OPEN ACCESS
Computer Science & IT Research Journal
P-ISSN: 2709-0043, E-ISSN: 2709-0051
Volume 5, Issue 5, P.1048-1075, May 2024
DOI: 10.51594/csitrj.v5i5.1115
Fair East Publishers
Journal Homepage: www.fepbl.com/index.php/csitrj

Innovation green technology in the age of cybersecurity: Balancing sustainability goals with security concerns

Excel G Chukwurah[1], Chukwuekem David Okeke[2], & Cynthia Chizoba Ekechi[3]

[1]Governance and Protected Data Organization, Google LLC, USA
[2]Tranter IT Infrastructure Services Limited, Nigeria
[3]Zustech Ltd, UK

*Corresponding Author: Excel G Chukwurah
Corresponding Author Email: chukwurah.excel@gmail.com
Article Received: 10-01-24 **Accepted:** 15-03-24 **Published:** 05-05-24

ABSTRACT

This study explores the critical intersection of cybersecurity measures and green technologies, aiming to assess their combined impact on sustainability goals and stakeholder implications. Employing a systematic literature review methodology, the research scrutinizes peer-reviewed journals, conference proceedings, and reports from reputable databases, focusing on publications from the year 2010 to 2024. The review identifies key themes, including the integration challenges and opportunities of cybersecurity within sustainable technologies, the evolving landscape of cybersecurity protocols, and the strategic implications for industry leaders, policymakers, and technologists. Key insights reveal the dual imperative of pursuing sustainability alongside security, highlighting the necessity of integrating robust cybersecurity measures without compromising the environmental benefits of green technologies. The study identifies significant challenges at this nexus, such as the rapid evolution of cyber threats and the complexity of embedding cybersecurity

in green innovations. It also outlines opportunities for innovation and the development of a security-aware culture that supports environmental sustainability. Strategic recommendations are provided for stakeholders to navigate these complexities, emphasizing the importance of multidisciplinary approaches, continuous learning, and the development of policies that encourage the adoption of secure and sustainable technologies. The study concludes that fostering innovation in green technology requires a concerted effort to integrate cybersecurity measures effectively, underscoring the need for future research to expand the knowledge frontiers in this critical area. This research contributes to the ongoing dialogue on achieving environmental sustainability and technological resilience, offering a foundation for further exploration and action towards these dual objectives.

Keywords: Cybersecurity, Green Technologies, Sustainable Technological, Stakeholder Security Concerns.

INTRODUCTION

The Intersection of Green Technology and Cybersecurity: A New Frontier

The intersection of green technology and cybersecurity represents a novel frontier in the quest for sustainable development. As the world grapples with the dual challenges of environmental sustainability and digital security, the convergence of these domains has become increasingly critical. Green technology, aimed at mitigating the impacts of human activity on the environment, encompasses a wide range of innovations designed to promote energy efficiency, reduce carbon emissions, and conserve natural resources. Cybersecurity, on the other hand, focuses on protecting information systems, networks, and data from digital attacks. The integration of these fields is essential in the development of sustainable technologies that are not only environmentally friendly but also secure against cyber threats.

The concept of adaptive cybersecurity in green Internet of Things (IoT) environments exemplifies this intersection (Halabi, Bellaïche, & Fung, 2022). The proliferation of IoT devices in various sectors, including smart grids, renewable energy systems, and precision agriculture, has underscored the need for energy-efficient security solutions. Adaptive cybersecurity approaches, which adjust to the changing threat landscape while minimizing energy consumption, offer a promising pathway to secure green technologies. These approaches not only protect IoT devices from cyberattacks but also contribute to the reduction of the carbon footprint associated with digital security measures

Moreover, the application of green cybersecurity principles in the transportation sector illustrates the potential for sustainable development through the integration of cybersecurity and green technology (Al-Dosari, Fetais, & Kucukvar, 2023). By adopting green cybersecurity strategies, transportation companies can enhance the security of their operations while promoting environmental sustainability. This dual focus not only supports the triple bottom line of economic, environmental, and social sustainability but also aligns with global efforts to combat climate change and cyber threats.

The agriculture and food industries further highlight the critical role of cybersecurity in supporting sustainable practices. With the advent of Agriculture 4.0, the sector has seen significant

technological advancements aimed at increasing food production and ensuring food security. However, these technologies also introduce new cybersecurity risks that could undermine sustainability efforts (Nobles, Burrell, Waller, & Cusak, 2022). Addressing these risks through cyberbiosecurity measures, which combine biosecurity and cybersecurity, is essential to protect the agriculture and food industries from cyberattacks while promoting sustainable food production.

In summary, the intersection of green technology and cybersecurity presents a new frontier that requires careful navigation. By integrating adaptive cybersecurity measures with green technologies, it is possible to achieve sustainability goals while ensuring the security of digital infrastructures. This balance is crucial for the development of sustainable technologies that are resilient to cyber threats, supporting global efforts to address environmental challenges and enhance digital security. As this field continues to evolve, further research and collaboration between industry, government, and academia will be essential to advance the integration of green technology and cybersecurity.

Defining the Landscape: Sustainability Meets Security

In the contemporary landscape where sustainability intersects with security, a nuanced understanding of both domains is imperative. The quest for sustainability, particularly in the context of the green energy transition, has underscored the critical role of lithium as a cornerstone for renewable energy technologies, including plug-in electric vehicles and grid-scale energy storage systems. Graham, Rupp, and Brungard (2021) highlight the dichotomy between the pursuit of sustainability and the emergent energy security risks, particularly given the geopolitical dynamics surrounding lithium supply chains. The dominance of certain countries in the lithium market introduces a complex layer of energy security concerns, juxtaposing the sustainability benefits of lithium-based technologies against the vulnerabilities of global supply chains. This scenario exemplifies the intricate balance between advancing green technologies and mitigating associated security risks, a theme that resonates across the spectrum of sustainable technologies.

Parallel to the challenges in the energy sector, the agriculture and food industries face their own set of cybersecurity risks, exacerbated by the advent of Agriculture 4.0 and smart farming technologies. Nobles, Burrell, Waller, and Cusak (2022) delve into the concept of cyberbiosecurity, an integrated approach that addresses the cybersecurity threats inherent in the digital transformation of agriculture. This approach is pivotal in safeguarding the food supply chain from cyber-attacks while ensuring the sustainability of agricultural practices. The intersection of cybersecurity and sustainability in agriculture illustrates the broader theme of securing critical infrastructure against cyber threats without compromising on environmental and sustainability goals.

The electrification of the transportation sector, particularly through the adoption of electric vehicles (EVs), represents another frontier where sustainability goals are intertwined with cybersecurity concerns. Muhammad et al. (2023) provide a comprehensive analysis of the cybersecurity and privacy threats facing the EV ecosystem. The vulnerabilities inherent in the digital technologies that underpin EVs not only pose risks to privacy and security but also have implications for environmental sustainability. The authors underscore the importance of developing robust cybersecurity measures that can protect against these threats while supporting

the sustainability objectives of the EV industry. This alignment of cybersecurity defenses with sustainability goals is crucial for the transition towards secure and sustainable smart cities.

The landscape where sustainability meets security is characterized by a dynamic interplay of challenges and opportunities. The examples from the energy, agriculture, and transportation sectors illustrate the critical need for an integrated approach that addresses cybersecurity risks in the context of sustainable development. By navigating this complex terrain, stakeholders can harness the potential of green technologies while ensuring the resilience and security of these systems against cyber threats. This dual focus on sustainability and security is essential for advancing towards a future where technological innovation and environmental stewardship go hand in hand.

Historical Overview: The Parallel Evolution of Green Technologies and Cybersecurity Measures

The historical evolution of green technologies and cybersecurity measures unfolds as a narrative of parallel and sometimes intersecting developments. This journey through time reveals how the maturation of these fields has been influenced by societal needs, technological advancements, and global challenges.

The genesis of green technologies can be traced back to the industrial revolution when the first seeds of environmental consciousness were sown in response to the visible impacts of industrialization on the natural world. However, it wasn't until the latter half of the 20th century that green technologies began to emerge as a formalized field, driven by the growing awareness of environmental degradation and the global push for sustainable development (Shevchuk, Oinas-Kukkonen, & Oinas-Kukkonen, 2017). The oil crises of the 1970s further accelerated this trend, prompting research and investment into alternative energy sources, recycling technologies, and energy-efficient systems. This period marked the beginning of a concerted effort to align technological innovation with environmental sustainability, laying the groundwork for the green technology revolution.

Parallel to the evolution of green technologies, the concept of cybersecurity emerged from the shadows of the Cold War, initially rooted in the need to protect information and communication systems from espionage and sabotage. The development of the internet and digital technologies in the late 20th century transformed cybersecurity from a niche concern of governments and militaries to a global imperative (Fouad, 2018). The proliferation of cyber-physical systems and the Internet of Things (IoT) has further blurred the lines between the physical and digital worlds, making cybersecurity an integral component of modern technological systems.

The intersection of green technologies and cybersecurity became increasingly prominent with the advent of smart grids, renewable energy systems, and sustainable urban development projects. These systems, characterized by their reliance on digital technologies for optimization and control, introduced new cybersecurity challenges. The need to protect these systems from cyber threats without compromising their environmental benefits has led to the development of green cybersecurity measures—strategies and technologies designed to secure digital infrastructure while adhering to principles of sustainability (Atat et al., 2018; Ehimuan et al., 2024).

