sustainability

Review

Beyond Data Protection: Exploring the Convergence between Cybersecurity and Sustainable Development in Business

Francisco Isaí Morales-Sáenz [1], José Melchor Medina-Quintero [1,*] and Miguel Reyna-Castillo [2,*]

[1] School of Business and Administration Victoria, Autonomous University of Tamaulipas, Boulevard Adolfo López Mateos SN, Centro Universitario, Ciudad Victoria 87149, Mexico; fmsaenz@uat.edu.mx

[2] Faculty of Architecture, Design and Urbanism, Autonomous University of Tamaulipas, Centro Universitario Tampico-Madero, Tampico 89339, Mexico

* Correspondence: jmedinaq@uat.edu.mx (J.M.M.-Q.); mreyna@docentes.uat.edu.mx (M.R.-C.)

Abstract: The increase in the use of information technology (IT) poses a challenge derived from the risks and threats of computer security in all areas of society. In this sense, cybersecurity emerges as an important pillar of support for protecting infrastructures essential for countries' sustainable economic and social development. This paper explores the possible links between cybersecurity and sustainable development within the high-impact scientific literature. The study uses a systematic literature review methodology based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol, ensuring a rigorous and structured approach to selecting and analyzing relevant literature. The scientific database Web of Science is used to ensure the integrity and quality of the data collected, following criteria widely validated in this type of methodology. The study reveals a significant interrelationship between cybersecurity and sustainable development in the business sphere. It highlights cybersecurity's contribution to economic sustainability by protecting critical infrastructure and minimizing financial risks. Concerning environmental sustainability, cybersecurity facilitates the implementation of cleaner and more efficient technology. Social sustainability ensures personal data protection and fosters a culture of responsibility and trust within organizations.

Keywords: cybersecurity; sustainable development;digital security; sustainability challenges; data protection; systematic review

check for updates

Citation: Morales-Sáenz, F.I.; Medina-Quintero, J.M.; Reyna-Castillo, M. Beyond Data Protection: Exploring the Convergence between Cybersecurity and Sustainable Development in Business. *Sustainability* **2024**, *16*, 5884. https://doi.org/10.3390/su16145884

Academic Editors: Riccardo Valentini, Andrea Falegnami and Andrea Tomassi

Received: 17 May 2024
Revised: 4 July 2024
Accepted: 8 July 2024
Published: 10 July 2024

1. Introduction

With the significant increase in online interactions and transactions resulting from the increase in the number of devices connected to the Internet, it has become more evident that computer security is a key factor in safeguarding the confidential information of organizations [1]. In addition, the reliance on online technology and networks has created fertile ground for cybercrime, with attacks becoming increasingly sophisticated and targeting organizations of all sizes and sectors [2]. Therefore, the implementation of robust cybersecurity measures has become imperative to protect organizations against cyber-threats, minimize the risk of security breaches, and ensure the continuity of business operations in an increasingly complex and challenging digital environment [3,4].

Even in the organizational framework, the phenomenon of the COVID-19 pandemic led companies around the world to redefine their work dynamics by migrating to routines based on digitalization. This radical change in the way organizations conduct their activities prompted a rapid migration to online environments to mitigate the adverse conditions they faced [5,6]. This massive transition to remote work and the digitization of operational processes has highlighted the critical importance of cybersecurity at all levels of organizations [7,8].

Concerns about cyber security have intensified to meet current challenges, both for governments, society, and businesses [9,10]. The mass migration to the digital environment has exposed the vulnerability of organizations that were not prepared to face cyber-threats [11]. Cyber-attacks targeting vulnerable people and systems have increased, posing a serious threat to data integrity, privacy, and the continuity of organizations' business operations and, above all, to the use of sophisticated technology that allows them to protect themselves and to deal with these types of situations [12]. Organizations that are not adequately prepared to deal with security issues face serious risks, ranging from financial losses and reputational damage to potential operational disruptions that can impact the delivery of essential services [13,14].

It is essential that all actors involved in the use of online technology adopt proactive measures to strengthen cybersecurity and protect themselves from evolving cyber-threats. Only in this way can a safe and reliable digital environment be guaranteed for the well-being and progress of society as a whole. The study of cybersecurity within the scientific community reviews fundamental importance in the current highly technological and digitalized context, addressing a wide spectrum of constantly evolving challenges related to data protection, the prevention of cyber-attacks, and the safeguarding of critical infrastructures [15,16], both at the government and business level [17]. Cybersecurity research can help understand and anticipate the tactics used by cybercriminals, as well as develop innovative strategies and solutions to counter these threats in an ever-changing environment [18,19].

In this sense, and as technology continues to penetrate all areas of society, the need to protect information as well as computing devices becomes increasingly critical as a result of all that it entails. It is essential to protect individuals, organizations and society as a whole, who need a solid framework to face the challenges posed by the digital age and safeguard the foundations of a world increasingly interconnected. The exchange of knowledge and research in the scientific community fosters cooperation between experts and collaboration in the search for comprehensive and effective solutions to ensure security in the digital environment.

Cybersecurity, in addition to having priority in the protection of computer systems, plays a crucial role in the sustainability of business operations in the digital age. In the academic literature, the link between cybersecurity and aspects of sustainable business development is increasingly appreciated, highlighting how the risks of computer systems are associated with the long-term risks of economic resources [20], environmental [21] and social resources [22]. In the context of risks to economic sustainability, in critical sectors such as natural gas, Rodger and George [20] showed that cyber-threats can affect the economic sustainability of the supply chain by severely affecting the continuity of business operations and increasing the risk of costly disruptions in the chain. Implementing cybersecurity measures, such as protection against data theft and service interruption, contributes to transparency and corporate social responsibility [20,22].

The interconnectedness of devices in Industry 4.0, technology-dependent supply chains, and the growing FINTECH sector highlight the critical need for robust cybersecurity measures to ensure communication and reliability between systems, protect information assets, and ensure safe and sustainable financial operations [23–25]. Studies such as those by Naffa and Fain [26] and Shaikh and Siponen [27] reinforce this idea, arguing that a comprehensive cybersecurity strategy not only mitigates risks and threats but is also essential for business continuity and the protection of stakeholders' interests.

The impacts of cyber-attacks transcend direct financial costs, eroding consumer trust, damaging corporate reputation, and compromising privacy, which can lead to devastating consequences for the long-term economic sustainability of companies [28,29]. Therefore, investing in cybersecurity becomes a crucial strategy to counter threats and foster a secure and sustainable business environment, vital for continued success in a highly competitive and Internet-dependent market [30,31]. This integration of cybersecurity into sustainable development policies is critical to ensuring economic resilience and promoting equitable and sustainable development.

Cybersecurity is also associated with environmental sustainability by protecting the integrity and confidentiality of data related to environmental and conservation practices. The use of technology such as blockchain in the automotive industry, as suggested by

Fraga-Lamas and Fernández-Caramés [21], not only improves data security but can also reduce the environmental footprint by optimizing supply chain management and material traceability. Cybersecurity technology, by optimizing the performance and efficiency of computer and network systems, can indirectly contribute to energy conservation and environmental impact mitigation. In addition, sustainable supply chain management, facilitated by robust cybersecurity practices, can reduce emissions and improve efficiency in transportation and logistics [32,33].

In the social realm, cybersecurity is crucial to maintaining customer privacy and trust, especially in online business transactions. Chun [34] highlights how customer trust in e-commerce is affected by the security of their personal and financial data. In addition, investment in cybersecurity infrastructures, as mentioned by Arcuri et al. [22], aligns with corporate responsibility and accountability in protecting digital assets and mitigating cyber risks. Not only does this protect the company's economic sustainability by avoiding financial losses, but it also reinforces its commitment to social sustainability by protecting customer and stakeholder data.

In summary, the literature reviewed demonstrates a growing recognition of cybersecurity as a data protection mechanism and an essential component of sustainable development [32]. However, there is notable variability in how cybersecurity is conceptualized and applied in different contexts, suggesting a need for more unified definitions and strategies tailored to various industry and geographic sectors [35]. Although some studies highlight the practical applications of cybersecurity in promoting environmental, economic, and social sustainability, significant gaps persist in integrating these dimensions [21]. The relationship between the research questions and the results obtained is direct, showing that the more integrated and aware the approach to cybersecurity, the more significant its contribution to sustainable development [20]. The central question that guides this research is: What is the relationship between cybersecurity and sustainable development in the business context? The following particular questions are also asked: How does cybersecurity contribute to the economic sustainability of companies? How does cybersecurity impact environmental sustainability? What is the role of cybersecurity in social sustainability within organizations? What methodologies and conceptual approaches are used to study the relationship between cybersecurity and sustainable development?

Therefore, cybersecurity awareness and training are critical to empowering individuals and organizations in cyber-threat prevention, thus promoting a culture of digital security and community engagement [34,36]. Although many studies have addressed the issue of corporate cybersecurity, this bibliometric study review shows that few works have explicitly addressed cybersecurity from the perspective of Sustainable Development. This aspect is essential for the sake of the business path toward sustainability since all the strategic actions established by firms in the face of risks must take into account economic, environmental, and social risks. This paper aims to contribute to filling this gap in the literature. Therefore, the objective of this review is to systematically analyze the links that exist between cybersecurity and aspects of sustainable development (social, environmental, and economic). The review methodology is based on Burgess et al. [37] and Wacker [38], who propose categories that have been frequently used in review articles. The general criteria for classification and review were (1) descriptive features of the literature, (2) definitional issues, (3) theoretical concerns, and (4) methodological issues of the research.

This document is structured as follows: In the method section, the process carried out to achieve the proposed objectives is described in detail, including the steps followed in the analysis. In the results section, the achievements obtained from empirical studies and a comprehensive analysis of the studies addressed are presented. Finally, in the conclusions section, the results are discussed from a general perspective, highlighting the implications and practical applications, as well as the possible limitations of the study. This rigorous and structured approach will allow for a clearer and more precise view of the approaches and relationships of cybersecurity with sustainable development, providing a solid knowledge base for future research and contributing to the advancement of the scientific field in this area.

2. Method

Systematic Review and Selection Criteria

To meet the research objective, the methodological design was analytical-conceptual [38], and the type of analysis was bibliometric and hermeneutic. Regarding the unit of analysis selected, it was the scientific platform of the We of Sciences (WOS), as a result of the fact that its importance at an international level has been highlighted, making it one of the platforms most recognized within the scientific community for its rigor [39] in which the export of metadata from this platform allows the execution of exhaustive analyses on a particular field of study tags [40]. A literature review is one of the most relevant approaches in scientific research, and it allows for the identification of knowledge gaps within the literature [41]. Therefore, the search for primary information sources is carried out, oriented towards scientific production related to the study of cybersecurity and sustainable development indexed within the platform.

The search for publications within the Web of Science platform was guided by specific criteria: "sustainability" OR "sustainable" OR "sustainable change" OR "triple bottom line" OR "green or environmental" OR "GRI" OR "SDG" OR "ESG" OR "social sustainability" OR "social sustainable" AND "corporate" OR "Enterprise" OR "company" OR "firm" AND "cybersecurity" OR "cyber security" OR "digital security". This broadened the scope of the study to all areas of knowledge within the platform. The collections chosen on the platform were the Social Science Citation Index (SSCI) and the Emerging Sources Citations Index(ESCI), which yielded a total of 641 publications related to the topic. The search was further filtered with the "topic" option, resulting in a total of 275 publications from 2014 to 2023. This information was exported in format .bib for analysis using the statistical software R v. 4.3.0. Figure 1 contains the steps of the systematic literature review process based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) review reporting guideline [42].

The analysis to answer the research question began with a bibliometric analysis of the articles found. This approach allowed for a comprehensive understanding of the publications on the subject, starting with the review of the annual scientific production, the most relevant journals, the areas and publishers of the journals, the institutions and countries to which they belong, the most relevant articles, the most used concepts, and the network mapping of the key terms most used in publications within the field of interest. Subsequently, each of the corresponding articles was reviewed, focusing on those that had the characteristics of studies that allow the analysis of the data related to cybersecurity and sustainable development.

To carry out the analysis of the theoretical status of cybersecurity and sustainable development, an adaptation was made to the proposal of Burgess et al. [37], where he offers a four-dimensional scheme for the classification and theoretical review of a topic (1) descriptive features of the literature, (2) definitional issues, (3) theoretical concerns, and (4) methodological issues of the research. As the author expresses in his article, the construct to classify his articles was reviewed and validated by three evaluators with practical and academic experience in methodology, in addition to using taxonomies widely used in the literature reviews for bibliometric purposes and methodological and epistemological analyses (Table 1).

