/10.51594/csitrj.v4i3.658

[3] Azevedo, G. P., Pellanda, P., & Campos, M. (2020). Addressing the Cybersecurity Challenges of Electrical Power Systems of the Future," 2020 12th International Conference on Cyber Conflict (CyCon), Estonia, 2020, pp. 293-308. https://doi.org/10.23919/CyCon49761.2020.9131732

[4] Bugaev, A., Grabchak, E., Grigoriev, V., & Loginov, E. (2021). Ensuring the security of cyber-physical systems in the energy sector in the context of the expansion of digital management services. In CEUR Workshop Proceedings, pp. 164-173.

[5] Chobanov, V., & Doychev, I. (2022). Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-5. https://doi.org/10.1109/hora55278.2022.9800102

[6] Chobanov, V., & Doychev, I. (2022). Cyber Security impact on energy systems. International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-5. https://doi.org/10.1109/hora55278.2022.9800102

[7] Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. Personal and ubiquitous computing, 25(5), 941-955. https://doi.org/10.1007/s00779-021-01569-6

[8] D'Alpaos, C., & Andreolli, F. (2021). Renewable Energy Communities: The challenge for new policy and regulatory frameworks design. In New Metropolitan Perspectives: Knowledge Dynamics and Innovation-driven Policies towards Urban and Regional Transition Volume 2, pp. 500-509. Springer International Publishing. https://doi.org/10.1007/978-3-030-48279-4_47

[9] Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. IEEE Access, 11, 125138-125158. https://doi.org/10.1109/ACCESS.2023.3327016

[10] Davydiuk, A., & Zubok, V. (2023). Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War," 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Tallinn, Estonia, 2023, pp. 121-139. https://doi.org/10.23919/CyCon58705.2023.10181813

[11] de Peralta, F. A. (2020). Cybersecurity Resiliency of Marine Renewable Energy Systems – Part 1: Identifying Cybersecurity Vulnerabilities and Determining Risk. Marine Technology Society Journal, 54(6), 97-107. https://doi.org/10.4031/mtsj.54.6.9

[12] de Peralta, F. A., Watson, M., Bays, R. M., Boles, J. R., & Powers, F. (2021). Cybersecurity Resiliency of Marine Renewable Energy Systems Part 2: Cybersecurity Best Practices and Risk Management. Marine Technology Society Journal, 55(2), 104-116. https://doi.org/10.4031/MTSJ.55.2.4

[13] Ersoy, N., & Taslak, S. (2023). Comparative Analysis of MCDM Methods for the Assessment of Corporate Sustainability Performance in Energy Sector. Ege Academic Review, 23(3), 341-362. https://doi.org/10.21121/eab.986122

[14] Flores, C., Gonzalez, J., Kajtazi, M., Bugeja, J., & Vogel, B. (2023). Human Factors for Cybersecurity Awareness in a Remote Work Environment. In 9th International Conference on Information Systems Security and Privacy (ICISSP 2023), Lisbon, Portugal, 22–24 February 2023, Vol. 1, pp. 608-616. SciTePress. https://dx.doi.org/10.5220/0011746000003405

[15] Freier, A. (2022). Digitalization and flexibility trading in the energy sector. Lessons learned from Northeastern Germany. Lessons learned from Northeastern Germany, January 3, 2022. Available at: https://doi.org/10.2139/ssrn.3998659

[16] Funabashi, Y., & Dickson, M. F. (2023). Fukushima: Lessons learned from a devastating "near-miss". Bulletin of the Atomic Scientists, 79(3), 161-165. https://doi.org/10.1080/00963402.2023.2200121

[17] Gaggero, G., Piserà, D., Girdinio, P., Silvestro, F., & Marchese, M. (2023). Novel Cybersecurity Issues in Smart Energy Communities," 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, pp. 1-6. https://doi.org/10.1109/ICAISC56366.2023.10085312

[18] Giriraj, A., Haggag, S., & Haggag, H. (2022). Human centric framework for customising and producing effective cybersecurity training materials. In Joint 4th International Workshop on Experience with SQuaRE Series and Its Future Direction and 1st Asia-Pacific Software Engineering and Diversity, Equity, and Inclusion Workshop, IWESQ 2022+ APSEDEI 2022, Tokyo, Japan, December 6, pp. 69-77. https://dblp.org/rec/conf/apsec/GirirajHH22.html