The historical journey of green technologies and cybersecurity measures reflects a broader narrative of technological evolution driven by human needs and aspirations. From the early efforts to mitigate the environmental impacts of industrialization to the contemporary challenges of securing cyber-physical systems, the parallel evolution of these fields underscores the complexity of navigating the twin imperatives of sustainability and security. As we move forward, the lessons learned from this history will be crucial in guiding the development of technologies that are not only secure and sustainable but also resilient and adaptable to the changing global landscape.

Application of Cybersecurity in Smart Water Management Systems

Smart water management systems, pivotal in the realm of sustainable green technologies, are increasingly integrating cybersecurity measures to safeguard critical infrastructure. Drawing upon recent studies, such as those by Olatunde et al. (2024), there is a clear demonstration of how cybersecurity has become essential in enhancing both the sustainability and security of water management technologies across Africa and the United States. This integration faces specific security challenges, particularly in remote monitoring systems which are critical for real-time data and operational efficiency. As highlighted by Adelani et al. (2024), the lessons learned from Africa-US collaborative projects reveal the importance of adopting advanced security protocols that not only ensure operational reliability but also guard against emerging cyber threats.

Further exploration into the integration of cybersecurity within these systems reveals its impact on safety practices and urban resilience. For instance, Adelani et al. (2024) discuss the implementation of theoretical frameworks for electrical safety practices in water treatment facilities, which are crucial for preventing cyber-physical threats. Additionally, the role of AI and machine learning in enhancing water cybersecurity has proven transformative, as these technologies help predict, detect, and mitigate cyber threats, thereby supporting the sustainability of these infrastructures. The exploration of urban resilience through smart water grids in various case studies from African and US cities, as discussed by Adelani et al. (2024), showcases how cybersecurity measures are essential components of urban planning and disaster preparedness, further emphasizing the critical need for integrating robust cybersecurity measures into green technologies.

Aim and Objectives

The aim of the study is to evaluate the integration of cybersecurity measures within green technologies, assessing the impact on sustainability goals, and identifying the implications for industry, government, and public stakeholders

The objectives of the study are;

- To understand the intersection of green technology and cybersecurity
- To analyze the impact of cybersecurity on sustainable technological advancements
- To explore trends in cybersecurity protocols for sustainable technologies

Research Gap

Despite the growing body of literature on the integration of cybersecurity measures within green technologies, a notable research gap persists in understanding the dynamic interplay between evolving cybersecurity threats and the rapid advancement of sustainable technologies. Specifically, there is a lack of comprehensive studies that explore the real-world implications of cybersecurity

protocols on the operational efficiency and environmental impact of green technologies across different sectors. Furthermore, while existing research has begun to address the implications for stakeholders such as industry, government, and the public, there is a scarcity of empirical evidence detailing how these groups can effectively collaborate to enhance both security and sustainability outcomes. This gap underscores the need for multidisciplinary research that not only examines the technical aspects of cybersecurity in green technologies but also considers the socio-economic and policy dimensions that influence the adoption and effectiveness of these measures. Addressing this research gap is crucial for developing robust, adaptive security frameworks that can support the sustainable growth of green technologies in a rapidly evolving digital landscape.

METHODOLOGY

The methodology section outlines the systematic literature review process employed to investigate the integration of cybersecurity measures within green technologies, assessing their impact on sustainability goals, and understanding the implications for various stakeholders.

Sources of Information

The primary data sources for this study included peer-reviewed journals, conference proceedings, and reports from reputable databases such as IEEE Xplore, ScienceDirect, and the Web of Science. These sources were chosen for their comprehensive coverage of topics related to cybersecurity, green technologies, and sustainable development.

Search Strategy: Identifying Interdisciplinary Research

A structured search strategy was employed to identify relevant literature. Keywords and phrases used in the search included "cybersecurity and green technology," "sustainable technology and security," "adaptive security for sustainable systems," and "standards and policies in green tech." Boolean operators (AND, OR) were used to combine search terms effectively. The search was limited to documents published in English from 2010 to 2024, to focus on the most recent advancements and discussions in the field.

Inclusion and Exclusion Criteria: Filtering the Relevant Body of Work

The literature review adhered to specific inclusion criteria, focusing on peer-reviewed articles and conference papers that delve into the integration of cybersecurity measures with green technologies, discuss the impact of cybersecurity on sustainable technological advancements, address standards, policies, and regulations affecting green technology and cybersecurity, and provide insights into stakeholder implications. Conversely, the exclusion criteria ruled out non-peer-reviewed articles, opinion pieces, editorials, studies published before 2010, articles not in English, and research focusing solely on cybersecurity or green technology without addressing their integration.

Selection Process: Prioritizing Quality and Relevance

The selection process involved two phases: an initial screening based on titles and abstracts to identify potentially relevant articles, followed by a full-text review to confirm their relevance to the study's aim and objectives. The criteria for selection during the full-text review included the depth of discussion on the integration of cybersecurity and green technologies, the presence of case studies or empirical data, and the contribution of the study to understanding stakeholder implications

Analytical Framework: Assessing the Intersection of Green Technology and Cybersecurity

Data extracted from the selected articles included authors, year of publication, study objectives, methodology, key findings, and implications for stakeholders. A thematic analysis was conducted to identify common themes and trends across the literature. This involved coding the data based on predefined themes related to the study's objectives, such as "impact of cybersecurity on sustainable technologies," "adaptive security measures," and "stakeholder implications." The analysis also considered emerging themes that were not initially identified. The findings were synthesized to provide a comprehensive overview of the current state of knowledge on the integration of cybersecurity measures with green technologies and their implications for sustainability goals and stakeholders.

CORE CONCEPTS AND THEORETICAL FRAMEWORK

Understanding Green Technology: Principles and Practices

Green technology, also known as sustainable technology, takes into account the long-term impact of environmental sustainability. It incorporates innovations that are designed to mitigate or reverse the effects of human activity on the environment. The principles of green technology are rooted in sustainability, resource efficiency, and the minimization of pollution. Practices within this domain are diverse, ranging from renewable energy systems to eco-friendly manufacturing processes. This section delves into the principles and practices underpinning green technology, guided by recent scholarly contributions.

The integration of Lean and Green manufacturing practices exemplifies a practical application of green technology principles. Hallam and Contreras (2016) discuss the synergistic relationship between Lean manufacturing, which focuses on waste reduction and efficiency, and Green manufacturing, which emphasizes environmental sustainability. Their study illustrates how companies can leverage the interrelation of Lean and Green practices to achieve competitive advantage while adhering to sustainable development goals. This approach not only enhances organizational performance but also contributes to environmental preservation by minimizing waste and reducing the carbon footprint of manufacturing activities.

In the realm of information systems, the governance of Green Information Technologies (IT) represents a critical aspect of green technology practices. Flaih (2022) explores the significance of Green IT governance, highlighting the necessity for organizations to adopt environmentally sensitive IT strategies. Green IT practices, such as energy-efficient data centers, sustainable software development, and e-waste management, are pivotal in reducing the environmental impact of digital technologies. Flaih (2022) underscores the importance of a structured framework for Green IT governance, ensuring that organizations can effectively implement sustainable IT strategies that align with broader environmental objectives.

The principles of green technology are fundamentally aligned with the concept of sustainability, which entails meeting present needs without compromising the ability of future generations to meet their own. This principle is operationalized through practices that reduce energy consumption, utilize renewable resources, and minimize environmental degradation. The adoption of green technology practices, as illustrated by the integration of Lean and Green manufacturing

and the governance of Green IT, demonstrates a commitment to environmental stewardship and sustainable development.

In essence, understanding green technology involves a comprehensive appreciation of its principles and practices. The principles of sustainability, resource efficiency, and pollution reduction guide the development and implementation of green technologies. Practices such as the synergistic application of Lean and Green manufacturing and the governance of Green IT illustrate the practical realization of these principles. As the global community continues to grapple with environmental challenges, the role of green technology in facilitating sustainable development becomes increasingly paramount. The ongoing research and innovation in this field are essential for advancing our understanding and application of green technology, ensuring a sustainable future for all.

Cybersecurity Fundamentals in the Context of Sustainable Technologies

The integration of cybersecurity fundamentals with sustainable technologies is pivotal in today's digital era, where the reliance on technology-based solutions for environmental sustainability is ever-increasing. This integration is not only essential for protecting sensitive data and infrastructure but also for ensuring that the advancements in green technology are resilient to cyber threats.

Sadik et al. (2020) emphasize the growing necessity of a sustainable cybersecurity ecosystem, particularly in the realm of smart grids and the Internet of Things (IoT). The paper highlights the importance of identifying, characterizing, and classifying cyber threats to establish a secure cyber-ecosystem. The use of blockchain technology in IoT and smart cities is discussed as an emerging trend, alongside solutions based on artificial intelligence (AI) and machine learning (ML) to mitigate cyber risks (Aderibigbe et al., 2023; Adewusi et al., 2024; Reis et al., 2024; Ajala and Balogun, 2024; Ajayi-Nifise et al., 2024; Oguejiofor et al., 2023; Okunade et al., 2023). This comprehensive approach towards cybersecurity is crucial for safeguarding the infrastructure that underpins sustainable technologies, thereby ensuring their longevity and reliability.