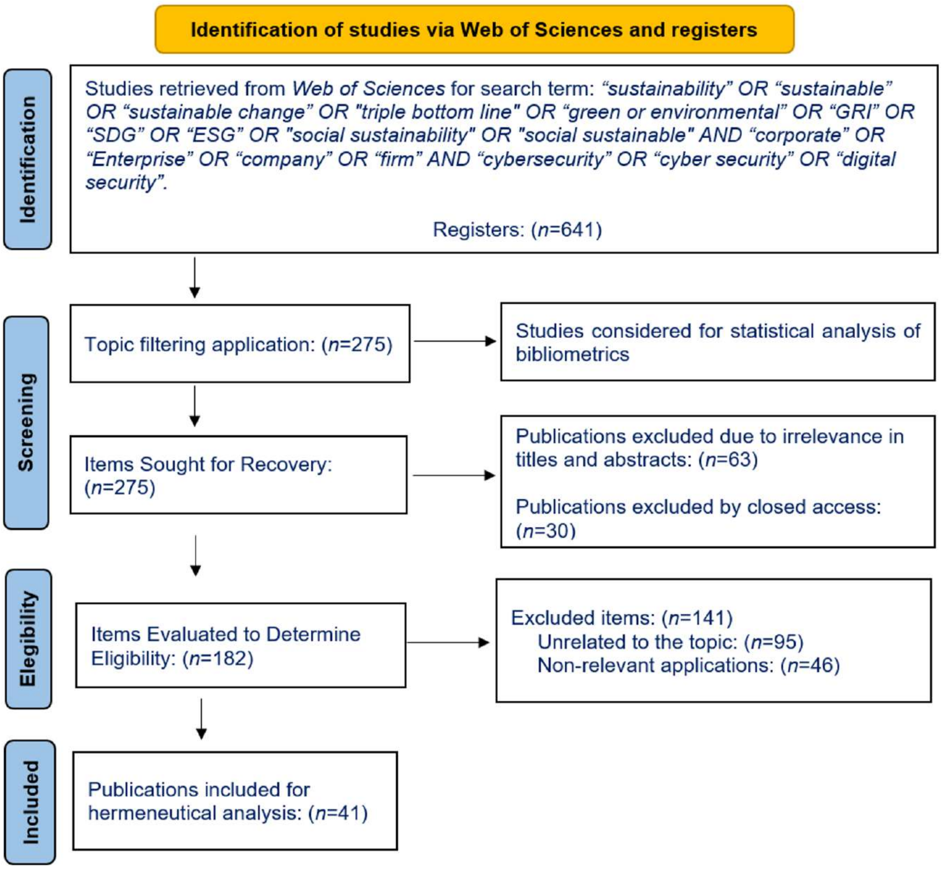
Identification of studies via Web of Sciences and registers
Identification
Studies retrieved from *Web of Sciences* for search term: *“sustainability” OR “sustainable” OR “sustainable change” OR "triple bottom line" OR “green or environmental” OR “GRI” OR “SDG” OR “ESG” OR "social sustainability" OR "social sustainable" AND “corporate” OR “Enterprise” OR “company” OR “firm” AND “cybersecurity” OR “cyber security” OR “digital security”.*
Registers: (*n*=641)
Screening
Topic filtering application: (*n*=275)
Studies considered for statistical analysis of bibliometrics
Items Sought for Recovery: (*n*=275)
Publications excluded due to irrelevance in titles and abstracts: (*n*=63)
Publications excluded by closed access: (*n*=30)
Elegibility
Items Evaluated to Determine Eligibility: (*n*=182)
Excluded items: (*n*=141)
Unrelated to the topic: (*n*=95)
Non-relevant applications: (*n*=46)
Included
Publications included for hermeneutical analysis: (*n*=41)

Figure 1. Process Flowchart for Systematic Review.

Table 1. Literature review classification framework.

Category	Covered Content	Foundation
I. Descriptive characteristics of the literature	1. Quality of journals and areas of knowledge 2. Temporal distribution of publications 3. Funding institutions 4. Frequency by most citations	Describe the characteristics of the sample analyzed
II. Conceptual and definitional issues	5. Frequency and network of key terms 6. Analysis of the use of definitions	To explore the consistency or variation in the researchers’ definitions of the variables. Define the territory that researchers claim lies within sustainable cybersecurity
III. Meetings between cybersecurity and sustainable development	7. Aspects of sustainable development 8. Cybersecurity and sustainability dimensions and indicators 9. Links between cybersecurity and sustainable development	Analyzing and synthesizing the links between cybersecurity and sustainability
IV. Questions about method and technique	10. Types of research.	Know the paths used to explore the variables studied

Adapted from Burgess et al. [37].

3. Results

As for the general information of the articles, they cover a period from 2014 to 2024, with 275 documents, and everyone is presented in the English language. Meanwhile, the research publishers that stand out the most in this type of publication are Elsevier, MDPI, Springer, IEEE, SAGE, Taylor & Francis, and Emerald Group Publishing. As far as the areas in which they are grouped within the Web of Sciences platform are concerned, they are environmental sciences, engineering, computer science, business economics, and, finally, the area of energy.

3.1. Quality of Journals and Areas of Knowledge

Table 2 shows the information regarding the scientific journals where publications on the subject have been made, where Sustainability, Journal of Cleaner Production, IEEE Access, Computer & Security, and Baltic Journal of Economic Studies are the ones with the most publications within the analyzed databases and, likewise, the areas of knowledge to which they belong are shown. It is shown that areas such as Business and Economics (40%), Computer Sciences (20%), and Engineering (20%) are the areas where the subject of study has been addressed in greater quantity.

Table 2. Classification by quality by areas of knowledge.

No	Journal	Area	Records	Ranking
1	Sustainability	Environmental Science	36	Q2
2	Journal of Cleaner Production	Engineering	7	Q1
3	IEEE Access	Business Economics	5	Q2
4	Computer Security	Computer Science	4	Q2
5	Baltic Journal of Economic Studies	Business Economics	4	Q2
6	Information	Computer Science	4	Q2
7	Journal of the Knowledge Economy	Business Economics	4	Q2
8	Technological Forecasting and Social Change	Business Economics	4	Q1
9	International Journal for Quality Research	Engineering	3	Q2
10	Sustainable Energy Technologies and Assessments	Energy	3	Q1

Based on WOS data.

As for publication rankings, there is an indicator called Scimago Journal Rank (SJR). This indicator evaluates the impact of scientific journals, considers citation networks to quantify the average prestige per article, and can be used for journal comparisons [43]. Based on this, most publications are considered to be of high quality at the Q1 level, with 27%, Q2 with 40%, and Q3 with 33%.

3.2. Temporal Distribution of Publications

The analysis of the annual scientific production on cybersecurity and sustainable development within the database reveals a significant trend in the growth of publications over the years (Figure 2). In 2014, a single article related to this topic was found, while in 2015, 2 publications were found in the database. However, from 2016, a gradual increase in scientific production was observed, with a total of 3 articles in that year and another 5 in 2017. From then on, production accelerated moderately, reaching 5 publications in 2018, 16 in 2019, and a marked increase to 25 in 2020.

2021 marked a significant milestone in the relationship between cybersecurity and sustainable development, with 38 scientific publications in the Web of Sciences database. This increase in scientific production may be related to the growing recognition of the importance of addressing emerging challenges in cybersecurity in the context of sustainability, especially since, during this time, we were in isolation derived from the COVID-19 pandemic. Therefore, it resulted in a topic of interest within the scientific community. Likewise, the year 2022 continued to show a sustained interest in the topic, with 51 publications. The highest number in terms of production on the subject was observed in the year 2023, with 80 articles. A total of 47 publications were found to date in 2024.

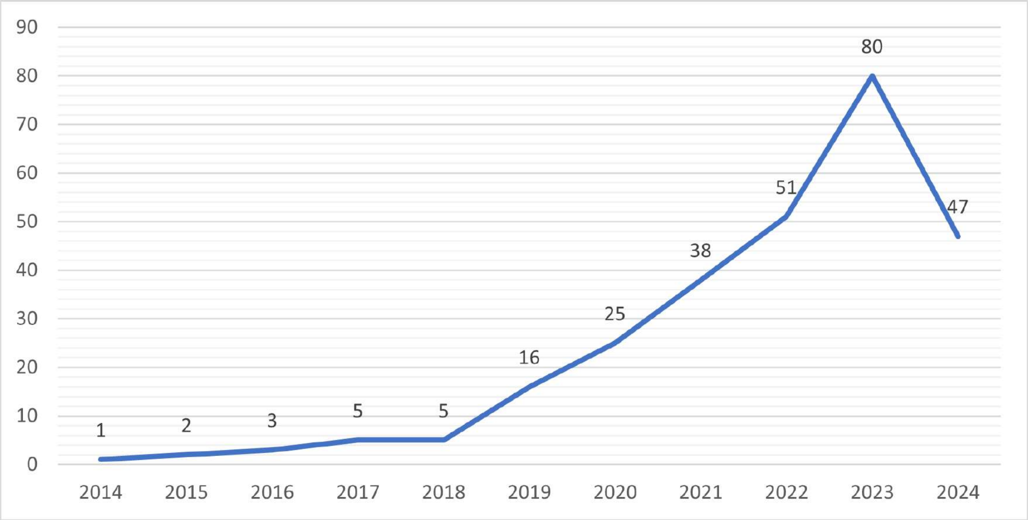

Figure 2. Number of publications per year.

3.3. Frequency by Funding Institution

Regarding analyzing the most relevant institutions in the study of the relationship between cybersecurity and sustainable development, based on the number of publications within the platform, Table 3 shows a diverse and significant distribution of scientific production. First, Indiana University stands out as a leading institution in this field, with a total of 9 publications that address this topic. Closely followed by 7 publications, Bucharest University of Economic Studies, Lutsk National Technical University, National University of Life and Environmental Sciences, and the Royal Melbourne Institute of Technology have also demonstrated significant interest and outstanding focus on research in the field of study. Likewise, a group of institutions, including Asia University, Seoul National University, Shanghai Maritime University, and the Universidad de Johannesburg, are positioned with 6 publications each. These institutions have also contributed significantly to advancing cybersecurity and sustainable development issues.

Table 3. Number of publications by institution.

Institution	N° of Publications	Country
Indiana University	9	USA
Bucharest University of Economic Studies	7	Romania
Lutsk National Technical University	7	Ukraine
National University of Life and Environmental Sciences	7	Ukraine
Royal Melbourne Institute of Technology	7	Australia
Dasia University	6	Taiwan
Seoul National University	6	South Korea
Shanghai Maritime University	6	China
University of Johannesburg	6	South Africa
Delhi Technological University	5	India

Based on WOS data.

3.4. Frequency by Most Cited

Regarding the influence of published articles, the top 10 articles within the platform are considered based on their citations within the field of study. Table 4 shows the records of the most cited publications in the study database.

It can be seen that the article with the highest number of citations is that of Litvinenko [32], called "Digital Economy as a Factor in the Technological Development of the Mineral Sector, "which focuses on the impact of the global digital economy on the technological development of this sector and presents an analysis of the possibilities of digital technology in prospecting, design, development, and use of mineral resources. In addition, it highlights the relevance of information and computing infrastructure for the secure process of generation, storage, and use of data, avoiding cybersecurity risks that could slow down technological progress. The article highlights how digital technology can drive sustainable development along the entire value chain, from exploration and production to sustainable resource planning and distribution.

Table 4. Most cited research.

Research	Title	Magazine	Total Citations
Litvinenko [32]	Digital Economy as a Factor in the Technological Development of the Mineral Sector	Natural Resources Research	229
Ghobakhloo [23]	Corporate survival in Industry 4.0 era: the enabling role of lean-digitized manufacturing	Journal of Manufacturing Technology Management	222
Fraga-Lamas and Fernández-Caramés [21]	A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry	IEEE Access	152
Laskuraín-Iturbe et al. [33]	Exploring the influence of Industry 4.0 technologies on the circular economy	Journal of Cleaner Production	72
Gupta et al. [44]	Examining the impact of Cloud ERP on sustainable performance: A dynamic capability view	International Journal of Information Management	67
Murch et al. [45]	Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy	Frontiers in Bioengineering and Biotechnology	56
Rodger and George [20]	Triple bottom line accounting for optimizing natural gas sustainability: A statistical linear programming fuzzy ILOWA optimized sustainment model approach to reducing supply chain global cybersecurity vulnerability through information and communications technology	Journal of Cleaner Production	42
Hernández et al. [46]	Engineering education for smart 4.0 technology: a review.	International Journal on Interactive Design and Manufacturing (IJIDeM)	48
Adbul-Hamid et al. [47]	The drivers of Industry 4.0 in a circular economy: The palm oil industry in Malaysia	Journal of Cleaner Production	23
Najaf et al. [48]	Fintech firms and banks sustainability: Why cybersecurity risk matters?	International Journal of Financial Engineering	19

Based on WOS data.

3.5. Frequency and Network of Key Concepts

Regarding the most frequently used terms, Figure 3 highlights the term “cybersecurity”, which appears 33 times, indicating a predominant focus on digital systems and data security in sustainable development. This is followed by “Sustainability”, which has 30 mentions, emphasizing the recognition of its importance in ensuring the protection of digital resources over the long term. The term “Industry 4.0” appears 22 times, reflecting the role of the industrial sector in implementing safe and sustainable practices in its digital infrastructure and operations. Other notable terms include “Blockchain”

(17 mentions), "Digital transformation" and "Security" (14 mentions each), "Digitalization" (13 mentions), "Big data" (12 mentions), "Cloud Computing" (11 mentions), and "Digital economy" (10 mentions). These frequencies underscore the emphasis on digital innovation and security aspects within sustainable development".