[19] Halkos, G., & Gkampoura, E.-C. (2020). Reviewing Usage, Potentials, and Limitations of Renewable Energy Sources. Energies, 13(11), 2906. https://doi.org/10.3390/en13112906

[20] Hossain, M., Gao, X., Ali, M., Rahman, A., & Sun, W. (2023). Coordinated Cyber Attacks in Distribution Grid with Distributed Energy Resources: Attacker Perspective," 2023 IEEE Kansas Power and Energy Conference (KPEC), Manhattan, KS, USA, 2023, pp. 1-4. https://doi.org/10.1109/KPEC58008.2023.10215106

[21] Huang, B., Majidi, M., & Baldick, R. (2018). Case Study of Power System Cyber Attack Using Cascading Outage Analysis Model," 2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, USA, 2018, pp. 1-5. https://doi.org/10.1109/PESGM.2018.8585921

[22] Ismail, S., Sitnikova, E., & Slay, J. (2015). SCADA systems cyber security for critical infrastructures: Case Studies in the transport sector. In International Conference on Cyber Warfare and Security, pp. 446-464. Academic Conferences International Limited. https://doi.org/10.4018/978-1-7998-2466-4.ch028

[23] Lamnatou, C., Cristofari, C., & Chemisana, D. (2023). Renewable energy sources as a catalyst for energy transition: Technological innovations and an example of the energy transition in France. Renewable Energy, 119600. https://doi.org/10.1016/j.renene.2023.119600

[24] Lu, J., Ren, L., Yao, S., Qiao, J., Strielkowski, W., & Streimikis, J. (2019). Comparative review of corporate social responsibility of energy utilities and sustainable energy development trends in the Baltic States. Energies, 12(18), 3417. https://doi.org/10.3390/en12183417

[25] Markopoulou, D. (2023). Tackling cybersecurity challenges in the energy and water sectors in the context of the cybersecurity and sectoral regulatory frameworks: the case of smart metering systems in the new digitalised environment. International Review of Law, Computers & Technology, 37(1), 52-77. https://doi.org/10.1080/13600869.2022.2094609

[26] Markopoulou, D. (2023). Tackling cybersecurity challenges in the energy and water sectors in the context of the cybersecurity and sectoral regulatory frameworks: the case of smart metering systems in the new digitalised environment. International Review of Law, Computers & Technology, 37(1), 52-77. https://doi.org/10.1080/13600869.2022.2094609

[27] Mladenov, V., Chobanov, V., Sarigiannidis, P., Radoglou-Grammatikis, P. I., Hristov, A., & Zlatev, P. (2020). Defense against cyber-attacks on the Hydro Power Plant connected in parallel with Energy System," 2020 12th Electrical Engineering Faculty Conference (BulEF), Varna, Bulgaria, 2020, pp. 1-6. https://doi.org/10.1109/BulEF51036.2020.9326016

[28] Mohamed, N., El-Guindy, M. E., Oubelaid, A., & Almazrouei, S. K. (2023). Smart Energy Meets Smart Security: A Comprehensive Review of AI Applications in Cybersecurity for Renewable Energy Systems. International Journal of Energy and Environmental Research, 11(3). 728-732. https://doi.org/10.37391/ijeer.110313

[29] Mohamed, N., El-Guindy, M., Oubelaid, A., & khameis Almazrouei, S. (2023). Smart Energy Meets Smart Security: A Comprehensive Review of AI Applications in Cybersecurity for Renewable Energy Systems. International Journal of Electrical and Electronics Research, 11(3), 728-732. https://doi.org/10.37391/ijeer.110313

[30] Mudaliyar, M., Sharma, A., & Panja, A. (2022). Strategies for Reducing Greenhouse Gas Emissions and Promoting Renewable Energy. Journal of Universal Community Empowerment Provision, 2(2), 45-51. https://doi.org/10.55885/jucep.v2i2.207