The role of cybersecurity in achieving Sustainable Development Goals (SDGs) is critically analyzed by Odumesi and Sanusi (2023). Their work underscores the significance of cybersecurity measures in enhancing economic growth, promoting social inclusivity, and safeguarding environmental sustainability. As digital networks increasingly host critical infrastructure, key services, and personal data, the intersection of cybersecurity and sustainable development becomes apparent. The paper elucidates the potential synergies and interdependencies between cybersecurity and the SDGs, advocating for a secure, inclusive, and sustainable future facilitated by digital technologies.

Michael et al. (2019) delve into the ethical dimensions of technology deployment in achieving sustainable development goals, focusing on privacy, data rights, and cybersecurity. The paper argues for the inclusion of these three ethical elements in the deployment of new technologies, highlighting their role in maintaining the freedom and dignity of individuals. The rapid deployment of technology in developing nations, aimed at achieving the SDGs, presents both opportunities and challenges. The authors provide historical examples to demonstrate the positive

or negative applications of technology, emphasizing the need for ethical considerations in technology deployment.

Therefore, the fundamentals of cybersecurity play a crucial role in the context of sustainable technologies. The protection of digital infrastructure supporting green technologies is paramount to their success and resilience. The discussions by Sadik et al. (2020), Odumesi and Sanusi (2023), and Michael et al. (2019) collectively highlight the necessity of integrating cybersecurity measures with sustainable technologies. This integration not only ensures the protection of critical infrastructure and sensitive data but also supports the achievement of sustainable development goals. As the world continues to advance towards a more sustainable and digitally interconnected future, the importance of cybersecurity in this context cannot be overstated.

The Synergy between Environmental Sustainability and Digital Security

The convergence of environmental sustainability and digital security is a critical area of interest in the modern era, where technological advancements are both a boon and a bane for sustainable development. Goswami et al. (2023) delve into the role of cybersecurity in advancing sustainable digitalization, highlighting the growing trend of leveraging digital technology to promote environmental, social, and economic sustainability. The paper underscores the importance of cybersecurity as an integral component of sustainable digitalization, pointing out that cyber threats can significantly undermine sustainability efforts, leading to economic and social disruptions. The authors argue for the critical need to integrate cybersecurity with sustainable digitalization to protect and advance the objectives of both fields. They advocate for flexible cybersecurity policies and regulations that can adapt to the rapidly changing digital landscape and recommend a multi-stakeholder approach to cybersecurity, involving governments, businesses, and individuals.

Singh et al. (2022) and Ohalete et al. (2023) discuss the digitalization of the energy sector with a focus on sustainability, termed "Energy System 4.0." The study emphasizes the significance of digital technologies such as the Internet of Things (IoT), artificial intelligence (AI), edge computing, blockchain, and big data in achieving sustainability in energy generation, distribution, transmission, smart grid, and energy trading. The authors highlight the challenges and recommendations for the effective implementation of digital technologies in the energy sector to meet sustainability goals. They propose innovative solutions like big data analytics for energy, digital twins in smart grid modeling, virtual power plants with Metaverse, and green IoT as key recommendations for future enhancements.

Muhammad et al. (2023) provide a systematic analysis of the cybersecurity and privacy threats to electric vehicles (EVs) and their impact on human and environmental sustainability. The paper presents three robust taxonomies to identify the dangers that can affect long-term sustainability domains, including life and well-being, safe environment, and innovation and development. The research measures the impact of cybersecurity threats on EVs and their sustainability goals, detailing how specific security controls can mitigate these threats to ensure a secure and sustainable future for smart cities.

From the study, the synergy between environmental sustainability and digital security is pivotal for the advancement of sustainable digitalization. The integration of cybersecurity measures with sustainable technologies is essential to protect against cyber threats that can undermine

sustainability efforts. The discussions by Goswami et al. (2023), Singh et al. (2022), and Muhammad et al. (2023) collectively highlight the necessity of adopting flexible cybersecurity policies, engaging in multi-stakeholder approaches, and implementing innovative digital solutions to address the challenges and opportunities at the intersection of environmental sustainability and digital security. As the world continues to navigate the complexities of sustainable development in the digital age, the role of cybersecurity in safeguarding and advancing these efforts cannot be overstated.

Key Technological Innovations at the Nexus of Green Tech and Cybersecurity

The intersection of green technology and cybersecurity is a burgeoning field, driven by the imperative to address environmental challenges while ensuring digital security. Marra et al. (2017) investigate the emerging specializations and clusters in the green-tech industry, focusing on the network of technological innovation at the metropolitan level. Their study highlights the role of innovative start-ups and small and medium-sized enterprises (SMEs) in driving green-tech advancements. The analysis reveals that green-tech firms, characterized by significant intangible assets and technological uncertainty, are pivotal in fostering sustainable energy transitions. The spatial aggregation of these companies into clusters, as observed in San Francisco, New York, and London, underscores the importance of collaborative ecosystems in stimulating R&D activities and innovative production. This clustering strategy not only enhances the environmental performance of green technologies but also integrates cybersecurity measures to protect these innovations from cyber threats.

Gao et al. (2021) delve into the integrated development mode of green technology innovation, emphasizing the "Four Modernizations" framework—industrialization, marketization, informatization, and internationalization. This framework supports the development of green industries by facilitating the transformation and transfer of green technologies. The study underscores the significance of informatization, which includes cybersecurity as a critical component, in promoting the industrial ecology of green technologies. By designing a model for the integration and development of international green technology innovation, Gao et al. highlight the need for robust cybersecurity measures to safeguard the information infrastructure that underpins green tech innovations.

Zhang et al. (2023) address the role of technology innovations in achieving carbon neutrality among technologically advanced economies. Their research emphasizes the negative impact of green technological innovations and technological diffusions on carbon emissions, highlighting the significance of environmental policy in mitigating environmental vulnerabilities. The study suggests that climate tech, including cybersecurity technologies, is imperative to ensure carbon neutrality. The integration of cybersecurity measures in green technological innovations and diffusions is crucial for protecting these systems from cyber threats, thereby supporting the green growth agenda.

From the foregoing, the nexus of green technology and cybersecurity is marked by key technological innovations that address both environmental sustainability and digital security. The studies by Marra et al. (2017), Gao et al., (2021), and Zhang et al. (2023) collectively illustrate the importance of collaborative ecosystems, the "Four Modernizations" framework, and climate tech

in advancing this field. As the world progresses towards a more sustainable and digitally secure future, the integration of green technology and cybersecurity will continue to play a pivotal role in achieving these objectives.

Review of Current Trends: Smart Grids, Renewable Energy Systems, and Secure IoT Devices

The integration of smart grids, renewable energy systems, and secure Internet of Things (IoT) devices represents a significant trend in the pursuit of environmental sustainability and enhanced energy efficiency. Goudarzi et al. (2022) provide a comprehensive survey on IoT-enabled smart grids, emphasizing their role in making the electrical grid more intelligent and responsive to consumer needs. The study outlines the architecture and infrastructure of IoT-enabled smart grids and discusses the major challenges and security issues associated with their implementation. Given the vulnerability of smart grids to cyberattacks, the paper underscores the importance of advanced solutions and technologies, such as blockchain, to make IoT-enabled smart grids more resilient and secure. The integration of IoT devices in energy systems necessitates robust security measures to protect the grid from cyber-physical adversaries, thereby ensuring the reliability and efficiency of power systems.

Kumar Balam et al. (2023) explore the integration of renewable energy sources (RES) with IoT systems for smart grid applications. Their work presents a novel approach to incorporating RES using IoT and multilevel converters to enhance energy efficiency, reduce energy losses, and ensure reliable power distribution. The study highlights the potential of IoT devices to collect, process, and analyze data for improved grid control and monitoring of renewable energy installations. The use of multilevel converters optimizes power distribution and voltage management, demonstrating the efficacy of the proposed strategy in achieving an intelligent and energy-efficient grid.

Khare and Namekar (2020) discuss the utilization of renewable energy, IoT, and Hydro Pumped Energy Storage (HPES) systems in smart grids. The paper examines the role of smart grid technology in the efficient use of available energy sources and the integration of renewable energy to make the grid more promising. The inclusion of IoT technology in smart grids for clean energy and the exploration of storage solutions like HPES systems are highlighted as key components in enhancing the sustainability and efficiency of energy systems. The study also addresses the challenges of storage and the potential of HPES systems in overcoming these obstacles.

In summary, the current trends in smart grids, renewable energy systems, and secure IoT devices are shaping the future of energy consumption and distribution. The integration of these technologies offers promising solutions for achieving environmental sustainability, enhancing energy efficiency, and ensuring the security of energy systems. The discussions by Goudarzi et al. (2022), Kumar Balam et al. (2023), and Khare and Namekar (2020) illustrate the importance of innovative approaches and security measures in the development and implementation of smart grids and renewable energy systems. As these technologies continue to evolve, their integration will play a pivotal role in meeting the global demand for clean, efficient, and secure energy solutions.