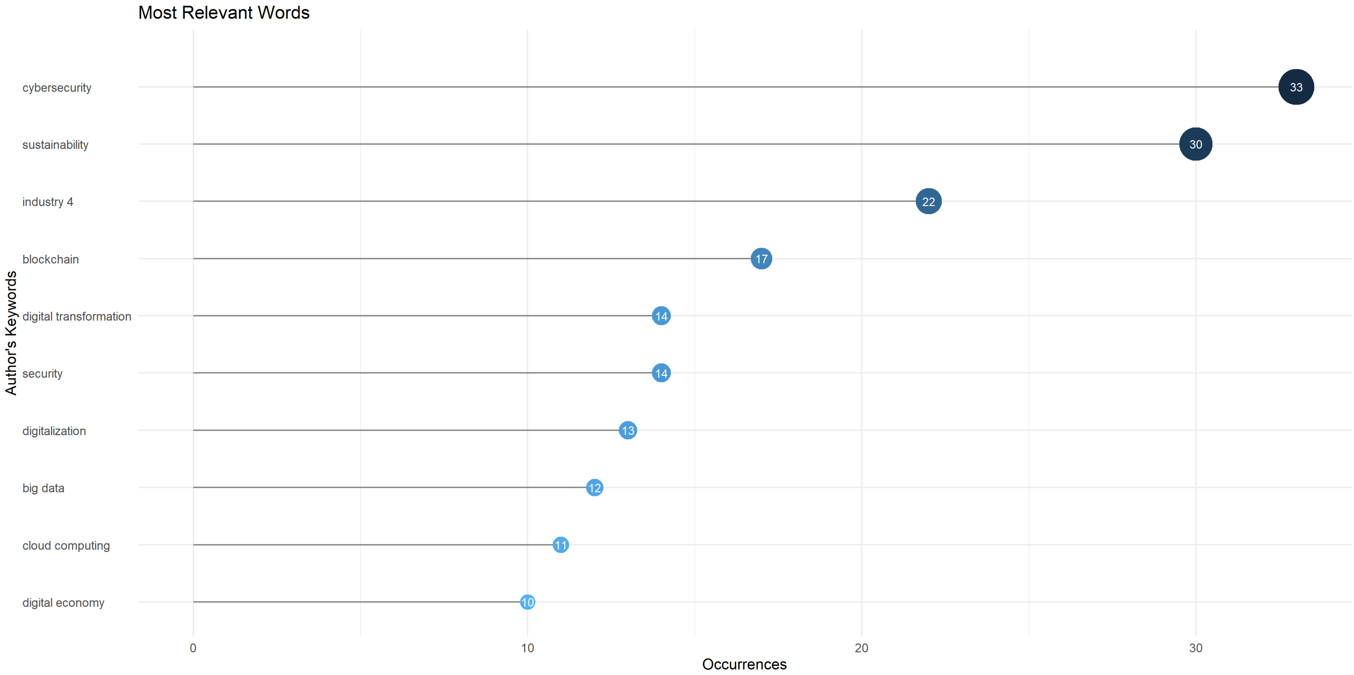

Figure 3. Most commonly used key terms.

This analysis of the key terms most used in scientific research about the subject of study offers an overview of the areas of interest and emphasis. These terms reflect the complexity and importance of approaching cybersecurity from a sustainable perspective, recognizing the need to protect digital assets while promoting responsible and sustainable development in the digital age. One of the questions that gave rise to the development of the research was related to the key terminology used by the researchers. To this end, identifying the most used words within the publications related to cybersecurity and sustainable development was taken into account to visualize better the grouping and linking of each of the terms found.

The information in Figure 4 not only highlights each key term but also elucidates the intricate web of connections between them and the topic of interest. The most salient graphic data reveals how cybersecurity and Sustainability are not isolated concepts but rather two key terms deeply intertwined with Industry 4.0 trends. Cybersecurity, which features prominently in the network, is not just about safeguarding digital systems and data, but also about promoting the economic, environmental, and social stability necessary for successful sustainable development. This is reflected in the frequent association of cybersecurity with terms such as "big data" and "cloud computing", indicating its role in protecting the reliability and security of data-driven processes.

The term "Sustainability", prominently featured, underscores its central importance in the network, connecting various concepts such as "digital transformation", "blockchain", and "Industry 4.0". This highlights the transformative role of digital and technological advancements in achieving sustainable goals. The frequent mention of "Industry 4.0" reflects its significance in modernizing industrial processes through digitalization, where cybersecurity is essential to prevent interruptions and ensure the security of connected systems.

"Blockchain" and "digital transformation" are other key terms that indicate the ongoing shift towards more secure and efficient digital operations. With its decentralized nature, blockchain offers promising solutions for enhancing security and transparency in various sectors. The term "digital transformation" signifies the comprehensive adoption of digital technology, further emphasizing the necessity of robust cybersecurity measures in this era of rapid technological change.

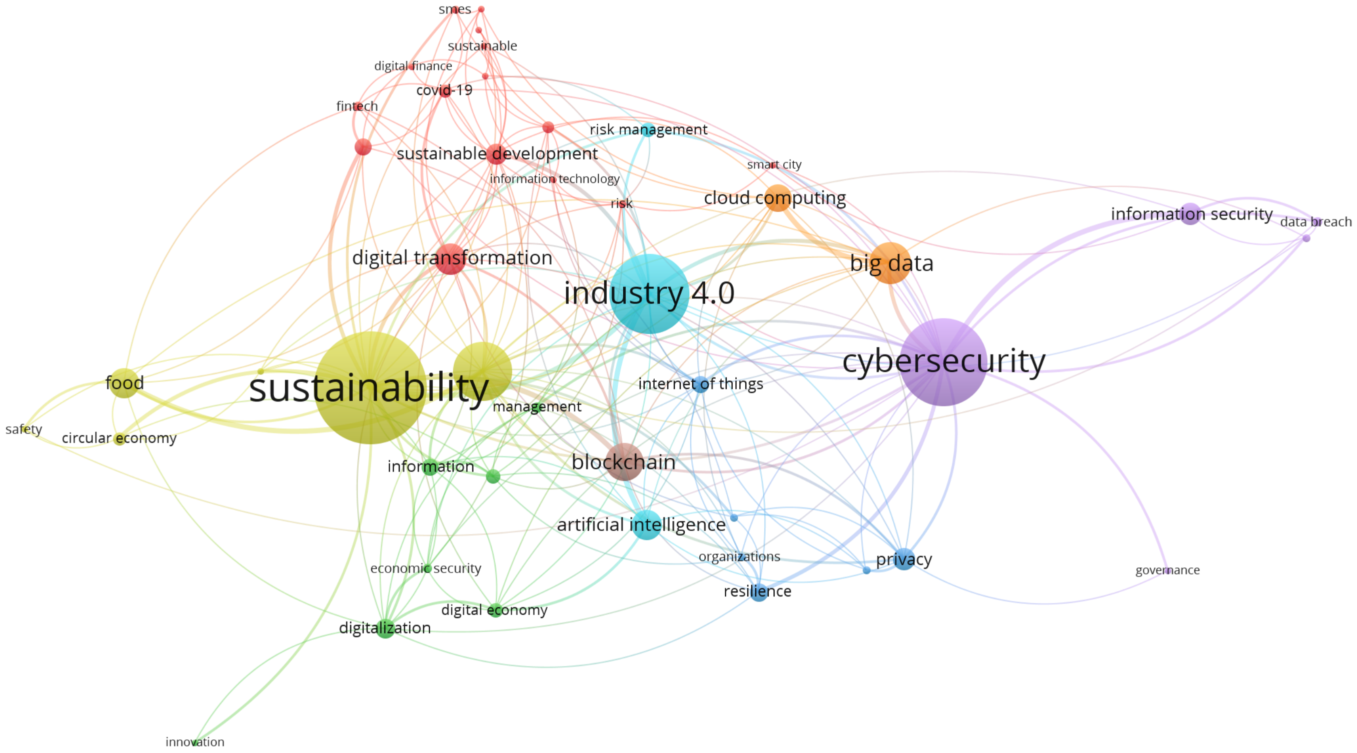

Figure 4. Key Terms Network.

The concept of "big data", frequently associated with cybersecurity, underscores the critical need for protecting large volumes of data from unauthorized access and manipulation. This ensures that data in various sectors like agriculture, energy, and health remains reliable and accurate, forming a solid foundation for sustainable development initiatives. Moreover, "artificial intelligence" and "privacy" are intricately linked to cybersecurity. The integration of AI presents new opportunities for predicting and addressing patterns in sustainable development but also introduces new risks that cybersecurity must mitigate. Protecting privacy is crucial in fostering trust in digital technology, ensuring data vulnerabilities do not compromise sustainable development projects. In this sense, cybersecurity policies play a pivotal role in establishing a legal and regulatory framework that supports sustainable development. These policies ensure that data and systems are protected from cyber-threats, creating a secure and trustworthy environment for digital innovation.

3.6. Analysis of the Use of Definitions

In the broad and diverse field of cybersecurity, understanding and classifying knowledge is critical to advancing research and practice. This effort to categorize and analyze the various approaches to cybersecurity is reflected in Table 5, which provides an overview of how scholars and experts have approached the topic through various perspectives and conceptual approaches. By breaking down the literature into specific categories, this table highlights the richness and complexity of the field and the different ways researchers have interpreted and contributed to the understanding of cybersecurity. This classification provides a solid basis for discussing current and future developments in the field, from explicit and implicit concepts to sustainability-related approaches and studies that dispense with a defined conceptual framework.

By presenting this table, we offer an overview that facilitates the identification of trends, gaps, and opportunities within the study of cybersecurity. Each category, supported by several relevant articles and studies, reflects different facets and depths of understanding the topic. Thus, from conceptual analyses to considerations on sustainability in cybersecurity, including works that assume an implicit understanding of the concept, this summary serves as an informative resource and a starting point for future research. With a total of 33 papers analyzed, the table stands as a testament to the rich diversity of approaches and the continued evolution of the field of cybersecurity within the scientific community.

Table 5. Frequency of cybersecurity definitions.

Category	Research	Count *
(a) Cybersecurity Concepts	Abdul-Hamid et al. [47]; Calabrese et al. [49]; Litvinenko [32]; Sulich et al. [50]; Muhammad et al. [51]; Lim [52]; Radu and Samili [28]; Ram et al. [24].	8
(b) Implicit Concept of Cybersecurity	Laskurain-Iturbe et al. [33]; Gupta et al. [44]; Morales-Menendez [18]; Malatji et al. [36]; Rodger and George [20]; Ramírez et al. [53]; Gutiérrez et al. [54]; Shackelford [35]; Fernández et al. [55] ; Najaf and Mostafiz et al. [48]; Fraga-Lamas and Fernández Caramés et al. [21]; Chun [34]; Annarelly and Palombi [56]; Arcuri et al. [22]; Abbas et al. [57]; Jerman et al. [58]; Fan et al. [59]; D'Adamo et al. [60]; Hu et al. [61]; Shackelford [62]; Okpa [29] (2022); Wang et al. [31]; Škerháková et al. [30]; Shaikh and Siponen [27]; Ghobakhlo et al. [23].	25
(c) Sustainable Cybersecurity Concept	Murch et al. [45]; Annarelly and Palombi [56] ; Sadik et al. [63]; Cassota and Sidortov [64]	4
(d) No concept of cybersecurity	Soltovski et al. [65]; D'Arcy and Basoglu [66]; Sidibé et al. [67]; Polverini et al. [68]	4

Based on literature review. * There are items that fall into more than one category.

In cybersecurity research and its intersection with sustainable development, it is crucial to understand the variety of definitions and conceptual approaches that the field encompasses and how these concepts apply to and relate to sustainable practices. Table 6 delves into the content of the definitions of cybersecurity presented by various authors, offering a detailed overview of how cybersecurity is conceptualized in different studies. Through this comparison, we seek to identify common and differentiating elements in the definitions and the dimensions of cybersecurity that are considered essential to promote a safe and sustainable digital environment. This analysis allows us to appreciate the diversity of approaches and evaluate how incorporating sustainable cybersecurity practices can contribute to the resilience and sustainability of information systems in the long term.

Table 6 presents a compilation of cybersecurity definitions obtained from various studies carried out between 2014 and 2024, classifying them according to their type: Own (P), From others (O), Explicit (E), and Implicit (I). By examining these definitions from the perspective of sustainable development, several relevant aspects can be identified that highlight the importance of cybersecurity in this context. First, it is noted that most definitions are classified as Implicit-Others (I-O), suggesting that much of the current understanding of cybersecurity is based on concepts and descriptions provided by external sources. However, as the years go by, the definitions become more comprehensive and detailed, encompassing various aspects of cybersecurity. For example, Laskurain-Iturbide et al. [33] offer a comprehensive definition that addresses the protection of systems, networks, and data and the prevention, detection, and response to threats and vulnerabilities in digital environments. Definitions are also tailored to specific contexts, such as e-commerce [34,60], the automotive industry [21], and healthcare [57]. This highlights the relevance of cybersecurity in various sectors and its impact on protecting sensitive data and user trust, which are fundamental aspects of sustainable development.

Table 6. Definition of Cybersecurity by type classification.