[31] Mujević, M. (2022). Synthesis of Threats and Risks of Cyber Security of Montenegro - The Vulnerability Aspect of Information Communication Infrastructure, Science Journal, 1(1), 1-12.https://doi.org/10.35120/sciencej010101m

[32] Mukherjee, S. (2019). Implementing Cybersecurity in the Energy Sector. Available at SSRN 3441974. https://doi.org/10.2139/ssrn.3441974

[33] Nasir, S. (2023). Exploring the effectiveness of cybersecurity training programs: factors, best practices, and future directions. In Proceedings of the Cyber Secure Nigeria Conference, pp. 151-160. https://dx.doi.org/10.22624/aims/csean-smart2023p18

[34] Nazare, T., Nardo, L., Arias-Garcia, J., & Nepomuceno, E. (2023). Ensuring Resilience in Ocean Energy Power Plants: A Survey of Cybersecurity Measures. In Proceedings of the European Wave and Tidal Energy Conference (Vol. 15). https://doi.org/10.36688/ewtec-2023-452

[35] Ohalete, N. C., Aderibigbe, A. O., Ani, E. C., & Efosa, P. (2023). AI-driven solutions in renewable energy: A review of data science applications in solar and wind energy optimization. World Journal of Advanced Research and Reviews, 20(3), 401-417. https://doi.org/10.30574/wjarr.2023.20.3.2433

[36] Ohalete, N. C., Aderibigbe, A. O., Ani, E. C., Efosa, P. O. & Akinoso A.E. (2023). Data Science in Energy Consumption Analysis: A Review of AI Techniques in Identifying Patterns and Efficiency Opportunities, 4(6), 357-380. https://doi.org/10.51594/estj.v4i6.637

[37] Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. World Journal of Advanced Research and Reviews, 21(01), 2286–2295. https://doi.org/10.30574/wjarr.2024.21.1.0315.

[38] Oyekale, J., Petrollese, M., Tola, V., & Cau, G. (2020). Impacts of Renewable Energy Resources on Effectiveness of Grid-Integrated Systems: Succinct Review of Current Challenges and Potential Solution Strategies. Energies, 13(18), 4856. https://doi.org/10.3390/EN13184856

[39] Rahardja, U., Devana, V. T., Santoso, N., Oganda, F. P., & Hardini, M. (2022). Cybersecurity for FinTech on Renewable Energy from ACD Countries," 2022 10th International Conference on Cyber and IT Service Management (CITSM), Yogyakarta, Indonesia, 2022, pp. 1-6. https://doi.org/10.1109/CITSM56380.2022.9935855

[40] Raissouni, K., Erra1 1 bih, Z., Charroud, S., Raissouni, R., Raissouni, M., Bourekkadi, S., & Maroc Mohamed Ben Abdellah. (2023). Cybersecurity in the Context of Moroccan Energy Companies. E3S Web of Conferences, 412, 01038. https://doi.org/10.1051/e3sconf/202341201038

[41] Rambabu, M., Nuvvula, R. S. S., Kumar, P. P., Mounich, K., Loor-Cevallos, M. E., & Gupta, M. K. (2023). Integrating Renewable Energy and Computer Science: Innovations and Challenges in a Sustainable Future," 2023 12th International Conference on Renewable Energy Research and Applications (ICRERA), Oshawa, ON, Canada, pp. 472-479. https://doi.org/10.1109/ICRERA59003.2023.10269392

[42] Rekeraho, A., Cotfas, D., Cotfas, P., Balan, T., Tuyishime, E., & Acheampong, R. (2023). Cybersecurity challenges in IoT-based smart renewable energy. Information Systems Frontiers, pp. 1-15. https://doi.org/10.1007/s10207-023-00732-9

[43] Ricciardi, C.L., & Valli, A. (2023). Applied Control and Artificial Intelligence for Energy Management: An Overview of Trends in EV Charging, Cyber-Physical Security and Predictive Maintenance. Energies, 16(12), 4678. https://doi.org/10.3390/en16124678

[44] Ríos-Ocampo, J. P., Arango-Aramburo, S., & Larsen, E. R. (2021). Renewable energy penetration and energy security in electricity markets. International Journal of Energy Research, 45(12), 17767-17783. https://doi.org/10.1002/er.6897