Future Directions in Green Technology and Cybersecurity

The integration of Artificial Intelligence (AI) and the Internet of Things (IoT) within the realm of green energy signifies a transformative shift towards achieving Sustainable Development Goals (SDGs). Pant et al. (2023) explore the intersection of AI and IoT in the green energy sector, highlighting the application of these technologies in wind and solar energy, as well as in DC microgrids. The study underscores the challenges faced in deploying these technologies, such as energy efficiency, security, and accuracy. To overcome these challenges, the authors suggest strategies like carbon mitigation and the adoption of open data frameworks. The integration of AI models, such as Support Vector Regression (SVR) and Artificial Neural Network (ANN), into green energy systems presents a promising avenue for enhancing the performance and security of these systems. Predictive models based on AI can significantly contribute to the optimization of energy production and distribution, ensuring a sustainable and secure energy future.

Bian and Fu (2022) discuss the application of data mining in the predictive analysis of network security models. This study emphasizes the importance of data mining technology in identifying potential security vulnerabilities within network systems. The increasing number of security vulnerabilities highlights the need for advanced predictive models to preemptively address these threats. By applying data mining techniques to network security, stakeholders can develop more robust defense mechanisms against cyber-physical attacks, thereby safeguarding the infrastructure critical to sustainable systems.

Sarkadi, Moraru, and Manning (2023) propose the use of evolutionary agent-based modeling to predict the effects of adopting AI-based agricultural technologies. This approach offers a holistic perspective on complex ecosystems and their resilience to socio-economic pressures. The application of sustainable AI and agricultural technologies is crucial for addressing challenges such as climate change, food security, and biodiversity decline. Predictive models play a key role in exploring the emergence of strategies within the food sector, considering various levels of abstraction. This forward-looking approach enables the identification of sustainable practices that can be implemented to enhance both the productivity and security of agricultural systems.

In summary, the future of green technology and cybersecurity is intricately linked to the development and application of predictive models. These models offer valuable insights into optimizing the performance and security of sustainable systems. The studies by Pant et al. (2023), Bian and Fu (2022), and Sarkadi, Moraru, and Manning (2023) highlight the potential of AI, IoT, and data mining in advancing green technology and cybersecurity. As the world continues to navigate the challenges of sustainability and digital security, the role of predictive models in shaping a secure and sustainable future becomes increasingly paramount.

Predictive Models for Enhancing Security in Sustainable Systems

The integration of predictive models into the security frameworks of sustainable systems represents a forward-thinking approach to mitigating risks and enhancing operational efficiency. Merzhynskyi, Melikhova, and Makarenko (2019) discuss the improvement of a conceptual model for forecasting the economic security of industrial enterprises. The model combines the Kohonen neural network for classifying economic security levels with a predictive neural network model, facilitating the complex task of adapting indicators to improve an enterprise's economic security

level. This integration of predictive modeling into the economic security framework enables enterprises to identify negative trends and potential threats proactively, thereby ensuring sustainable development based on adaptive economic security levels.

Akdeniz and Bagriyanik (2023) present a preventive control approach for power system vulnerability assessment and predictive stability evaluation. Their work introduces an algorithm that selects critical contingencies through dynamic vulnerability analysis, utilizing a decision tree with a multi-parameter knowledge base. This approach allows for the early detection of potential cascading failures, proposing secure operational system states through vulnerability-based, security-constrained optimal power flow algorithms. The predictive model's modular structure enables the evaluation of vulnerable scenarios and the formulation of strategies to mitigate technical and economic impacts, thereby enhancing the sustainability and security of power systems.

Sen et al. (2023) explore the application of a predictive controller-based Energy Management System (EMS) and its techno-economic implications for an electrical-thermal community microgrid (MG). The study emphasizes the integration of renewable energy sources (RESs) and electric vehicles (EVs) within community MGs, forming a system of systems (SoS) architecture. The predictive controller optimizes component sizing and energy management, considering both technical and economic aspects. This approach ensures efficient energy use and load scheduling, coordinated EVs, and minimal fuel consumption, highlighting the predictive model's role in establishing secure and sustainable community MGs.

The studies by these authors illustrate the potential of predictive modeling in economic security, power system vulnerability assessment, and community microgrid management. As the demand for sustainable and secure systems continues to grow, the integration of predictive models into security frameworks will become increasingly vital. These models not only enable proactive threat identification and mitigation but also support the strategic development and implementation of sustainable practices across sectors.

Integration Challenges and Opportunities in Green Technologies

The integration of green technologies into existing systems presents a complex array of challenges and opportunities, particularly in the context of sustainable smart cities and green supply chain management. Almalki et al. (2021) discuss the integration of Internet of Things (IoT) technologies in smart cities, emphasizing the transition towards green IoT to create eco-friendly and sustainable urban environments. The authors highlight several challenges associated with green IoT, including increased energy consumption, toxic pollution, and e-waste generation. Despite these challenges, green IoT offers significant opportunities for reducing pollution hazards, managing resources and energy consumption efficiently, and enhancing public safety and life quality. The survey underscores the need for innovative techniques and strategies to overcome these challenges, making cities smarter, more sustainable, and eco-friendly. Furthermore, it points out the potential of IoT to merge into various aspects of smart cities, addressing the needs for sustainability.

Mehanneche and Zemmouchi-Ghomari (2022) explore the impact of technologies on green supply chain management (GSCM), identifying both facilitators and obstacles. The study emphasizes that supply chain management requires the integration and coordination of business processes and the

alignment of strategy, including environmental sustainability. Technological advancements such as artificial intelligence, cloud computing, the Internet of Things, and blockchain have drastically changed supply management methods. However, while these technologies offer opportunities to enhance GSCM, they also present challenges that need to be addressed. The authors suggest that further exploration of prominent case studies can shed light on how technologies can be effectively utilized to facilitate or hinder GSCM.

Magyari, Hegedűs, and Sinóros-Szabó (2022) examine the integration opportunities of power-to-gas (P2G) and IoT technical advancements, focusing on their strategic importance in renewable-rich grid developments. The study highlights how P2G applications, which produce and use green hydrogen, enable the integration of more renewable energy into the energy system. Meanwhile, IoT solutions could optimize renewable energy applications in decentralized systems. Despite the potential of both technologies to support renewable energy integration, the study identifies a research gap regarding their operative and strategic integration. The authors call for further empirical research on cost reduction, risk management, and policy incentives to support the integration of P2G and IoT in renewable energy systems.

The integration of green technologies into existing systems presents both challenges and opportunities. The discussions by Almalki et al. (2021), Mehanneche and Zemmouchi-Ghomari (2022), and Magyari, Hegedűs, and Sinóros-Szabó (2022) highlight the need for innovative solutions to overcome integration challenges. As the world moves towards a more sustainable future, the role of green technologies in smart cities, supply chain management, and renewable energy systems will become increasingly vital. Addressing the integration challenges and leveraging the opportunities will be crucial for achieving sustainability goals.

Optimizing Decision Support Systems for Sustainable Compliance in U.S. Green Technologies

This section critically examines the integration of decision support systems (DSS) in enhancing both sustainability and cybersecurity within the U.S. regulatory framework for green technologies. Utilizing the insights from Chukwurah et al. (2024), this analysis highlights the role of DSS in facilitating environmentally conscious project management that adheres to both environmental regulations and cybersecurity mandates. The adaptation of DSS in technology companies showcases how these systems support the strategic navigation of regulatory complexities, ensuring that projects not only comply with sustainable practices but also secure sensitive data.

Further exploration reveals the importance of aligning global data protection regulations, such as the CCPA and GDPR, with agile methodologies in the technology sector. The integration of such frameworks within agile practices, as detailed in the studies by Chukwurah et al. (2024), demonstrates how DSS can enhance compliance and sustainability simultaneously. This approach not only bolsters the resilience and security of green technologies but also supports their rapid adaptation to changing environmental and regulatory landscapes. Additionally, the role of technology project management systems (TPMS) in managing compliance within the regulatory boundaries, particularly in SaaS applications for green technologies, underscores the crucial function of DSS in balancing innovation, sustainability, and compliance.

By synthesizing these findings, this section sheds light on the indispensable role of decision support systems in ensuring that green technologies not only meet stringent security and privacy requirements but also advance environmental sustainability goals. The strategic application of DSS in navigating the dual challenges of maintaining robust security measures while promoting sustainable practices offers valuable insights for stakeholders in the technology sector, suggesting a path forward for integrating advanced technological solutions with environmental and regulatory demands.

IN-DEPTH ANALYSIS AND DISCUSSION

Evaluating the Impact of Cybersecurity on Sustainable Technological Advancements

The intersection of cybersecurity and sustainable technological advancements presents a complex landscape of challenges and opportunities. Kumari et al. (2024) delve into the integration of cybersecurity within the healthcare sector, particularly focusing on water remediation processes powered by sustainable smart grid (SG) energy analysis. The study introduces a novel approach that synergizes cybersecurity with bioprocessing techniques for energy-centric water remediation, utilizing a federated blockchain model for network security analysis. This innovative method demonstrates significant improvements in network integrity, throughput, scalability, and training accuracy, highlighting the critical role of cybersecurity in enhancing the sustainability and efficiency of water remediation efforts. The research underscores the necessity of advanced security solutions to protect the infrastructure essential for sustainable technologies, thereby ensuring their effective and safe application in critical sectors like healthcare.