Research	Type */Definition of Cybersecurity
Rodger and George [20]	[I-O]/Cybersecurity is addressed as a potential threat to the sustainability of the natural gas supply chain. It protects computer systems, networks, and data against unauthorized access, attacks, and damage. It involves implementing measures to prevent, detect, and respond to cyber-threats and ensure information confidentiality, integrity, and availability.
Lim [52]	[E-P]/Cybersecurity protects the integrity, confidentiality, and accessibility of information.
Chun [34]	[I-O]/In the context of e-commerce and online transactions, cybersecurity is crucial to ensure the privacy and security of customer information and to maintain customers' confidence in conducting business online.
Fan et al. [59]	[I-O]/Threats to the cybersecurity of electrical systems were summarized into four types: unauthorized access to information, unauthorized modification or theft of information, denial of service, and repudiation/lack of accountability.
Fraga-Lamas and Fernández-Caramés [21]	[I-O]/Cybersecurity is an important concept in the context of blockchain technology and its application in the automotive industry. Blockchain can improve data security, privacy, and integrity, providing a higher level of cybersecurity to the industry.
Arcuri et al. [22]	[I-O]/In particular, to reduce cyber incidents that can adversely affect the activity of organizations, as well as trust in electronic transactions and customer interactions, companies should invest in cybersecurity infrastructures to protect system networks against unauthorized access and data alteration.
Gupta et al. [44]	[I-O]/Organizations should consider cybersecurity when adopting cloud-based operations and services like Cloud ERP.
Litvinenko [32]	[E-P]/Cybersecurity is the steady state of protection of information, its carriers, and infrastructure, which ensures the integrity and stability of information-related processes against natural, artificial, intentional, or unintentional impacts. Impacts are information security threats that can harm the subjects of information relationships.
Malatji et al. [36]	[I-O]/The authors argue that cybersecurity is not only about implementing technical measures; it is also important to consider the social and organizational aspects of information security. Therefore, the socio-technical approach focuses on the interaction between the technical and non-technical aspects of information security and seeks to optimize both to improve the overall security of business systems.
Morales-Menendez [18]	[I-O]/Cybersecurity is essential to ensuring the integrity, confidentiality, and availability of data and systems and to mitigate the risks associated with interconnected industrial networks.
Shackelford [69]	[I-O]/Cybersecurity refers to the protection of computer systems and networks against unauthorized access, data theft, service interruption, and other types of cyber-attacks. The paper explores how cybersecurity relates to human rights and cyber peace and how it can be improved domestically and internationally.
Abdul-Hamid et al. [47]	[E-P]/Services and technologies designed to protect industrial users, systems, equipment, networks, and data from illicit intrusion.
D'Adamo et al. [60]	[I-O]/Cybersecurity is important to ensure the privacy and security of users' personal and financial information and to protect the integrity of critical systems and infrastructure. In the context of e-commerce, cybersecurity is essential to ensure consumer confidence in online transactions and to protect them from potential fraud.
Férnandez et al. [55]	[I-O]/To formulate appropriate risk mitigation strategies, it is essential to understand the cybersecurity risk and threat landscape to classify, detect, analyze, protect, and protect privacy.
Gutierrez et al. [54]	[I-O]/It involves developing and implementing technologies and strategies to prevent and mitigate cyber-attacks, hacking, and cybersecurity breaches.
Laskurain-Iturbide et al. [33]	[I-O]/Cybersecurity protects computer systems, networks, and data from unauthorized access, attacks, and damage. It involves implementing measures to prevent, detect, and respond to threats and vulnerabilities in digital environments. Cybersecurity is crucial to ensure the confidentiality, integrity, and availability of information and systems and to safeguard against cybercrime and data breaches. It encompasses various technologies, processes, and practices to secure digital assets and mitigate the risks associated with cyber-threats.

Table 6. *Cont.*

Research	Type */Definition of Cybersecurity
Najaf et al. [48]	[I-O]/Cybersecurity refers to the measures and practices used to protect computer systems, networks, and data from unauthorized access, attacks, and damage. It protects information and technology assets against cyber-threats such as hacking, data breaches, malware, and phishing attacks.
Sulich et al. [50]	[E-P]/The concept of cybersecurity is related, among other things, to protecting the information processing space and the interactions in information technology networks.
Hu et al. [61]	[I-O]/Cybersecurity refers to the measures and practices to protect computer systems, networks, and data from unauthorized access, attacks, and damage. It involves using technologies, processes, and policies to prevent, detect, and respond to cyber-threats and ensure information and systems' confidentiality, integrity, and availability.
Jerman et al. [58]	[I-O]/Effective cybersecurity education and awareness are crucial for individuals and organizations to understand the risks and adopt best practices to mitigate them.
Abbas et al. [57]	[I-O]/In healthcare, cybersecurity measures are crucial to ensure the security and privacy of sensitive patient data and the smooth functioning of digital health systems.
Ramírez et al. [53]	[I-O]/For the corporate realm, cybersecurity becomes an inescapable business responsibility, and accountability becomes a way to provide trust and ensure resilience in the face of high-impact cyber risks and threats.
Calabrese et al. [49]	[E-P]/A set of technologies that enable data security, storage, and transfer.
Muhammad et al. [51]	[E-P]/Cybersecurity is the practice of protecting networks, systems, and programs from cyber-attacks.
Ghobakhlo et al. [23]	[I]/Cybersecurity ensures the safety, reliability, and security of communications between interconnected devices within the Industry 4.0 environment.
Ram et al. [24]	[P]/Defending against cyber-threats is crucial as it prevents unauthorized use, denial of service, modification, disclosure, loss of revenue, or even the destruction of critical systems or information assets, which can have severe consequences for your organization.
Radu and Smaili [28]	[P]/It is the activity, process, ability, or state by which information and communications systems and the information contained are protected and defended against damage, unauthorized use or modification, or exploitation.
Naffa and Fain [26]	[I]/Cybersecurity is considered an essential topic in corporate governance, and its relevance to the responsibility of boards of directors to protect companies in cyberspace and manage associated cyber risks is highlighted.
Bondarenk et al. [25]	[I]/They note that increased digitization and the development of financial technology have led to an increased focus on cybersecurity to protect systems and data in the financial sector.
Okpa et al. [29]	[I]/The authors strongly advocate for the need to take proactive measures and stay ahead of the latest trends and threats in cybersecurity. This approach empowers your organization to protect both itself and its individuals from potential cyber-attacks, giving you a sense of control in an ever-evolving digital landscape.
Wang et al. [31]	[I]/Cybersecurity is not just a protective measure, it is a vital element that ensures the smooth operation of business activities in a highly competitive and Internet-dependent environment, giving your organization a sense of security and confidence.
Škerháková et al. [30]	[I]/The company's management team stresses that cybersecurity is a significant part of sustainable corporate reputation and that proper online reputation management is essential for companies in a constantly evolving digital environment.
Shaikh and Siponen [27]	[I]/Refers to the measures, practices, and strategies organizations implement to protect their information systems, networks, and data against cyber-threats, such as attacks, intrusions, and security breaches.

* Own definition (P), others (O), explicit (E), implicit (I). Based on the literature review.

In this sense, and from a sustainable development perspective, cybersecurity is a crucial factor for the sustainability of various sectors. For example, Rodger and George [20] address cybersecurity as a potential threat to the sustainability of the natural gas supply chain, while D'Adamo et al. [60] highlight its importance in e-commerce. Protecting systems, networks, and data against unauthorized access and cyber-attacks is essential to ensure the continuity and resilience of these industries, thus contributing to sustainable development.

In addition, cybersecurity plays a critical role in protecting the privacy and security of users' personal and financial information [60]. In an increasingly digitalized world, consumer trust in online transactions and data protection are critical to encouraging participation in the digital economy and promoting inclusive, sustainable development. Another noteworthy aspect is the importance of cybersecurity in sectors critical to sustainable development, such as healthcare [57] and the energy industry [59]. Protecting sensitive patient data and ensuring the smooth functioning of digital health systems are critical to providing quality and accessible healthcare. Likewise, cybersecurity in electricity systems is vital to ensure a reliable and sustainable energy supply. Therefore, protecting systems, networks, and data is essential to ensure sustainability, resilience, and trust in critical industries and safeguard users' privacy and security in an increasingly digitized world. Integrating cybersecurity considerations into sustainable development strategies is essential to address the challenges and opportunities in the digital age presents.

The findings indicate various definitions of cybersecurity, each tailored to different industrial and organizational contexts. This underscores the importance of having a clear and unified definition that facilitates the effective implementation of cybersecurity strategies aligned with sustainable development objectives. In addition, the diversity in definitions reflects the different approaches and concerns related to cybersecurity in different sectors, showing that, although its strategic importance is recognized, the lack of consistency in definitions can hinder the integration of cybersecurity with sustainability policies. This variability in conceptualization directly answers the research questions by illustrating how the understanding of cybersecurity influences practical and theoretical application in the context of sustainable development and suggests the need for greater clarity and consensus in definitions to improve cooperation and practical implementation in organizations.

3.7. Aspects of Sustainable Development

At the intersection of cybersecurity and sustainable development, a complex and multifaceted landscape that encompasses social, environmental, and economic aspects is revealed. Table 7 presents a mapping of how current cybersecurity research contributes to and intertwines with the principles of sustainable development. This compilation of studies illustrates the diversity of approaches and methodologies researchers employ to address sustainability challenges through the lens of cybersecurity and how these efforts can bolster or transform practices across a wide range of sectors. By categorizing the contributions according to their focus on social, environmental, and economic aspects, Table 7 provides a comprehensive view of the sustainability dimensions impacted by cybersecurity.

This section examined how cybersecurity integrates with and affects aspects of sustainable development in social, economic, and environmental dimensions. This analysis is crucial to answer research questions on how cybersecurity contributes to sustainable development in the business environment. The findings reveal that cybersecurity not only protects information and systems but also supports the economic sustainability of companies by protecting critical infrastructure and preventing financial losses due to cyber-attacks. In environmental terms, cybersecurity facilitates the adoption of clean and efficient technology, protecting systems that manage energy resources and thus reducing environmental impact. Socially, cybersecurity enhances user trust and security, protecting personal data and fostering a safe digital environment, which is essential for social welfare and equity. These findings are fundamental to understanding how cybersecurity measures respond to immediate data and system protection needs and have profound and direct implications for promoting more sustainable development in the business context. It underscores the relevance of incorporating cybersecurity strategies into organizations' sustainable development policies to comprehensively address the challenges of the digital era.

Table 7. Cybersecurity studies and their relationship with sustainability dimensions.

Research	Social Aspects	Environmental Aspects	Economic Aspects	Dimensions of Sustainability
Shackelford [62]	✓		✓	Polycentric governance: Cybersecurity best practices in the public and private sectors would help reduce threats of conflict, crime, and cyber espionage comparable to national and enterprise security risks.
Rodger and George [20]	✓	✓	✓	Economic: Economic gains, transparency, social responsibility. Social: Employee well-being, community involvement, work practices. Environmental: environmental impact, carbon emissions, energy conservation.
Polverini et al. [68]		✓		Resource Efficiency and Reduction of Environmental Impacts.
Murch et al. [45]	✓	✓	✓	Environmental sustainability, social equity, inclusivity, economic viability, governance, and institutions.
Lim [52]	✓	✓	✓	Transport Infrastructure.
Casotta and Sidortov [64]	✓	✓	✓	Critical Infrastructure, Energy Sector, Governance.
Fan et al. [59]		✓		Energy.
Fraga-Lamas and Fernández-Caramés [21]			✓	Supplies, gas reduction, sustainable management, resilience to environmental and social impacts.
Gupta et al. [44]	✓	✓	✓	Economic performance, environmental performance, and social performance.
Litvinenko [32]		✓		Sustainable planning, distribution of energy resources and materials, infrastructure development, clean energy, renewable energies, energy efficiency of investment, and mining industry training that addresses technical, economic, environmental, governance, and social aspects.
Morales-Menendez [18]	✓	✓	✓	It addresses sustainability-related challenges such as reducing energy consumption and reducing greenhouse gases.
Malatji et al. [36]	✓			Cybersecurity is an element for awareness campaigns and consideration of protecting privacy and user rights, which contributes to social sustainability.
Sadik et al. [63]	✓	✓	✓	Sustainable security, sustainable cybersecurity.
Abdul-Hamid et al. [47]	✓	✓	✓	Sustainability awareness, stakeholders, supply chain collaboration, waste management, emission reduction, and natural resource conservation, Blockchain can contribute to and benefit the circular economy, economic recovery, and social and environmental sustainability.
Fernández et al. [55]		✓	✓	Circular economy, food supply chain.
Laskurain et al. [33]		✓	✓	The circular economy involves reducing input consumption, reuse, recycling, reducing waste and emissions, preventing money laundering (Blockchain), and protecting privacy and data.

Table 7. *Cont.*

Research	Social Aspects	Environmental Aspects	Economic Aspects	Dimensions of Sustainability
Shackelford [69]	✓	✓	✓	They argue that organizations should treat cybersecurity as a matter of corporate social responsibility (CSR) and make an integrated assessment of public policies, environmental sustainability, intergenerational equity, political participation, and intergenerational responsibility.
Sidibé and Olabisi [67]	✓	✓		Digital technologies in sustainable agriculture and food security.
Sulich et al. [50]	✓	✓	✓	Environmental protection, social equity, economic viability.
Hu et al. [61]	✓	✓	✓	Energy footprint, carbon, climate change, sustainable development goals.
Jerman et al. [58]	✓			Education.
Abbas et al. [57]	✓		✓	Governance and institutional capacity, strengthening institutions, promoting transparency, accountability, and governance for sustainable development.
Muhammad et al. [51]	✓	✓	✓	Life and well-being, safe environment, innovation, and development.
Gutiérrez [54]	✓	✓	✓	Ensuring resilient infrastructure, promoting inclusive and sustainable Industrialization.
Naffa and Fain [26]	✓	✓	✓	Corporate governance; corporate governance. Energy efficiency, food security, water scarcity.
Bondarenko et al. [25]	✓		✓	Sustainable development of financial technologies, user confidence, and personal data protection.
Okpa et al. [29]	✓		✓	Economic sustainability; business and financial sustainability.
Wang et al. [31]			✓	Corporate sustainability.
Škerháková et al. [30]	✓		✓	Social responsibility, sustainable corporate reputation.
Shaikh and Siponen [27]			✓	Organizational learning; business resilience.
Ghobakhlo et al. [23]	✓		✓	Business sustainability, productivity efficiency, and business competitiveness.
Radu and Smaili [28]	✓		✓	Supply chain sustainability.