[45] Saleem, D., Sundararajan, A., Sanghvi, A., Rivera, J., Sarwat, A., & Kroposki, B. (2020). A Multidimensional Holistic Framework for the Security of Distributed Energy and Control Systems," in IEEE Systems Journal, 14(1), 17-27. https://doi.org/10.1109/JSYST.2019.2919464

[46] Sharma, M. A., & Saraswat, P. (2021). Review of the Literature on Smart Grid Cybersecurity. International Journal of Innovative Research in Computer Science & Technology (IJIRCST), 9(6), 253-256. https://doi.org/10.55524/ijircst.2021.9.6.56

[47] Simonovich, L. (2020). Cyber Security Incident Response in the Utility Sector. In Abu Dhabi International Petroleum Exhibition and Conference (p. D021S042R003). SPE. https://doi.org/10.2118/203220-ms

[48] Smith, D. C. (2018). Enhancing cybersecurity in the energy sector: a critical priority. Journal of Energy & Natural Resources Law, 36(4), 373-380. https://doi.org/10.1080/02646811.2018.1516362

[49] Tarasova, A., Sutyrina, O., & Krayneva, R. (2021). Technological Solutions for Renewable Energy (Automation, Blockchain, and Smart Cities). In Second Conference on Sustainable Development: Industrial Future of Territories (IFT 2021), pp. 45-49. Atlantis Press. https://doi.org/10.2991/aebmr.k.211118.009

[50] Timčenko, V., Rakas, S. B., Kabović, M., & Kabović, A. (2023). Digitalization in Power Energy Sector: Principles of Cybersecurity, 30th International Conference on Systems, Signals and Image Processing (IWSSIP), Ohrid, North Macedonia, 2023, pp. 1-5. https://doi.org/10.1109/IWSSIP58668.2023.10180280

[51] Tobar Rosero, O. A., Pérez González, E., Botero Vega, J. F., Zapata Madrigal, G. D., Roa, O., Candelo-Becerra, J., & GarcÍa Sierra, R. (2023). Digital Substations and Cybersecurity in the Transformation of the Electricity Sector, IEEE Colombian Caribbean Conference (C3), Barranquilla, Colombia, 2023, pp. 1-6. https://doi.org/10.1109/C358072.2023.10436315

[52] Trifunović, D., & Bjelica, Z. (2021). Cyber War - Trends and Technologies. National Security & the Future, 21(3). https://doi.org/10.37458/NSTF.21.3.2

[53] Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: state of the art, trends and future directions. International Journal of Information Security, 22, 737-748. https://doi.org/10.1007/s10207-023-00660-8

[54] Tuyen, N. D., Quan, N. S., Linh, V. B., Tuyen, V. V., & Fujita, G. (2022). A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System amid the Boom of Renewable Energy," in IEEE Access, vol. 10, pp. 35846-35875. https://doi.org/10.1109/access.2022.3163551

[55] Venkatachary, S. K., Alagappan, A., & Andrews, L. J. B. (2021). Cybersecurity challenges in energy sector (virtual power plants)-can edge computing principles be applied to enhance security? Energy Informatics, 4(1), 5. https://doi.org/10.1186/s42162-021-00139-7

[56] Xiong, Y., Liu, R., Hao, S., Binti Md Nor, D. M., Guo, H., & Song, A. (2023). Quantifying Sustainable and Reliable Urban Microgrid Energy Solutions: Probabilistic Analysis of Renewable Adoption, Economic Viability, and Technological Innovations. Sustainable Cities and Society, 101,105157. https://doi.org/10.1016/j.scs.2023.105157

[57] Xue, J., Fan, H., & Yue, G. (2020). The Emerging Trends of Risk Management in Renewable Energy Projects. IOP Conference Series: Earth and Environmental Science, 586(1), 012014. https://doi.org/10.1088/1755-1315/586/1/012014

[58] Yeremyan, A., & Yeremyan, L. (2022). International Law Issues of Cyber Defense. Moscow Journal of International Law, (2), 85-100. https://doi.org/10.24833/0869-0049-2022-2-85-100.