Rautela et al. (2023) discuss the significance of technological advancements, including cybersecurity, in the transition to a green economy. The study emphasizes the role of exponential technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), Big Data Analytics, and Blockchain in achieving the Sustainable Development Goals (SDGs) set by the United Nations Environment Programme. The integration of these technologies, particularly cybersecurity measures, is crucial for ensuring the security and reliability of green technologies. By safeguarding the data and systems that underpin sustainable advancements, cybersecurity plays a pivotal role in facilitating the transition to a green economy, highlighting the interdependence between technological innovation and environmental sustainability.

Squillace, Hozella, and Cappella (2023) examine the relationship between cybersecurity awareness, eWaste reduction, and sustainable green computing practices. Their study identifies specific computing actions that contribute to eWaste and proposes ethical user actions that can reduce carbon output without compromising privacy or security. By fostering a secure foundation of cybersecurity awareness, the research suggests that consumers can adopt more sustainable computing practices, thereby contributing to the reduction of eWaste and supporting environmental sustainability. This approach not only enhances the security of computing systems but also aligns with the broader goals of sustainable technological advancements.

Therefore, the integration of cybersecurity measures into sustainable technologies is essential for ensuring their safe, efficient, and effective implementation. The studies by Kumari et al. (2024), Rautela et al. (2023), and Squillace, Hozella, and Cappella (2023) collectively highlight the multifaceted impact of cybersecurity on sustainable technological advancements. As the world

continues to navigate the challenges of sustainability and digital security, the role of cybersecurity in supporting and enhancing green technologies will become increasingly vital. Addressing cybersecurity concerns not only safeguards critical infrastructure but also facilitates the broader adoption and acceptance of sustainable technologies, thereby contributing to the global pursuit of environmental sustainability and a green economy.

Case Studies: Successes and Setbacks

The integration of cybersecurity measures into sustainable technologies is a critical endeavor, aiming to safeguard advancements while promoting environmental sustainability. Quader and Janeja (2021) provide a comprehensive evaluation of real-world cyber-attacks across multiple industries, identifying the characteristics and factors leading to these attacks. Their study reveals that human behavioral aspects are often the weakest link in preventing cyber threats, despite significant investments in cybersecurity. The case studies examined underscore the importance of a proactive approach to cybersecurity, emphasizing the need for organizations to learn from past incidents. By focusing on human factors and discussing mitigation strategies, this research highlights the critical role of cybersecurity awareness and training in enhancing the security readiness of organizations involved in sustainable technologies.

Okewu, Onobhayedo, and Moru (2023) propose a blockchain-based cybersecurity system aimed at engendering transparency and accountability in governance, with a focus on achieving the Sustainable Development Goals (SDGs). Using Nigeria as a case study, the paper illustrates how blockchain technology can address trust deficits caused by crime and criminality in cyberspace, thereby facilitating sustainable development. The implementation of this system demonstrates a successful integration of cybersecurity measures into sustainable development initiatives, showcasing the potential of technology to combat corruption and promote SDG 16, which is pivotal for the realization of other SDGs.

Muhammad et al. (2023) discuss the cybersecurity and privacy threats to electric vehicles (EVs) and their impact on human and environmental sustainability. The study presents three robust taxonomies to identify threats that can affect long-term sustainability domains, measuring the impact of cybersecurity threats on EVs and their sustainability goals. The research details how specific security controls can mitigate these threats, allowing for a secure transition towards sustainable future smart cities. This case study highlights both the challenges and opportunities in integrating cybersecurity with sustainable technologies, emphasizing the need for comprehensive security measures to protect against emerging threats.

In summary, the integration of cybersecurity and sustainable technologies presents a complex landscape of challenges and opportunities. The case studies by Quader and Janeja (2021), Okewu, Onobhayedo, and Moru (2023), and Muhammad, Anwar, Saleem, and Shahid (2023) illustrate the multifaceted nature of this integration, highlighting the importance of proactive cybersecurity measures, the potential of blockchain technology for sustainable development, and the need for robust security controls in the context of EVs. As the world continues to advance towards a more sustainable and digitally secure future, the lessons learned from these case studies will be invaluable in guiding the development and implementation of integrated cybersecurity and sustainable technologies.

Balancing Act: Security Measures vs. Environmental Impact

The integration of cybersecurity measures into sustainable technologies presents a complex balancing act between enhancing security and minimizing environmental impact. Saprykina (2023) discusses the technologies of environmental engineering protection within the context of sustainable architecture development, highlighting alternative approaches to creating eco-sustainable habitats. The study emphasizes the importance of integrating engineering proposals for waste disposal, seawater purification, and the transformation of urban waste into energy and materials. These technologies not only ensure sustainable waste management but also necessitate the incorporation of cybersecurity measures to protect the data and operational integrity of these systems. The challenge lies in implementing these security measures without significantly increasing the environmental footprint of the technologies involved.

Muhammad et al. (2023) examine the cybersecurity and privacy threats to electric vehicles (EVs) and their impact on human and environmental sustainability. The study presents a systematic analysis of the sustainability of EVs, highlighting the potential cybersecurity threats and the corresponding defense mechanisms. While EVs contribute to a sustainable environment by reducing emissions, the integration of digital technologies for enhanced sustainability exposes them to security and privacy threats. The research underscores the need for specific security controls to mitigate these threats, facilitating a secure transition towards sustainable future smart cities. The balancing act in this context involves implementing robust cybersecurity measures that do not compromise the environmental benefits of EVs.

Das et al. (2023) address the potential obstruction of greenwashing in promoting environmental sustainability through sustainable environmental technologies and green financing. The study assesses the impacts of green growth on environmental conditions in India, emphasizing the role of green technologies and financing in achieving environmental development targets. The findings suggest that while green technologies and financing initiatives promote environmental sustainability, the presence of greenwashing misleading claims about the environmental benefits of a product or technology can undermine these efforts. The challenge here is to ensure that the adoption of cybersecurity measures in green technologies and financing does not contribute to greenwashing, thereby genuinely supporting environmental sustainability.

In summary, the integration of cybersecurity measures into sustainable technologies requires a careful balance between enhancing security and minimizing environmental impact. The studies by Saprykina (2023), Muhammad, Anwar, Saleem, and Shahid (2023), and Das et al. (2023) highlight the complexities involved in this balancing act. As the world advances towards a more sustainable and digitally secure future, addressing these challenges will be crucial in ensuring that cybersecurity measures support rather than hinder the environmental benefits of sustainable technologies. Achieving this balance will necessitate innovative solutions that prioritize both security and environmental sustainability.

Trends in Cybersecurity Protocols for Sustainable Technologies

The integration of cybersecurity protocols into sustainable technologies is a critical aspect of ensuring the resilience and reliability of green innovations. Sadik et al. (2020) emphasize the importance of developing a sustainable cybersecurity ecosystem to address the increasing

cybersecurity challenges in technology-based economies. The paper discusses the cybersecurity of smart grids and the potential of blockchain technology in the Internet of Things (IoT) to enhance security measures. The study highlights emerging trends such as the use of artificial intelligence (AI) and machine learning (ML) frameworks to prevent cyber risks, underscoring the necessity of adapting security countermeasures to protect systems from cyber threats. This approach towards a sustainable cybersecurity ecosystem is crucial for providing a safe and secure environment for online users, thereby supporting the sustainable development of smart cities and other emerging technologies.

Srujana et al. (2022) survey cutting-edge technologies that contribute to an improved cybersecurity model, particularly in the context of Industry 4.0. The paper analyzes various technological advancements, including AI, IoT, and blockchain, and their role in enhancing cybersecurity measures. The study suggests that these technologies can lead to the sustainability of resources by processing networks and designing parameters to protect against unauthorized access. By integrating these advanced technologies into cybersecurity protocols, sustainable technologies can achieve higher levels of security, ensuring the effective and safe use of resources in automated and digitalized environments.

Jha (2023) focuses on the challenges and strategies associated with ensuring cybersecurity and confidentiality in smart grids to enhance sustainability and reliability. The research examines various techniques and technologies, such as encryption, authentication, intrusion detection, and secure communication protocols, that can be employed to safeguard smart grid infrastructure from cyber threats. By highlighting the significance of a robust cybersecurity framework and the integration of privacy-preserving measures, this study contributes to the development of secure and resilient smart grid systems. The findings provide valuable insights for policymakers, industry professionals, and researchers involved in designing and implementing secure solutions for smart grids, ultimately leading to the advancement of sustainable and reliable energy infrastructures.

In summary, the trends in cybersecurity protocols for sustainable technologies underscore the critical role of advanced technologies and innovative security measures in protecting green innovations. The discussions by Sadik et al. (2020), Srujana et al. (2022), and Jha (2023) illustrate the evolving landscape of cybersecurity, highlighting the importance of developing sustainable cybersecurity ecosystems, integrating cutting-edge technologies, and ensuring the confidentiality and security of smart grids. As sustainable technologies continue to advance, the integration of robust cybersecurity protocols will be paramount in ensuring their resilience, reliability, and contribution to a sustainable future.