The checkmarks [✓] indicate the aspect covered by each investigation. Based on literature review.

3.8. Cybersecurity and Sustainability Dimensions and Indicators

Table 8 presents a comprehensive analysis of the critical dimensions and indicators in cybersecurity and sustainability, highlighting how each research addresses these fundamental aspects for contemporary development. This compendium of studies provides a detailed overview of the multiple factors that constitute cybersecurity, covering technical, organizational, legal, and cultural aspects. It is observed that cybersecurity concepts include security, reliability, protection, and trust, along with their subdimensions that encompass confidentiality, integrity, availability, authentication, and resilience, among others. In addition, the importance of data protection, risk management, privacy, infrastructure security, and user awareness is evident.

In parallel, the table exposes how sustainability is conceptualized and measured through various practices and objectives, focusing on economic, environmental, and social dimensions. Topics such as the circular economy, reducing energy consumption, waste management, energy efficiency, reducing emissions, governance, and social equity are addressed, highlighting their interconnection with cybersecurity. This table serves as an informative resource for understanding the intersection of cybersecurity and sustainability but also highlights the importance of considering both aspects in an integrated manner to meet the challenges of the digital age and promote safer and more sustainable development. In addition, it is presented as a valuable guide for future research and practices that seek to integrate these two critical domains to move towards a more resilient and equitable future.

Table 8. Cybersecurity and Sustainability Dimensions and Indicators.

Research	Cybersecurity	Sustainability
Shackelford [62]	Technical vulnerability, hardware failures, configuration issues, laws and regulations, privacy, data protection, cybersecurity breaches, censorship, cyber peace.	Polycentric Governance
Rodger and George [20]		Economic: profits, transparency, social responsibility. Social: Employee well-being, community involvement, work practices. Environmental: Environmental impact, carbon emissions, energy conservation.
Lim [52]	Privacy risks, security risks	transport infrastructure, greenhouse gas emissions.
Polverini et al. [68]	Privacy, data protection, digital infrastructure.	resource efficiency, reduction of environmental impact.
Murch et al. [45]	Biosecurity, supply chain security, data privacy and confidentiality, risk assessment and management, regulatory and legal considerations.	environmental sustainability, social equity and inclusivity, economic viability, governance and institutions.
Cassotta and Sidortov [64]	Sustainable/Sustainable Cybersecurity	Definition of cybersecurity
Fan et al. [59]	Confidentiality, integrity, information availability, risks, intrusion detection and prevention, user and device authentication and authorization, vulnerability management, user education and awareness.	Energy
Fraga-Lamas et al. [21]	Encryption, Authentication, Access Control, Network Security, Security Policies, Risk Management, Incident Response, Awareness and Training, Resilience, Legal and Regulatory Dimensions, User Behavior, Social Engineering, Cyber-Threat Psychology. Implementation costs, impact of cyber-attacks, ROI on cybersecurity solutions, critical infrastructure.	Supply chain management, gas reduction, sustainable management, resilience to environmental and social impacts.
Chun [34]	Personal and Financial Data Protection—Fraud and Cybercrime Prevention—Network Infrastructure and Computer Systems Security—Protection against Viruses, Malware and Other Cyber Risks—Password Management and User Authentication—Privacy Policies and Information Security—Online Safety User Training and Awareness—Compliance with Cyber Security Laws and Regulations—Incident Management Security	Emergency Response.
Gupta et al. [44]		Economic Performance, Environmental Performance, Social Performance.

Table 8. *Cont.*

Research	Cybersecurity	Sustainability
Morales-Menendez [18]	Attacks, decreased productivity, counterfeiting, theft.	It hints at some challenges related to sustainability, such as reducing energy consumption and greenhouse gases.
Malatji et al. [36]	Organizational: communication, cybersecurity governance, physical access controls, awareness campaigns, organizational structure. Technical: Antimalware, antivirus, user awareness policies.	
Litvinenko [32]	Reliability, Security, Storage and Use of Data in the Mineral Sector.	Sustainable planning, distribution of material and energy resources, development of infrastructure such as clean energy, renewable energies, energy efficiency, and investment. It mentions the need for high training in the mining industry that addresses technical, economic, environmental, governance and social factors.
Arcuri et al. [22]	Confidentiality, integrity, availability, risk management, incident response, infrastructure security.	
Laskurain et al. [33]	Security, Reliability, Protection, Trust: Confidentiality, Integrity, Availability, Authentication, Authorization, Resilience, Risk Management.	Circular Economy: Reduction of Input Consumption, Reuse, Recycling, Reduction of Waste and Emissions, Prevention of Money Laundering (Blockchain), Privacy and Data Protection.
Sadik et al. [63]	Assets, Threats, Vulnerabilities, Risk, Assessment, Mitigation, Resilience.	Sustainable Security, Sustainable Cybersecurity.
Abdul et al. [47]	Protection of the user, systems, equipment, networks, data.	Stakeholders, sustainability awareness, supply chain collaboration, waste management, emissions reduction, and natural resource conservation.
D'Adamo et al. [60]	Data Protection, Attack Prevention, Transaction Security, Trust.	
Fernández et al. [55]	Industry Digitalization, Associated Logistics, Strategies, Risk Mitigation, and Asset Protection	Circular Economy, Food Supply Chain.
Gutiérrez et al. [54]	I+D in cybersecurity	
Najaf et al. [48]	Encryption systems, data integrity, cloud computing.	
Shackelford [69]	Confidentiality, integrity, availability, consistency, control, and auditing to build trust.	Integrated evaluation of public policies, environmental sustainability, intergenerational equity, political participation, intergenerational responsibility.
Sidibé and Olabisi [67]	Digital Capabilities and Skills, Device Security, Infrastructure and Support Services.	Digital Technologies in Sustainable Agriculture and Food Security.
Sulich et al. [50]	Technical, legal, organizational, and cultural. Green Cybersecurity.	Environmental protection, social equity, economic viability.
D'Arcy and Basoglu [66]	Breaches, viruses, information security, intrusion, cyber-attack, computer virus, data theft, risks, phishing, cyber-attack.	
Hu et al. [61]	Security, Data Privacy, Laws and Regulations, Confidentiality, Availability and Integrity, Privacy.	Energy footprint, carbon, climate change Sustainable development goals. Governance.

Table 8. *Cont.*

Research	Cybersecurity	Sustainability
Jerman and Jerman [58]	Cybersecurity Awareness, Online Shopping Security, Cybersecurity Skills, Knowledge, Experience, Privacy, Data Protection.	Education
Abbas et al. [57]	Data Protection, Firewall, Threat Detection, Vulnerability Management	Governance and institutional capacity: strengthening institutions, promoting transparency, accountability, and good governance practices to support sustainable development efforts.
Ramírez et al. [53]	Risk, Incident and Breach Management.	
Calabrese et al. [49]	Security, attack, vulnerability, threat, privacy, phishing, defense, cyber-attack, intelligence, malicious, detection, sophisticated, hacking, software, secure, cloud, information, digital, tactical, crime, response, detection, analytics, regulation, networks, Internet, accessibility, applicability, digitalization.	Environmental footprint
Muhammad et al. [51]	Confidentiality, integrity, and availability of data and systems, security maturity, incident responsiveness, effectiveness of controls. Network Security, Software Security, and Data Security.	Innovation and Development.
Ghobakhlo et al. [23]	Cyber security.	Business sustainability, productivity efficiency, and business competitiveness.
Ram et al. [24]	Information security, information protection, data leakage, cyber-attacks.	Supply chain sustainability. Continuity and integrity of operations.
Naffa and Fain [26]	Cyber risks, disruptive technologies.	Corporate governance; corporate governance. Energy efficiency, food security, water scarcity.
Bondarenk et al. [25]	Fraud, cyber-attack, security of financial transactions, resilience of systems.	Sustainable development of financial technologies, user confidence, personal data protection.
Radu and Smaili [28]	Confidentiality, integrity, and availability of information.	Sustainability initiatives.
Okpa et al. [29]	Information protection, cybersecurity awareness, security software, and financial transaction security.	Economic, business and financial sustainability.
Wang et al. [31]	Cybersecurity awareness and training, prevention and management of vulnerabilities, protection of data and digital assets.	Corporate sustainability; sustainability of operations.
Škerháková et al. [30]	Digital security.	Social responsibility; sustainability promotion; sustainable corporate reputation.
Shaikh and Siponen [27]	Cybersecurity performance.	Organizational learning; organizational resilience.

Based on literature review.

Table 9 presents an exhaustive analysis of the academic literature, examining the relationship between cybersecurity and sustainable development. With 41 articles reviewed, the table is divided into two main categories. The first category, which encompasses 35 articles, highlights studies that explore the intersection of cybersecurity with the principles and practices of sustainable development. This work covers various approaches, from cybersecurity's contribution to the circular economy and sustainable infrastructure to its role in protecting privacy and data in contexts that promote social, environmental, and economic sustainability. Authors such as Laskurain-Iturbe et al. [33], Malatji et al. [36], Rodger and George [20], and Hu et al. [61], among others, have made significant contributions in this area, highlighting the importance of integrating cybersecurity into sustainable development strategies.

On the other hand, the second category, made up of 6 articles, groups together those studies that, although relevant to cybersecurity, do not establish an explicit connection with sustainable development. Studies such as those by Gupta et al. [44], Morales-Menéndez [18], and Calabrese et al. [49] focus on specific aspects of cybersecurity without delving into its relationship with sustainability.

This detailed analysis provides a comprehensive perspective on the current state of research at the intersection of cybersecurity and sustainable development. The table underscores the importance of integrating sustainability into cybersecurity strategies and policies. It highlights the need to foster interdisciplinary dialogue to address global challenges more effectively and sustainably. In addition, this resource serves as a valuable source of information for those interested in these fields of study. It identifies areas where further research and collaboration across disciplines is required.

Table 9. Classification based on the analysis of the relationship between cybersecurity and sustainable development.

Category	Research	Count
(a) Relationship between cybersecurity and sustainable development.	Laskurain-Iturbe et al. [33]; Malatji et al. [36]; Soltovski et al. [65]; Rodger and George [20]; Abdul-Hamid et al. [47]; Hu et al. [61]; Gutiérrez [54]; Shackelford [62]; Fernández et al. [55]; Najaf et al. [48]; Litvinenko [32]; Fraga-Lamas and Fernández-Caramés [21]; Chun [34]; Anarelly and Palombi [56]; Sulich et al. [50]; Murch et al. [45]; Arcuri et al. [22]; Abbas et al. [57]; Muhammad et al. [51]; Jerman et al. [58]; Sidibé and Olabisi [67]; Lim [52]; Sadik et al. [63]; Cassotta and Sidortov [64]; Fan et al. [59]; Ghobakhlo et al. [23]; Ram et al. [24]; Naffa and Fain [26]; Bondarenko et al. [25]; Radu and Smaili [28]; Okpa et al. [29]; Wang et al. [31]; Škerháková et al. [30]; Shaikh and Siponen [27]; D'Adamo et al. [60]	35
(b) No reference/relationship between cybersecurity and sustainable development.	Gupta et al. [44]; Morales-Menendez [18]; D'Arcy and Basoglu [66]; Ramirez et al. [53]; Polverini et al. [68]; Calabrese et al. [49]	6
TOTAL		41

Based on literature review.

In summary, after mapping and intertwining the dimensions of cybersecurity with sustainable development indicators within organizations, the findings show that cybersecurity directly influences the economic sustainability of companies by protecting critical assets, preventing service interruptions, and minimizing the financial risks associated with cyber-attacks. In environmental terms, cybersecurity is essential to secure IT infrastructure related to energy systems and environmental management, helping companies to operate cleaner and more efficiently. On the social side, cybersecurity protects personal and corporate information, contributing to a safer society and fostering a culture of trust and responsibility between consumers and employees.

In addition, the section highlights the different approaches and methodologies used to study the interaction between cybersecurity and sustainable development, underlining the need for a holistic approach that incorporates multiple analytical perspectives and techniques. This robust and diversified methodological approach ensures that the study results can offer a solid basis for strategies for integrating cybersecurity into corporate sustainability policies, therefore answering research questions and advancing the understanding of how cybersecurity can be a crucial enabler of sustainable development in the business environment.

3.9. Links between Cybersecurity and Sustainable Development

Table 10 below delves into the explicit connection between cybersecurity and sustainable development through research and academic articles. This compilation highlights how different authors have integrated the concept of cybersecurity within the sustainable development framework, covering sectors as varied as the circular economy, supply chain management, and the energy industry, among others. Each entry in the table identifies each author's or article's specific reference to this critical intersection and summarizes each paper's key contributions to the debate on how cybersecurity can be a critical pillar for promoting sustainable practices. From data protection in the circular economy context to ensuring resilient and sustainable energy infrastructures, these studies underscore the importance of integrating robust cybersecurity measures in pursuing sustainable development goals. This table provides a comprehensive view of the growing convergence between cybersecurity and sustainable development, providing a solid foundation for future research and strategies in these interconnected fields.