Anticipating the Future: Adaptive Security for Evolving Green Technologies

The evolution of green technologies is intrinsically linked to the advancement of cybersecurity measures to protect these innovations. Adaptive security models, which dynamically adjust to emerging threats and vulnerabilities, are becoming increasingly crucial in safeguarding the integrity and sustainability of green technologies. Lindgren (2022) discusses the potential of 6G technologies in supporting future green business model innovation. The paper highlights the security challenges associated with green business models, such as the need to ensure that these models are genuinely sustainable and not based on greenwashing. With the demand for open

business model innovation, there arises a critical need for new and advanced security technologies to protect intellectual property rights and competences. The study suggests that 6G technologies, supported by AI, AR, and blockchain, could play a significant role in addressing these security challenges, thereby supporting society's green transformation. This evolution necessitates adaptive security measures that can respond to the unique and complex threats faced by green business models.

Aman (2016) evaluates the feasibility of adaptive security models for the Internet of Things (IoT), a key component of green technology ecosystems. The paper presents an evaluation framework that assesses adaptive security models from a risk management perspective, considering their ecosystem awareness and adaptation aptitude. This framework is crucial in determining the security and architectural capabilities of models in IoT settings, where the diversity and dynamism of technology and threats require flexible and responsive security solutions. The study underscores the importance of adaptive security in IoT-driven ecosystems, highlighting the need for models that can dynamically observe and respond to threats.

Ferrag et al. (2020) delve into the security and privacy challenges in green IoT-based agriculture, presenting a comprehensive review of blockchain solutions and challenges. The paper outlines a taxonomy of threat models against green IoT-based agriculture and discusses state-of-the-art methods for secure and privacy-preserving technologies. The study emphasizes the role of privacy-oriented blockchain-based solutions in enhancing the security and privacy of green IoT-based agriculture. This approach to adaptive security is particularly relevant in the agricultural sector, where the integration of green technologies and IoT applications presents unique security and privacy challenges.

From the foregoing, the future of adaptive security in the context of evolving green technologies is marked by the need for innovative solutions that can dynamically adjust to new threats and vulnerabilities. The discussions by Lindgren (2022), Aman (2016), and Ferrag et al. (2020) highlight the critical role of adaptive security models in ensuring the sustainability and integrity of green technologies. As these technologies continue to advance, the development and implementation of adaptive security measures will be paramount in safeguarding them against emerging cyber threats, thereby supporting the global pursuit of environmental sustainability.

Standards, Policies, and Regulations: Shaping the Future of Green Tech and Cybersecurity

The interplay between standards, policies, and regulations plays a pivotal role in shaping the future of green technology and cybersecurity. These frameworks not only guide the development and implementation of sustainable technologies but also ensure that these innovations are secure and resilient against cyber threats.

Chakwizira (2021) provides a comprehensive review of the regulatory frameworks, policies, norms, and standards within the transport sector, emphasizing the application of green transport lenses. The study outlines the impact and outcomes of governmental and non-governmental transport interventions from a green transport perspective. It highlights the critical role of norms and standards in promoting green transport policy, innovation, and activities. This analysis underscores the importance of regulatory frameworks in fostering sustainable transport solutions that are secure and environmentally friendly. The discussion on green transport issues within

Limpopo province serves as a case study for understanding the application and impact of these regulatory measures in promoting sustainable and secure transport systems.

Bortone, Sakar, and Soares (2022) analyze the gaps in regulation and policies concerning the application of green technologies at the household level in the United Kingdom. The study provides an overview of existing regulations and standards in the UK building/household sector to identify discrepancies preventing the wider implementation and use of green technologies. The analysis highlights the need for complete and clear guidelines that address environmental awareness, performance, and the economic convenience of green tech implementation. This research points to the critical role of regulatory frameworks in facilitating the adoption of green technologies, ensuring that these innovations contribute effectively to sustainability and Net-Zero targets while adhering to cybersecurity measures.

Zhang, Li, Shi, and Feng (2022) discuss the impact of environmental technology standards on the green transformation of the manufacturing industry in China. Employing a difference-in-differences (DID) model, the study examines the effects of cleaner production industry standard policies on environmental and economic performance. The findings reveal that environmental technology standards can promote the green transformation of the manufacturing industry by mediating the effects of terminal governance, capital renewal, and resource structure adjustments. This research underscores the significance of environmental technology standards in achieving a "win-win" scenario, where both environmental sustainability and economic performance are enhanced. The study suggests that updating environmental technology standards regularly is crucial for supporting the green transformation.

Therefore, standards, policies, and regulations are instrumental in shaping the future of green technology and cybersecurity. The discussions by Chakwizira (2021), Bortone, Sakar, and Soares (2022), and Zhang, Li, Shi, and Feng (2022) illustrate the multifaceted role of these frameworks in promoting sustainable and secure technologies. As the global community continues to advance towards a more sustainable and digitally secure future, the development and implementation of comprehensive regulatory frameworks will be paramount in ensuring the success of green technologies and cybersecurity measures.

Stakeholder Implications: Industry, Government, and Public Perspectives on Secure Sustainable Technologies

The integration of secure sustainable technologies is a multifaceted challenge that involves various stakeholders, including industry, government, and the public. Each group plays a crucial role in shaping the future of sustainable technologies, with distinct perspectives on security, innovation, and environmental impact. Roberts, Herkert, and Kuzma (2020) delve into the attitudes of stakeholders involved in biotechnology towards the Responsible Innovation (RI) framework, particularly in the context of genetically modified organisms (GMOs) in agriculture and the environment. The study reveals that while all stakeholder groups have neutral to positive attitudes towards the general principles of RI, significant differences exist in their reactions to the scholarly definitions of RI and attitudes towards its implementation practices. Industry stakeholders, trade organizations, and academics exhibit more negative reactions to social science definitions of RI and practices that relinquish control to external voices. This resistance underscores the tension

between the need for open innovation and the protection of intellectual property rights, highlighting the challenges of integrating security measures in sustainable technologies without stifling innovation.

Bonilla et al. (2018) analyze the sustainability impact and challenges of Industry 4.0 technologies, such as the Internet of Things, big data analytics, and cyber-physical systems. The paper presents a scenario-based analysis of the positive and negative impacts of these technologies on sustainability and the environment. The findings suggest that while Industry 4.0 technologies have the potential to contribute positively to sustainability goals, their implementation also poses significant challenges. For industry stakeholders, the key is to navigate these challenges by integrating Industry 4.0 with sustainable development goals in an eco-innovation platform to ensure environmental performance. This approach requires collaboration between industry, government, and the public to support the positive impacts through policies and financial initiatives.

Roehrl (2019) discusses the lessons from the COVID-19 pandemic for a better science-policy-society interface and a resilient, sustainable, and inclusive recovery. The paper emphasizes the importance of multi-stakeholder cooperation in addressing global challenges and the role of science, technology, and innovation (STI) in the recovery process. It highlights the need for responsive science advice mechanisms to improve the science-policy interface among governments, the UN system, stakeholders, including the scientific community, and the private sector. This cooperative action is crucial for advancing solutions to deal with the outcomes emerging from the massive adoption of technologies and supporting the expected positive impacts through policies and financial initiatives.

In summary, the perspectives of industry, government, and the public on secure sustainable technologies are interlinked, with each stakeholder group facing distinct challenges and opportunities. The discussions by Roberts, Herkert, and Kuzma (2020), Bonilla et al. (2018), and Roehrl (2019) highlight the importance of collaboration, open innovation, and responsive science advice mechanisms in integrating security measures with sustainable technologies. As the global community continues to advance towards a more sustainable and digitally secure future, understanding and addressing the implications for all stakeholders will be paramount in achieving environmental sustainability and technological resilience.

CONCLUSIONS

The study underscores the critical importance of simultaneously pursuing sustainability and security within the realm of green technologies. It highlights that the integration of cybersecurity measures into sustainable technologies is not merely a technical challenge but a strategic imperative that encompasses environmental, economic, and social dimensions. The findings reveal that while cybersecurity measures are essential for protecting green technologies from emerging threats, they must be implemented in a manner that does not compromise the environmental benefits of these technologies.

Looking forward, the intersection of green technology and cybersecurity presents both significant challenges and opportunities. Challenges include the rapid evolution of cyber threats, the complexity of integrating cybersecurity measures with existing and new green technologies, and the need for cross-sector collaboration. However, these challenges are accompanied by

opportunities to innovate in the development of secure, sustainable technologies and to foster a culture of security awareness that complements environmental sustainability efforts.

To effectively navigate the complexities at the intersection of green technology and cybersecurity, this study proposes a set of strategic recommendations tailored for key stakeholders. Industry leaders are encouraged to channel investments into research and development that prioritizes the integration of robust cybersecurity measures within green technologies. This involves not only the allocation of resources towards innovation in secure sustainable technologies but also the cultivation of partnerships with cybersecurity firms to ensure that protection measures are seamlessly integrated right from the design phase. For policymakers, the call to action involves the development and enforcement of policies and regulations that not only encourage the adoption of secure sustainable technologies but also offer incentives for companies that demonstrate a commitment to prioritizing both sustainability and security in their operations. This regulatory support is crucial for creating an enabling environment that fosters the growth of green technologies while ensuring their resilience against cyber threats. Technologists, on their hand, are urged to adopt a multidisciplinary approach that incorporates cybersecurity considerations into the development of green technologies. This includes a commitment to continuous learning and adaptation to stay abreast of the rapidly evolving landscape of cyber threats. By embracing these strategic recommendations, stakeholders across the board can contribute to fostering innovation in green technology, ensuring that advancements in this field are both sustainable and secure.