Table 10. Contributions to the literature and links between cybersecurity and sustainable development.

Research	Reference to Cybersecurity and Sustainable Development
Rodger and George [20]	The paper links cybersecurity to sustainable development by addressing its importance in managing the global natural gas supply chain, reducing the risk of disruptions, and improving efficiency and transparency in supply chain management.
Lim [52]	Secure and affordable access to global networks is a crucial criterion for social and economic progress, ensuring cybersecurity and privacy while expanding Internet access and inculcating human rights is vital for sustainable development.
Chun [34]	It helps protect customers' sensitive information, maintain privacy, and prevent identity theft, thus fostering a secure and trustworthy digital ecosystem. By addressing cybersecurity challenges and ensuring the resilience of digital systems, sustainable development goals related to innovation, economic growth, and social well-being can be achieved.
Fan et al. [59]	Cybersecurity is essential to ensuring the security and stability of critical infrastructure, protecting the environment, and improving energy efficiency, which contributes to sustainable development. However, cybersecurity measures also promote the resilience of energy systems, allowing them to resist and recover from cyber-attacks, minimizing their impact on sustainable development efforts.
Fraga-Lamas and Fernández-Caramés [21]	Cybersecurity is related to sustainable development, as it plays a crucial role in ensuring the long-term viability and resilience of digital systems and infrastructures. By improving data security, privacy, and integrity, blockchain technology can contribute to sustainable development by providing a secure foundation for various industries, including the automotive sector. Using blockchain in the automotive industry can improve data security, privacy, anonymity, traceability, and accountability, leading to higher cybersecurity.
Arcuri et al. [22]	The sources discussed the relationship between cybersecurity and sustainable development, highlighting the importance of cybersecurity in achieving the SDGs and the potential negative impact of cyber-attacks on the economic value and growth of the hotel sector.
Murch et al. [45]	Cyber biosecurity plays a crucial role in safeguarding the bio-economy and the sustainable development of sectors dependent on biological and biomedical systems. It ensures their safe use while minimizing risks and potential damage.
Litvinenko [32]	It delves into aspects such as the development of integrated and advanced mineral processing systems, the efficient use of energy and material resources, and the management of industrial and domestic waste, highlighting the role of digitalization and the integration of data, processes, and users in the mining industry to achieve scientific and technological advances. It also underlines how digital technology can drive sustainable development along the entire value chain, from exploration and production to sustainable resource planning and distribution. The study contributes significantly to cybersecurity and sustainable development in the mineral sector by providing a comprehensive view of how digital technology can improve efficiency, safety, and sustainability in using mineral resources.

Table 10. *Cont.*

Research	Reference to Cybersecurity and Sustainable Development
Malatji et al. [36]	Although it is not explicitly mentioned, it refers to cybersecurity as an important element for the sustainable development of companies and business society. It highlights the importance of protecting users' privacy and rights, which contributes to social sustainability.
Shackelford [69]	They argue that organizations should treat cybersecurity as a matter of corporate social responsibility (CSR) to safeguard their customers and the public, similar to companies' role in fostering sustainability.
Abdul-Hamid et al. [47]	It is not explicitly mentioned, but it refers to the fact that digitalization, including blockchain technology, can contribute to the circular economy and, therefore, benefit economic recovery and social and environmental sustainability.
D'Adamo et al. [60]	In the context of e-commerce, cybersecurity is important to ensure consumer confidence in online transactions and to protect them from potential fraud and scams, which can, in turn, foster the sustainable growth of e-commerce.
Férnandez et al. [55]	Cybersecurity is crucial in achieving sustainable development, particularly in the logistics, supply chain, and agriculture. It ensures the protection of critical infrastructure, data, and systems, which are essential for these sectors' efficient and secure operation and play a vital role in achieving the Sustainable Development Goals.
Gutierrez et al. [54]	By safeguarding data and systems, cybersecurity ensures the continuity of operations, avoiding disruptions that can have negative environmental, social, and economic impacts. In addition, it contributes to sustainable development goals such as ensuring resilient infrastructure and promoting inclusive and sustainable industrialization, which are supported by robust cybersecurity measures.
Laskurain-Iturbide et al. [33]	Cybersecurity is critical in the context of the circular economy, as it helps to ensure the traceability of products, prevent corporate circular laundering, and promote good practices that enhance circularity. It also addresses privacy and data protection concerns, which are crucial for building trust in digital technologies and promoting their adoption for sustainable development.
Najaf et al. [48]	Cybersecurity threats constantly put the assets and information of corporations, institutions, governments, and individuals, including financial institutions, at constant risk, which can have implications for sustainable development.
Sulich et al. [50]	It mentions that cybersecurity is essential to protect ICTs and the information they handle and that the lack of security can be a significant obstacle to sustainable development. In short, cybersecurity is an indispensable element for the success of the green technological revolution and for achieving sustainable development goals. Cybersecurity measures help counter attacks by criminal groups and prevent the penetration of hostile entities, thus safeguarding sustainable development efforts.
Hu et al. [61]	By protecting Energy-IT systems from cyber-threats, cybersecurity contributes to the stability and security of the energy sector, enabling the transition to a greener and more sustainable energy economy.
Jerman et al. [58]	The paper focuses on cybersecurity and its importance in education and sustainable development.
Abbas et al. [57]	Effective cybersecurity measures in healthcare improve data management systems, online services, and secure Internet services, leading to efficient and secure health services, which are essential for sustainable development.
Sadik et al. [63]	Integrating emerging technologies such as blockchain, artificial intelligence, and machine learning into cybersecurity improves the effectiveness and efficiency of security measures, supporting sustainable development efforts.
Muhammad et al. [51]	Electric vehicles serve multiple domains of sustainability, and on a broader level, sustainability can be divided into three main domains (also sometimes referred to as sustainability goals), such as (1) life and well-being, (2) safe environment, and (3) innovation and development.
Ghobakhlo et al. [23]	In the context of Industry 4.0, cybersecurity plays a pivotal role in ensuring security, reliability, and communication between interconnected devices.
Ram et al. [24]	The increasing reliance on information technology and real-time information sharing in supply chains makes cybersecurity a critical aspect of protecting information assets and technology infrastructure.

Table 10. *Cont.*

Research	Reference to Cybersecurity and Sustainable Development
Naffa and Fain [48]	Cybersecurity is crucial to ensuring the long-term sustainability of organizations. Protecting digital assets and data privacy, preventing cyber-attacks, and effectively managing cyber risks are critical elements for business continuity and protecting stakeholders' interests.
Bondarenko et al. [25]	It is highlighted that the sustainable development of FINTECHs focuses on issues of uncertainty and perceived quality, and cybersecurity plays a crucial role in ensuring the sustainability of financial operations in digital environments.
Radu and Smaili [28]	It is noted that the effects of cyber-attacks could materialize in financial costs, reputational costs, loss of confidential data, erosion of consumer trust in e-commerce, and violation of privacy, among others. In addition, it is mentioned that cybersecurity is critical not only for shareholders, managers, and employees but also for society as a whole, which highlights the importance of protecting information and systems against potential cyber-threats to ensure a safe and sustainable environment.
Okpa et al. [29]	An in-depth analysis reveals the profound impact of cybercrime on companies, affecting their reputation, financial resources, and economic stability. These implications can have far-reaching effects on the sustainable development of businesses.
Wang et al. [31]	In a highly competitive and Internet-dependent environment, the importance of cybersecurity for companies cannot be overstated. Proactively mitigating cyber risks is critical to ensuring the sustainability and continuity of business operations in an increasingly complex and challenging digital environment.
Škerháková et al. [30]	Cybersecurity is a crucial component in ensuring organizations' economic sustainability and growth. It protects their assets, data, and business operations from potential cyber-threats that could jeopardize their financial stability and reputation. In this sense, investing in cybersecurity measures is presented as a key strategy to promote a safe and sustainable business environment in today's digital economy.
Shaikh and Siponen [27]	It is pointed out that the relationship between cybersecurity and sustainable development is established through the impact that investments in cybersecurity have on business continuity and the protection of organizations' digital assets. By ensuring the security of information and technology infrastructure, businesses can mitigate risks, protect data privacy, and maintain the trust of customers and business partners. This cyber protection contributes to the sustainability of business operations and the fulfillment of long-term organizational objectives. In addition, by strengthening cybersecurity, organizations can reduce the negative impact of potential cyber incidents on the environment, society, and economy, thus promoting sustainable development in the digital realm.

Based on literature review.

In summary, the results show how cybersecurity not only acts as a protective shield for information and systems but is also a critical strategic tool for promoting sustainable business practices. The findings highlight that cybersecurity contributes significantly to economic sustainability by protecting digital and physical assets, which in turn helps companies avoid costs associated with data breaches and cyber-attacks. These aspects are critical to maintaining financial stability and market confidence. Regarding environmental sustainability, cybersecurity makes implementing and maintaining more efficient and less environmentally damaging technological operations possible. This includes protecting critical infrastructures that support sustainable operations, such as renewable energy and natural resource management systems. Finally, regarding social sustainability, cybersecurity is essential to protect users' data and ensure equity in access to technology, thus promoting a more inclusive and just society. These links establish how cybersecurity can and should be integrated within sustainable development strategies in companies, underscoring the importance of including cybersecurity in strategic planning for meeting sustainability goals. These findings reinforce the need for a holistic approach that considers cybersecurity an integral element of sustainable development in the business context.

3.10. Aspects of Methodology and Technique

Table 11, presented below, provides a meticulous classification of various research in the field of cybersecurity, segmenting them according to their research methodology. According to Wacker's epistemology (1998) [38], the various methodologies complement each other to address the same phenomenon from different facets. This scheme ranges from conceptual and analytical approaches through empirical methodologies such as mathematical studies, statistics, experimental design, and statistical sampling to detailed case studies. Through this methodological diversification, it is possible to appreciate the richness and depth with which the authors approach the topic of cybersecurity, reflecting the complexity and multifaceted nature of this field.

Table 11. Methodological approaches used in research on cybersecurity and sustainable development.

Research		Analytic			Empirical	
	Conceptual	Mathematician	Statistical	Experimental Design	Statistical Sampling	Case Study
Abdul-hamid et al. [47]	✓	✓				
Calabrese [49]		✓			✓	
Litvinenko et al. [32]						✓
Sulich et al. [50]		✓				✓
Muhammad et al. [51]	✓					
Rodger and George [20]			✓			
Laskurain-Iturbe et al. [33]			✓			
Gupta et al. [44]					✓	
Malatji et al. [36]						✓
Gutierrez et al. [54]					✓	
Polverini et al. [68]						✓
Fernández et al. [55]	✓					
Najaf et al. [48]						
Fraga-Lamas and Fernández-Caramés [21]	✓					
Chun [34]		✓				
Annarelly and Palombi [56]	✓					
Arcuri et al. [22]					✓	
Abbas et al. [57]					✓	
Jerman et al. [58]					✓	
Fan et al. [59]	✓					
D'Adamo et al. [60]	✓				✓	
Hu et al. [61]	✓				✓	
Soltovsvki et al. [65]	✓					
D'Arcy and Basoglu [66]					✓	
Sidibé and Olabisi [67]						✓
Murch et al. [45]	✓					
Sadik et al. [63]	✓					
Cassota and Sidortov [64]	✓					

Table 11. *Cont.*

		Analytic			Empirical	
Research	**Conceptual**	**Mathematician**	**Statistical**	**Experimental Design**	**Statistical Sampling**	**Case Study**
Ghobakhlo et al. [23]	✓					✓
Ram et al. [24]	✓					
Naffa and Fain [26]		✓	✓			
Bondarenko et al. [25]	✓					
Radu and Smaili [28]	✓				✓	
Okpa et al. [29]			✓		✓	
Wang et al. [31]		✓	✓	✓		
Škerháková et al. [30]					✓	
Shaikh and Siponen [27]		✓			✓	

Based on literature review. The checkmarks [✓] indicate the aspect covered by each investigation.

Each entry in the table highlights the main focus of the study conducted by the author(s) and provides a bird's-eye view of the prevailing methodological trends in cybersecurity research. This ranking demonstrates the dynamism and constant evolution in how cybersecurity is researched, underscoring the importance of employing multiple approaches to understanding and addressing the challenges presented by this critical field. It also shows the technical and methodological gaps in the literature for a comprehensive approach to the relationship between cybersecurity and sustainable development.

After a meticulous analysis of the methodologies and techniques used to investigate the relationship between cybersecurity and sustainable development, it is possible to address one of the critical research questions, which inquires into the conceptual and methodological approaches employed in this study. The findings in this section reveal the use of diverse methodologies to address the complexity of the interaction between cybersecurity and sustainable development. Analytical and conceptual studies predominate, while empirical studies, both statistical and case studies, are less frequent. There is a notable call to deepen the relationship between cybersecurity and sustainability through empirical methods.

4. Discussion

The bibliometric and systematic review study has addressed the intersection between cybersecurity and sustainable development by analyzing 41 articles published between 2014 and 2024. Through the analysis of the definitions, dimensions, indicators, and methodological approaches employed in this research, patterns, trends, and areas of opportunity in this emerging field have been identified.