In summary, fostering innovation in green technology requires a concerted effort to integrate cybersecurity measures effectively. This study highlights the necessity of a holistic approach that considers the environmental, technological, and societal implications of secure sustainable technologies. By prioritizing both sustainability and security, stakeholders can unlock the full potential of green technologies to contribute to a more sustainable and secure future. As the digital and environmental landscapes continue to evolve, the insights from this study serve as a foundation for ongoing dialogue and action towards achieving these dual objectives.

Finally, the study identifies several areas for future research, including the development of advanced cybersecurity frameworks that can dynamically adapt to new threats and vulnerabilities, the exploration of the socio-economic impacts of integrating cybersecurity measures into green technologies, and the examination of cross-sectoral collaboration models that can enhance both security and sustainability outcomes. Further research in these areas will be crucial for expanding the frontiers of knowledge in green technology and cybersecurity, supporting the global pursuit of environmental sustainability and technological resilience.

References

Adelani, F.A., Okafor, E.S., Jacks, B.S., & Ajala, O.A. (2024). Theoretical insights into securing remote monitoring systems in water distribution networks: lessons learned from Africa-US Projects. *Engineering Science & Technology Journal*, 5(3), 995-1007.

Adelani, F.A., Okafor, E.S., Jacks, B.S., & Ajala, O.A. (2024). A review of theoretical frameworks for electrical safety practices in water treatment facilities: lessons learned from Africa and the United States. *Engineering Science & Technology Journal*, 5(3), 974-983.

Adelani, F.A., Okafor, E.S., Jacks, B.S., & Ajala, O.A. (2024). Exploring Theoretical Constructs of Urban Resilience through Smart Water Grids: Case Studies in African and US Cities. *Engineering Science & Technology Journal*, 5(3), 984-994.

Adelani, F.A., Okafor, E.S., Jacks, B.S., & Ajala, O.A. (2024). Theoretical frameworks for the role of AI and machine learning in water cybersecurity: insights from African and US applications. *Computer Science & IT Research Journal*, 5(3), 681-692.

Aderibigbe, A. O., Ani, E. C., Efosa, P. O. Ohalete, N. C., & Daraojimba, D.O. (2023). Enhancing energy efficiency with AI: a review of machine learning models in electricity demand forecasting. https://doi.org/10.51594/estj.v4i6.636.

Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA. *World Journal of Advanced Research and Reviews, 21*(1), 2263-2275. https://doi.org/10.30574/wjarr.2024.21.1.0313

Ajala, O.A., & Balogun, O. (2024). Leveraging AI/ML for anomaly detection, threat prediction, and automated response. *World Journal of Advanced Research and Reviews, 21*(1), 2584-2598. https://doi.org/10.30574/wjarr.2024.21.1.0287.

Ajayi-Nifise, A. O., Falaiye, T., Olubusola, O., Daraojimba, A. I., & Mhlongo, N. Z. (2024). Blockchain in US accounting: a review: assessing its transformative potential for enhancing transparency and integrity. *Finance & Accounting Research Journal, 6*(2), 159-182.

Akdeniz, E., & Bagriyanik, M. (2023). A preventive control approach for power system vulnerability assessment and predictive stability evaluation. *Sustainability, 15*(8), 6691. https://dx.doi.org/10.3390/su15086691

AL-Dosari, K., Fetais, N., & Kucukvar, M. (2023). A shift to green cybersecurity sustainability development: Using triple bottom-line sustainability assessment in Qatar transportation sector. *International Journal of Sustainable Transportation*, 1-15. DOI: 10.1080/15568318.2023.2171321

Almalki, F. A., Alsamhi, S. H., Sahal, R., Hassan, J., Hawbani, A., Rajput, N. S., ... & Breslin, J. (2023). Green IoT for eco-friendly and sustainable smart cities: future directions and opportunities. *Mobile Networks and Applications, 28*(1), 178-202. DOI: 10.1007/s11036-021-01790-w

Aman, W. (2016). Assessing the feasibility of adaptive security models for the internet of things. In human aspects of information security, privacy, and trust: 4th International Conference, HAS 2016, Held as Part of HCI International 2016, Toronto, ON, Canada, July 17-22, 2016, Proceedings 4 (pp. 201-211). Springer International Publishing. https://dx.doi.org/10.1007/978-3-319-39381-0_18

Atat, R., Liu, L., Wu, J., Li, G., Ye, C., & Yang, Y. (2018). Big data meet cyber-physical systems: A panoramic survey. *IEEE Access, 6*, 73603-73636. https://dx.doi.org/10.1109/ACCESS.2018.2878681

Bian, J., & Fu, S. (2022). Application of data mining in predictive analysis of network security model. *Security and Communication Networks, 2022*, Article ID 4922377, 8 pages, 2022. https://doi.org/10.1155/2022/4922377

Bonilla, S. H., Silva, H. R., Terra da Silva, M., Franco Gonçalves, R., & Sacomano, J. B. (2018). Industry 4.0 and sustainability implications: A scenario-based analysis of the impacts and challenges. *Sustainability, 10*(10), 3740. DOI: 10.3390/SU10103740

Bortone, I., Sakar, H., & Soares, A. (2022). Gaps in regulation and policies on the application of green technologies at household level in the United Kingdom. *Sustainability, 14*(7), 4030. DOI: 10.3390/su14074030

Chakwizira, J. (2022). Regulatory frameworks, policies, norms and standards. green economy in the transport sector, 79. DOI: 10.1007/978-3-030-86178-0_7

Chukwurah, E.G. (2024). Decision support systems reimagined: crafting project management solutions for the U.S. Market. *International Journal of Multidisciplinary Research Updates*. https://doi.org/10.53430/ijmru.2024.7.2.0034

Chukwurah, E.G., & Aderemi, S. (2024). Harmonizing teams and regulations: strategies for data protection compliance in U.S. technology companies. *Computer Science & IT Research Journal*. https://doi.org/10.51594/csitrj/v5i4.1044

Chukwurah, E.G. (2024). Agile privacy in practice: integrating CCPA and GDPR within agile frameworks in the U.S. tech scene. *International Journal of Scientific Research Updates*. https://doi.org/10.53430/ijsru.2024.7.2.0035

Chukwurah, E.G. (2024). Leading SaaS innovation within U.S. regulatory boundaries: the role of TPMS in navigating compliance. *Engineering Science & Technology Journal*. https://doi.org/10.51594/estj/v5i4.1039

Das, N., Gangopadhyay, P., Alam, M. M., Mahmood, H., Bera, P., Khudoykulov, K., ... & Hossain, M. E. (2024). Does greenwashing obstruct sustainable environmental technologies and green financing from promoting environmental sustainability? Analytical evidence from the Indian economy. *Sustainable Development, 32*(1), 1069-1080. DOI: 10.1002/sd.2722

Ehimuan, B., Anyanwu, A., Olorunsogo, T., Akindote, O. J., Abrahams, T. O., & Reis, O. (2024). Digital inclusion initiatives: Bridging the connectivity gap in Africa and the USA–A review. *International Journal of Science and Research Archive, 11*(1), 488-501. https://doi.org/10.30574/ijsra.2024.11.1.0061.

Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access, 8*, 32031-32053. https://dx.doi.org/10.1109/ACCESS.2020.2973178

Flaih, L. R. (2022). Information systems governance and green information technologies. 4th International Conference on Communication Engineering and Computer Science (Cic-Cocos'22) https://dx.doi.org/10.24086/cocos2022/paper.516

Fouad, N. S. (2018, June). Security as a context, generative force, and policy concern for the co-production of cyberspace: historical overview since WWII until the end of the Cold War.

In ECCWS 2018-Proceedings of the 17th European Conference on Cyber Warfare and Security. Academic Conferences and Publishing International. pp 507-514

Gao, Y., Sun, L., & Liu, X. (2021). An exploration into green-tech innovations based on "Four Modernizations". *Journal of Environmental Protection, 12*(01), 29. https://dx.doi.org/10.4236/JEP.2021.121003

Goswami, S. S., Sarkar, S., Gupta, K. K., & Mondal, S. (2023). The role of cyber security in advancing sustainable digitalization: Opportunities and challenges. *Journal of Decision Analytics and Intelligent Computing, 3*(1), 270-285. DOI: 10.31181/jdaic10018122023g

Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., & Traore, I. (2022). A survey on IoT-Enabled smart grids: emerging, applications, challenges, and outlook. *Energies, 15*(19), 6984. DOI: 10.3390/en15196984

Graham, J. D., Rupp, J. A., & Brungard, E. (2021). Lithium in the green energy transition: The quest for both sustainability and security. *Sustainability, 13*(20), 11274. DOI: 10.3390/su132011274

Halabi, T., Bellaiche, M., & Fung, B. C. (2022). Towards adaptive cybersecurity for green IoT. IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), BALI, Indonesia, 64-69. DOI: 10.1109/IoTaIS56727.2022.9975990

Hallam, C. R., & Contreras, C. (2016). The interrelation of Lean and green manufacturing Practices: A case of push or pull in implementation," 2016 Portland International Conference on Management of Engineering and Technology (PICMET), Honolulu, HI, USA, 1815-1823. DOI: 10.1109/PICMET.2016.7806669

Jha, R. K. (2023). Cybersecurity and confidentiality in smart grid for enhancing sustainability and reliability. *Recent Research Reviews Journal, 2*(2), 215-241. DOI: 10.36548/rrrj.2023.2.001

Khare, S., & Namekar, S. (2020). Smart grid using renewable energy, Iot and Hpes systems. *International Journal of Engineering Applied Sciences and Technology, 4*(12), 205-210. DOI: 10.33564/ijeast.2020.v04i12.031

Kumar Balam, S., Jain, R., Alaric, J. S., Pattanaik, B., & Ayele, T. B. (2023). Renewable Energy Integration of IoT Systems for Smart Grid Applications," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, 374-379. DOI:10.1109/ICESC57686.2023.10193428

Kumari, K. S., Ghorpade, V., Sami, F. M., Haleem, S. L. A., Kondaveeti, S., & Kiyosov, S. (2024). Synergizing cybersecurity in healthcare with novel bioprocessing for sustainable energy-centric water remediation. *Water Reuse, jwrd2024121*. DOI: 10.2166/wrd.2024.121

Lindgren, P. (2022). 6G Technologies – How Can It Help Future Green Business Model Innovation. *Journal of ICT Standardization, 10*(01), 11–38. https://doi.org/10.13052/jicts2245-800X.1012

Magyari, J., Hegedüs, K., & Sinóros-Szabó, B. (2022). Integration opportunities of power-to-gas and Internet-of-Things technical advancements: a systematic literature review. *Energies, 15*(19), 6999. DOI: 10.3390/en15196999

Marra, A., Antonelli, P., & Pozzi, C. (2017). Emerging green-tech specializations and clusters–A network analysis on technological innovation at the metropolitan level. *Renewable and Sustainable Energy Reviews, 67,* 1037-1046. DOI: 10.1007/978-3-319-60435-0_12

Mehanneche, K., & Zemmouchi-Ghomari, L. (2022). Green Supply Chain Management, Challenges, and Technological Opportunities. *International Journal of Information Systems and Social Change (IJISSC), 13*(1), 1-13. DOI: 10.4018/ijissc.303594

Merzhynskyi, Y., Melikhova, T., & Makarenko, A. (2019, September). Improvement of a conceptual model forecasting the level of economic security of industrial enterprise. In 6th International Conference on Strategies, Models and Technologies of Economic Systems Management (SMTESM 2019) (pp. 137-141). Atlantis Press. https://dx.doi.org/10.2991/smtesm-19.2019.27

Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019). Privacy, data rights and cybersecurity: technology for good in the achievement of sustainable development goals. *IEEE International Symposium on Technology and Society (ISTAS),* Medford, MA, USA, 2019, 1-13. DOI: 10.1109/istas48451.2019.8937956

Muhammad, Z., Anwar, Z., Saleem, B., & Shahid, J. (2023). Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability. *Energies, 16*(3), 1113. https://dx.doi.org/10.3390/en16031113

Muhammad, Z., Anwar, Z., Saleem, B., & Shahid, J. (2023). Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability. *Energies, 16*(3), 1113. DOI: 10.3390/en16031113

Nobles, C., Burrell, D. N., Waller, T., & Cusak, A. (2022). Food sustainability, cyber-biosecurity, emerging technologies, and cybersecurity risks in the agriculture and food industries. *International Journal of Environmental Sustainability and Green Technologies (IJESGT), 13*(1), 1-17. DOI: 10.4018/ijesgt.309744

Odumesi, J.O. & Sanusi, B.S. (2023): Achieving sustainable development goals from a cybersecurity perspective. proceedings of the cyber secure Nigeria conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria. 11-12th July, 2023. Pp 1-10 https://www.csean.org.ng/. dx.doi.org/10.22624/AIMS/CSEAN-SMART2023P3

Oguejiofor, B. B., Omotosho, A., Abioye, K. M., Alabi, A. M., Oguntoyinbo, F. N., Daraojimba, A. I., & Daraojimba, C. (2023). A review on data-driven regulatory compliance in Nigeria. *International Journal of Applied Research in Social Sciences, 5*(8), 231-243.

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

Okewu, E., Onobhayedo, P., & Moru, D. (2023). Attaining the sustainable development goals using blockchain-based cybersecurity. *Sustainable Social Development, 1*(3). https://dx.doi.org/10.54517/ssd.v1i3.2309

Okunade, B. A., Adediran, F. E., Bukola, A., Adewusi, O. E., & Daraojimba, R. E. (2023). Technological advancements in African social work: Implications for US

practice. *International Journal of Management & Entrepreneurship Research, 5*(12), 1012-1035. https://doi.org/10.51594/ijmer.v5i12.645

Olatunde, T.M., Adelani, F.A., & Sikhakhane, Z.Q. (2024). A review of smart water management systems from Africa and the United States. *Engineering Science & Technology Journal*, 5(4), 1231-1242.

Pant, S., Rawat, P., Kathuria, S., Singh, R., Chanti, Y., & Pachouri, V. (2023). Artificial Intelligence and Internet of Things Intersection in Green Energy," 2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT), Dehradun, India, 2023, 1-5. https://dx.doi.org/10.1109/CISCT57197.2023.10351314

Quader, F., & Janeja, V. P. (2021). Insights into organizational security readiness: Lessons learned from cyber-attack case studies. *Journal of Cybersecurity and Privacy, 1*(4), 638-659. https://dx.doi.org/10.3390/jcp1040032

Rautela, R., Kumar, S., Pandey, S., Prakash, N., Malik, P. K., & Kumar, A. (2023). Significance of Emerging Technological Advancements in Transition of Green Economy," 2023 IEEE Devices for Integrated Circuit (DevIC), Kalyani, India, 2023, 221-224. DOI: 10.1109/DevIC57758.2023.10134956

Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age: a global review of legislation and enforcement. *International Journal of Applied Research in Social Sciences, 6*(1), 73-88. https://doi.org/10.51594/ijarss.v6i1.733.

Roberts, P., Herkert, J., & Kuzma, J. (2020). Responsible innovation in biotechnology: Stakeholder attitudes and implications for research policy. Elem Sci Anth, 8, 47. DOI: 10.1525/elementa.446

Roehrl, R. (2019). Multi-stakeholder forum on science, technology and innovation for the Sustainable Development Goals. *Report of the Economic and Social Council on its 2016 Session*, pp 20-20, https://dx.doi.org/10.18356/c733847b-en DOI: 10.18356/c733847b-en

Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. N. (2020). Toward a sustainable cybersecurity ecosystem. *Computers, 9*(3), 74. DOI: 10.3390/computers9030074

Saprykina, N. (2023). Technologies of environmental engineering protection in the context of sustainable architecture development: alternative approaches. In E3S Web of Conferences (Vol. 389, p. 02016). EDP Sciences. DOI: 10.1051/e3sconf/202338902016

Sarkadi, Ș., Moraru, I., & Manning, L. (2023). Sustainable AI & Agricultural Technologies. IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C), Toronto, ON, Canada, 90-91. doi: 10.1109/ACSOS-C58168.2023.00045.

Sen, S., Kumar, M., Vedik, B., Shiva, C. K., & Prajapati, A. K. (2023). Predictive Controller Based EMS and Techno-Economics of an Electrical-Thermal Community MG. IEEE IAS Global Conference on Renewable Energy and Hydrogen Technologies (GlobConHT), Male, Maldives, 1-6. https://dx.doi.org/10.1109/GlobConHT56829.2023.10087854

Shevchuk, N., Oinas-Kukkonen, H., & Oinas-Kukkonen, H. (2017, April). Green IS/IT: an overview of historical periods, recent research initiatives and theoretical approaches.

In Proceedings of the 6th International Conference on Smart Cities and Green ICT Systems. Scitepress science and technology publications. DOI: 10.5220/0006235101270134

Singh, R., Akram, S. V., Gehlot, A., Buddhi, D., Priyadarshi, N., & Twala, B. (2022). Energy System 4.0: Digitalization of the energy sector with inclination towards sustainability. *Sensors, 22*(17), 6619. DOI: 10.3390/s22176619

Squillace, J., Hozella, Z., & Cappella, J. (2023). Maintaining a Secure Foundation of Cybersecurity Awareness while reducing eWaste and Carbon Output through Ethical User Actions and Sustainable Green Computing. AI, Computer Science and Robotics Technology. DOI: 10.5772/acrt.18

Srujana, S., Sreeja, P., Swetha, G., & Shanmugasundaram, H. (2022). Cutting Edge Technologies for Improved Cybersecurity Model: A Survey. International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 1392-1396. DOI: 10.1109/ICAAIC53929.2022.9793228

Zhang, M., Zhang, D., & Xie, T. (2023). Technology innovations and carbon neutrality in technologically advanced economies: imperative agenda for COP26. *Economic Research-Ekonomska Istraživanja, 36*(2), 2178017. https://dx.doi.org/10.1080/1331677x.2023.2178017

Zhang, X., Li, Y., Shi, K., & Feng, Y. (2022). How Do Environmental Technology Standards Affect the Green Transformation? New Evidence from China. *International Journal of Environmental Research and Public Health.*