Definitions of cybersecurity have evolved from implicit concepts based on external sources to more complete and detailed definitions covering various technical, organizational, legal, and cultural aspects. There is also evidence of an adaptation of definitions to specific contexts, such as e-commerce, the automotive industry, and healthcare, highlighting the relevance of cybersecurity in various sectors and its impact on the protection of sensitive data and user trust.

From a sustainable development perspective, cybersecurity is crucial to the sustainability of various sectors, such as the natural gas supply chain and e-commerce. Protecting systems, networks, and data against unauthorized access and cyber-attacks is essential to ensure the continuity and resilience of these industries, thus contributing to sustainable development. In addition, cybersecurity plays a crucial role in protecting the privacy and security of users' personal and financial information, which are fundamental aspects for fostering participation in the digital economy and promoting inclusive and sustainable development.

The dimensions and indicators of cybersecurity and sustainability observe a wide range of factors, covering technical, organizational, legal, and cultural aspects, as well as economic, environmental, and social aspects. Issues such as the circular economy, energy consumption reduction, waste management, energy efficiency, emissions reduction, governance, and social equity stand out, highlighting their interconnection with cybersecurity.

The study's results underline the importance of cybersecurity in protecting critical infrastructure and mitigating financial risks, which supports companies' economic sustainability. In this regard, authors such as Ghobakhlo et al. [23], and Ram et al. [24] have highlighted how cybersecurity ensures reliability and communication between interconnected devices in the framework of Industry 4.0, being fundamental for the continuity of business operations and the protection of information assets.

Naffa and Fain [26] highlight cybersecurity as fundamental to digital asset protection and privacy, underscoring its role in the long-term sustainability of organizations. This perspective is reflected in the findings of the study, which present cybersecurity as key to business continuity and the protection of stakeholders' interests, directly contributing to economic sustainability. In addition, Škerháková et al. [30] highlight that cybersecurity is essential to maintain financial stability and reputation, which is crucial in a safe and sustainable business environment in today's digital economy.

Regarding environmental sustainability, the study highlights how cybersecurity facilitates the implementation of clean and efficient technology. Authors such as Litvinenko [32] have explored this point by describing how digitization and cybersecurity can drive sustainability in sectors such as mining by optimizing resource use and minimizing environmental impact.

Concerning social sustainability, cybersecurity is essential to protect data privacy and foster an organizational culture of trust and accountability. This point aligns with the observations of Wang et al. [31], who argue that effective cybersecurity management not only protects digital assets but also strengthens stakeholder trust, a crucial aspect of social well-being and cohesion.

On the other hand, the study's results also reflect the ideas of Radu and Smaili [28], who point out that cyber-attacks can have severe financial and reputational repercussions, affecting consumer trust and privacy. Protection against these risks is vital to ensure a safe and sustainable environment. It is directly related to social sustainability through protecting personal data and promoting a culture of responsibility and trust. Shaikh and Siponen [27] argue that investments in cybersecurity are critical for business continuity and the protection of digital assets, which mitigates risks and supports sustainable development in the digital realm, reducing the negative impact of cyber incidents on the environment, society, and economy.

Finally, the methodological approaches used to study these relationships, mainly through systematic reviews and bibliometric analyses, are consistent with the recommendations of authors such as Snyder [41], who emphasizes the importance of rigorous methodologies to address complex phenomena in scientific research. Various methodological approaches are observed, from conceptual and analytical studies to empirical methodologies such as mathematical studies, statistics, experimental design, statistical sampling, and case studies. This methodological diversification reflects cybersecurity's complexity, multifaceted nature, and relationship to sustainable development.

Compared to other bibliometric studies on cybersecurity, this work is distinguished by its focus on exploring the relationship between cybersecurity and sustainable development. While research such as Cui et al. [70] focuses on the extensive data ecosystem in manufacturing and Ganji and Afshan [71] address cybersecurity in the context of the Internet of Things (IoT), our study seeks to provide a comprehensive and holistic view of how cybersecurity and sustainable development intertwine and influence each other, generating new insights and knowledge in this field.

In summary, the paper's discussion provides a holistic view of how cybersecurity influences sustainable development, drawing on relevant literature and answering the research questions. This analysis highlights the interdependence between cybersecurity and sustainability and underscores the need to continue exploring this relationship through empirical studies and innovative methodologies.

5. Conclusions

This bibliometric study focused on analyzing the relationship between cybersecurity and sustainable development, highlighting the importance of addressing this issue from a multidimensional perspective that involves social, environmental, and economic aspects. As a complex and multidimensional topic, cybersecurity requires a holistic approach to address questions and concerns beyond simple figures and statistics.

Key terms such as big data, artificial intelligence, privacy, risk management, and policy reveal the interconnectedness between cybersecurity and sustainable development. Cybersecurity ensures data reliability in a data-driven world and protects the integrity of digital systems and processes in various sustainable fields. In addition, it underlines the importance of privacy in the digital age and how cybersecurity contributes to maintaining trust in the technology underlying sustainable development.

The analysis of scientific production on cybersecurity and sustainable development shows steady publication growth. This increase indicates a growing interest in and recognition of the relevance of this thematic intersection. In addition, leading institutions that have contributed significantly to the field are identified, demonstrating an outstanding focus on research in this area.

As for the studies that were analyzed to determine the dimensions and variables addressed in the study, as well as the elements that linked cybersecurity with sustainable development, they highlight the importance of cybersecurity in promoting critical aspects of sustainable development, ranging from socioeconomic and environmental interactions to the adoption of emerging technology. Cybersecurity is essential to balance innovation, security, and sustainability in contemporary society.

Cybersecurity contributes significantly to companies' economic sustainability by protecting critical infrastructures and minimizing financial risks, ensuring the continuity of business operations and the protection of stakeholders' interests. Regarding environmental sustainability, cybersecurity facilitates the implementation of cleaner and more efficient technology, protecting the systems that manage energy resources and thus reducing environmental impact. Social sustainability strengthens the protection of personal data and fosters a culture of responsibility and trust within organizations, contributing to social equity.

In addition, the reviewed studies use methodologies ranging from systematic reviews to case studies, underscoring the complexity of studying the interactions between cybersecurity and sustainable development. However, more empirical research that combines qualitative and quantitative approaches is needed to explore further how cybersecurity can be incorporated into corporate sustainability policies. Deepening empirical research that explores this relationship is recommended to design more effective strategies that integrate cybersecurity within the framework of sustainable development.

Finally, this bibliometric study offers a structured and in-depth view of the relationship between cybersecurity and sustainable development. Cybersecurity is critical to support progress toward a sustainable future by protecting essential data, systems, and technology. This research not only offers a rigorous analysis of scientific output in the field but also provides a solid foundation for developing theoretical models for future research and scientific breakthroughs in this crucial area for contemporary society.

6. Gaps in the Literature and Future Lines of Research

This bibliometric study and systematic review have identified several gaps in the existing literature on the intersection between cybersecurity and sustainable development. These gaps represent opportunities for future research to deepen understanding of this relationship and address the challenges posed by the digital age for a sustainable future.

First, further research is needed that explicitly addresses the connection between cybersecurity and sustainable development. While many studies explore this intersection, some works still need an explicit connection. Future research could establish stronger and clearer links between these two fields, exploring how cybersecurity practices can directly contribute to the Sustainable Development Goals.

In addition, a gap in research related to the social aspects of cybersecurity and sustainable development is identified. While environmental and economic aspects have received increased attention, the societal impacts of cybersecurity in the context of sustainability require further analysis. Future research could address digital equity, social inclusion, and empowering communities through socially responsible cybersecurity practices.

There is also an opportunity to conduct comparative studies between different sectors and geographical contexts. While some studies address specific industries, such as e-commerce or healthcare, a broader exploration of how cybersecurity and sustainable development are intertwined across various sectors and regions is required. This would allow identifying best practices, common challenges, and solutions adapted to different contexts.

Methodologically, the literature calls for developing empirical research designs that can qualitatively study cases of sustainable cybersecurity in specific companies. Likewise, there is a call for statistical sample cut designs that allow a scope of association with greater representativeness in the sectors. In addition, the need for research addressing the temporal dimension of cybersecurity and sustainable development has also been identified. Most studies focus on a specific point in time, limiting understanding of how this relationship evolves. Future research could take longitudinal approaches to examine how cybersecurity practices and sustainability considerations change and adapt in response to technological advances and societal demands.

The literature review reveals several significant gaps in the study of the relationship between cybersecurity and sustainable development, especially in the business context. One of the main areas for improvement identified is the need for empirical studies exploring the direct impacts of cybersecurity on the three dimensions of sustainability: economic, environmental, and social. Although there is theoretical and analytical research, quantitative data must support the proposed theories. In addition, considerable variability is observed in the conceptualization and application of cybersecurity between different sectors and industries, suggesting the need to develop more adaptive and context-specific strategies.

To address these gaps, future research using mixed methodologies, combining qualitative and quantitative approaches, is recommended to gain a deeper and more nuanced understanding of how cybersecurity can influence each aspect of sustainability. It is crucial to study specific cases within varied industries to examine how cybersecurity practices are implemented and perceived in different environments. In addition, it would be beneficial to explore how cybersecurity policies influence corporate sustainability in emerging and developing markets, where security practices may differ significantly from those in developed markets. It is also suggested that the impact of cybersecurity on environmental sustainability, a relatively unexplored area, be investigated to understand how secure practices can contribute to cleaner and more efficient operations.

Finally, more research is needed to be related to the practical implementation of sustainable cybersecurity. While conceptual and analytical studies are valuable, more applied research is required that explores how organizations can effectively integrate cybersecurity and sustainability into their operations and strategies. This could include developing frameworks, tools, and metrics to assess and improve sustainable cybersecurity performance.

Undoubtedly, the gaps identified in the literature on the intersection between cybersecurity and sustainable development present exciting opportunities for future research. By addressing these gaps, researchers can contribute to a more complete and nuanced understanding of how cybersecurity can catalyze a sustainable future. These future lines of research will enrich academic knowledge and inform decision-makers and practitioners in developing strategies and practices that integrate cybersecurity and sustainability effectively.

7. Managerial Implications

The intersection between cybersecurity and sustainable business development is a multidimensional field that encompasses economic, environmental, and social aspects. Cybersecurity, defined as protecting computer systems, networks, and data from unauthorized access, attacks, and damage, plays a crucial role in the sustainability of business operations in the digital age. Through a detailed analysis of the academic research provided, several links between cybersecurity and the principles of sustainable business development can be identified. Practical examples illustrating how companies can achieve environmental, social, and economic sustainability through cybersecurity and how sustainability can strengthen cybersecurity practices include:

i. Implementing clean and efficient technology where cybersecurity protects the systems that manage renewable energies and other environmental resources allows companies to reduce their carbon footprint and improve their energy efficiency. A specific example is using blockchain technology to improve traceability and security in renewable energy supply chains, ensuring that energy consumption and production data are reliable and cannot be maliciously altered [21].

ii. The protection of personal data and privacy is a key aspect of cybersecurity. Robust cybersecurity measures help protect the personal information of customers and employees, fostering trust and social fairness. A specific example of this aspect is compliance with the General Data Protection Regulation (GDPR) in Europe, which requires companies to adopt strong cybersecurity policies to protect users' privacy.

iii. Business continuity and financial risk reduction are significant benefits of cybersecurity. Companies can use cybersecurity to protect against service interruptions and cyber-attacks, ensuring business continuity and minimizing economic losses. Specifically, the implementation of advanced cybersecurity solutions, such as artificial intelligence, to detect and respond to threats in real time can mean significant savings in the long term.

iv. Strengthening Cybersecurity through Sustainability through sustainability initiatives that strengthen cybersecurity. By implementing sustainability strategies that include cybersecurity training and awareness, companies protect the environment and strengthen their defenses against cyber-attacks. A specific example is training employees to securely manage electronic devices and data, which can significantly reduce the risk of security incidents [26].

These practical examples illustrate how management can integrate cybersecurity into business practices to protect against digital threats and support the company's sustainability goals at various levels, creating a win-win cycle between cybersecurity and sustainability.

In short, cybersecurity and sustainable business development are intrinsically interconnected, as they pursue common goals of asset protection, risk mitigation, and promotion of trust and transparency. By integrating cybersecurity considerations into business decision-making, organizations can move towards a more resilient, responsible, and sustainable business model in an ever-evolving digital environment.

Author Contributions: Conceptualization, F.I.M.-S.; methodology, F.I.M.-S.; software, M.R.-C.; validation, J.M.M.-Q., M.R.-C. and F.I.M.-S.; formal analysis, M.R.-C.; investigation, F.I.M.-S.; resources, M.R.-C.; data curation, M.R.-C.; writing—original draft preparation, J.M.M.-Q.; writing—review and editing, M.R.-C.; visualization, M.R.-C.; supervision, J.M.M.-Q.; project administration, F.I.M.-S.; funding acquisition, F.I.M.-S. All authors have read and agreed to the published version of the manuscript.

Funding: Francisco Isaí Morales-Sáenz gratefully acknowledges funding through the Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT) grant number CVU-853204.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Al-Sibai, H.; Alrubaie, T.; Elmedany, W. IoT cybersecurity threats mitigation via integrated technical and non-technical solutions. *Int. J. Electron. Secur. Digit. Forensics* **2021**, *13*, 298–333. [CrossRef]
2. Darem, A. Anti-Phishing Awareness Delivery Methods. *Eng. Technol. Appl. Sci. Res.* **2021**, *11*, 7944–7949. [CrossRef]
3. Taherdoost, H. Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics* **2022**, *11*, 2181. [CrossRef]
4. Arroyabe, I.; Arranz, C.; Arroyabe, M.; Arroyabe, J. Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Comput. Secur.* **2023**, *124*, 102954. [CrossRef]
5. Abidi, N.; El Herradi, M.; Sakha, S. Digitalization and resilience during the COVID-19 pandemic? *Telecommun. Policy* **2023**, *47*, 102522. [CrossRef] [PubMed]
6. Sendur, Y. The Covid-19 Pandemic and Digitalization in Financial Markets. *Istanb. J. Econ.* **2022**, *72*, 1025–1038. [CrossRef]
7. García-Perez, A.; Sallos, M.; Tiwasing, P. Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: An intellectual capital perspective. *J. Intellect. Cap.* **2023**, *24*, 465–486. [CrossRef]
8. Bodin, L.; Gordon, L.; Loeb, M.; Wang, A. Cybersecurity insurance and risk-sharing. *J. Account. Public Policy* **2018**, *37*, 527–544. [CrossRef]
9. Williams, C.; Chaturvedi, R.; Chakravarthy, K. Cybersecurity Risks in a Pandemic. *J. Med. Internet Res.* **2020**, *22*, e23692. [CrossRef]
10. Al-Qahtani, A.; Cresci, S. The COVID-19 scamdemic: A survey of pishing attacks and their countermeasures during COVID-19. *IET Inf. Secur.* **2022**, *16*, 324–345. [CrossRef]
11. Berlilana; Noparumpa, T.; Ruangkanjanases, A.; Hariguna, T.; Sarmini. Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. *Sustainability* **2021**, *13*, 13761. [CrossRef]
12. Silaule, C.; Makhubele, L.; Mamorobela, S. A model to reduce insider cybersecurity threats in a South African telecommunications company. *S. Afr. J. Inf. Manag.* **2022**, *24*, 1573. [CrossRef]
13. Suomalainen, J.; Juhola, A.; Shahabuddin, S.; Mammela, A.; Ahmad, I. Machine Learning Threatens 5G Security. *IEEE Access* **2020**, *8*, 190822–190842. [CrossRef]
14. World-Bank-Group. Internet Crime Complaint Center IC3. 2021. Available online: https://www.ic3.gov/ (accessed on 1 July 2024).
15. Lee, I. Cybersecurity: Risk management framework and investment cost analysis. *Bus. Horiz.* **2021**, *64*, 659–671. [CrossRef]
16. Buil-Gil, D.; Lord, N.; Barret, E. The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. *Vict. Offenders* **2021**, *16*, 286–315. [CrossRef]
17. Nugraha, Y.; Martin, A. Cybersecurity service level agreements: Understanding government data confidentiality requirements. *J. Cybersecur.* **2022**, *8*, tyac004. [CrossRef]
18. Morales-Sáenz, F.; Medina-Quintero, J.; Ortíz-Rodríguez, F. Bibliometrics Study of Organizational Cybersecurity. In *Emerging Technologies and Digital Transformation in the Manufacturing Industry*; IGI Global: Hershey, PA, USA, 2023; pp. 115–139.
19. Sabillon, R. A Practical Model to Perform Comprehensive Cybersecurity Audits. *Enfoque UTE* **2018**, *9*, 127–137. [CrossRef]
20. Rodger, J.A.; George, J.A. Triple bottom line accounting for optimizing natural gas sustainability: A statistical linear programming fuzzy ILOWA optimized sustainment model approach to reducing supply chain global cybersecurity vulnerability through information and communications technology. *J. Clean. Prod.* **2017**, *142*, 1931–1949. [CrossRef]
21. Fraga-Lamas, P.; Fernández-Caramés, T. A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. *IEEE Access* **2019**, *7*, 17578–17598. [CrossRef]
22. Arcuri, M.C.; Gai, L.; Ielasi, F.; Ventisette, E. Cyber attacks on hospitality sector: Stock market reaction. *J. Hosp. Tour. Technol.* **2020**, *11*, 277–290. [CrossRef]
23. Ghobakhloo, M.; Fathi, M. Corporate survival in Industry 4.0 era: The enabling role of lean-digitized manufacturing. *J. Manuf. Technol. Manag.* **2019**, *31*, 1–30. [CrossRef]
24. Ram, J.; Zhang, Z. Belt and road initiative (BRI) supply chain risks: Propositions and model development. *Int. J. Logist. Manag.* **2020**, *31*, 777–799. [CrossRef]
25. Bondarenko, L.; Moroz, N.; Zhelizniak, R.; Bonetskyy, O. Fintech market development in the world and in Ukraine. *Financ. Credit Act. Probl. Theory Pract.* **2022**, *6*, 121–127. [CrossRef]
26. Naffa, H.; Fain, M. Performance measurement of ESG-themed megatrend investments in global equity markets using pure factor portfolios methodology. *PLoS ONE* **2020**, *15*, e0244225. [CrossRef]
27. Shaikh, F.A.; Siponen, M. Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Inf. Syst. Front.* **2024**, *26*, 1109–1120. [CrossRef]
28. Radu, C.; Smaili, N. Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure. *J. Bus. Ethics* **2022**, *177*, 351–374. [CrossRef]
29. Okpa, J.T.; Ajah, B.O.; Nzeakor, O.F.; Eshiotse, E.; Abang, T.A. Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Secur. J.* **2023**, *36*, 350–372. [CrossRef]
30. Skerhakova, V.; Taha, V.A.; Tirpák, D.; Kral', S. Perception of Corporate Reputation in the Era of Digitization: Case Study of Online Shopping Behavior on Young Consumers. *Sustainability* **2022**, *14*, 14302. [CrossRef]
31. Wang, G.; Tse, D.; Cui, Y.; Jiang, H. An Exploratory Study on Sustaining Cyber Security Protection through SETA Implementation. *Sustainability* **2022**, *14*, 8319. [CrossRef]

32. Litvinenko, V. Digital Economy as a Factor in the Technological Development of the Mineral Sector. *Nat. Resour. Res.* **2020**, *29*, 1521–1541. [CrossRef]
33. Laskuraín-Iturbe, I.; Arana-Landín, G.; Landeta-Manzano, B.; Uriarte-Gallastegi, N. Exploring the influence of industry 4.0 technologies on the circular economy. *J. Clean. Prod.* **2021**, *321*, 128944. [CrossRef]
34. Chun, S.H. E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability. *Sustainability* **2019**, *11*, 715. [CrossRef]
35. Shackelford, S.; Fort, T.; Charoen, D. Sustainable cybersecurity: Applying lessons from the green movement to managing Cyber Attacks. *U. Ill. L. Rev.* **2016**, 1995. [CrossRef]
36. Malatji, M.; Marnewick, A.; von Solms, S. Validation of a socio-technical management process for optimising cybersecurity practices. *Comput. Secur.* **2020**, *95*, 101846. [CrossRef]
37. Burgess, K.; Singh, P.; Koroglu, R. Supply chain management: A structured literature review and implications for future research. *Int. J. Oper. Prod. Manag.* **2006**, *26*, 703–729. [CrossRef]
38. Wacker, J.G. A definition of theory: Research guidelines for different theory-building research methods in operations management. *J. Oper. Manag.* **1998**, *16*, 361–385. [CrossRef]
39. Goyanes, M.; Demeter, M. How the geographic diversity of editorial boards affects what is published in JCR-Ranked communication journals. *Journal. Mass Commun. Q.* **2020**, *97*, 1123–1148. [CrossRef]
40. Kipper, L.; Furstenau, L.; Hoppe, D.; Frozza, R.; Lespen, S. Scopus scientific mapping production in industry 4.0 (2011–2018): A bibliometric analysis. *Int. J. Prod. Res.* **2019**, *58*, 1605–1627. [CrossRef]
41. Snyder, H. Literature review as a research methodology: An overview and guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [CrossRef]
42. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef]
43. Vaccaro, G.; Sánchez-Núñez, P.; Witt-Rodríguez, P. Bibliometrics Evaluation of Scientific Journals and Country Research Output of Dental Research in Latin America Using. *Scimago J. Ctry. Rank Publ.* **2022**, *10*, 26. [CrossRef]
44. Gupta, S.; Meissonier, R.; Drave, V.; Roubaud, D. Examining the impact of Cloud ERP on sustainable performance: A dynamic capability view. *Int. J. Inf. Manag.* **2020**, *51*, 102028. [CrossRef]
45. Murch, R.; So, W.; Buchholz, W.; Raman, S.; Peccoud, J. Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. *Front. Bioeng. Biotechnol.* **2018**, *6*, 39. [CrossRef] [PubMed]
46. Henrandez-de Mendenez, M.; Escobar, C.; Morales-Menendez, R. Engineering education for smart 4.0 technology: A review. *Int. J. Interact. Des. Manuf.* **2020**, *14*, 789–803. [CrossRef]
47. Adbul-Hamid, A.; Ali, M.; Osman, L.; Tseng, M. The drivers of industry 4.0 in a circular economy: The palm oil industry in Malaysia. *J. Clean. Prod.* **2021**, *324*, 129216. [CrossRef]
48. Najaf, K.; Mostafiz, M.; Najaf, R. Fintech firms and banks sustainability: Why cybersecurity risk matters? *Int. J. Financ. Eng.* **2021**, *8*, 2150019. [CrossRef]
49. Calabrese, A.; Costa, R.; Tiburzi, L.; Brem, A. Merging two revolutions: A human-artificial intelligence method to study how sustainability and Industry 4.0 are intertwined. *Technol. Forecast. Soc. Chang.* **2023**, *188*, 122265. [CrossRef]
50. Sulich, A.; Rutkowska, M.; Krawczyk-Jezierska, A.; Jezierski, J.; Zema, T. Cybersecurity and Sustainable Development. *Procedia Comput. Sci.* **2021**, *192*, 20–28. [CrossRef]
51. Muhammad, Z.; Anwar, Z.; Saleem, B.; Shahid, J. Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability. *Energies* **2023**, *16*, 1113. [CrossRef]
52. Lim, H.; Taeihagh, A. Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications. *Energies* **2018**, *11*, 1062. [CrossRef]
53. Ramírez, M.; Ariza, L.R.; Miranda, M.E.G.; Vartika. The Disclosures of Information on Cybersecurity in Listed Companies in Latin Americaâ€”Proposal for a Cybersecurity Disclosure Index. *Sustainability* **2022**, *14*, 1390. [CrossRef]
54. Ponce, H.G.; González, J.C.; Al-Mohareb, M. Sustainable finance in cybersecurity investment for future profitability under uncertainty. *J. Sustain. Financ. Invest.* **2023**, *13*, 614–633. [CrossRef]
55. Fernandez, C.M.; Alves, J.; Gaspar, P.D.; Lima, T.M. Fostering Awareness on Environmentally Sustainable Technological Solutions for the Post-Harvest Food Supply Chain. *Processes* **2021**, *9*, 1611. [CrossRef]
56. Annarelli, A.; Palombi, G. Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. *Sustainability* **2021**, *13*, 13065. [CrossRef]
57. Abbas, H.S.M.; Qaisar, Z.H.; Ali, G.; Alturise, F.; Alkhalifah, T. Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. *PLoS ONE* **2022**, *17*, e0274550. [CrossRef]
58. Blažič, B.J.; Blažič, A.J. Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. *Sustainability* **2022**, *14*, 4763. [CrossRef]
59. Fan, Y.; Li, J.; Zhang, D.; Pi, J.; Song, J.; Zhao, G. Supporting Sustainable Maintenance of Substations under Cyber-Threats: An Evaluation Method of Cybersecurity Risk for Power CPS. *Sustainability* **2019**, *11*, 982. [CrossRef]
60. D'Adamo, I.; González-Sánchez, R.; Medina-Salgado, M.S.; Settembre-Blundo, D. Methodological Perspective for Assessing European Consumers´ Awareness of Cybersecurity and Sustainability in E-Commerce. *Sustainability* **2021**, *13*, 11343. [CrossRef]

61. Hu, J.L.; Chen, Y.C.; Yang, Y.P. The Development and Issues of Energy-ICT: A Review of Literature with Economic and Managerial Viewpoints. *Energies* **2022**, *15*, 594. [CrossRef]
62. Shackelford, S. Exploring the Shared Responsibilityy of Cyber Peace: Should Cybersecurity Be a Human Right? *SSRN Electron. J.* **2017**. [CrossRef]
63. Sadik, S.; Ahmed, M.; Sikos, L.F.; Islam, A.K.M.N. Toward a Sustainable Cybersecurity Ecosystem. *Computers* **2020**, *9*, 74. [CrossRef]
64. Cassotta, S.; Sidortsov, R. Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. *Energy Res. Soc. Sci.* **2019**, *51*, 129–133. [CrossRef]
65. Soltovski, R.; de Resende, L.M.M.; Pontes, J.; Yoshino, R.T.; da Silva, L.B.P. Um estudo quantitativo sobre os riscos da indústria 4.0 no contexto industrial: Uma revisão sistemática da literatura. *Rev. Gestão Desenvolv.* **2020**, *17*, 165. [CrossRef]
66. D'Arcy, J.; Basoglu, A. The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. *J. Assoc. Inf. Syst.* **2022**, *23*, 779–805. [CrossRef]
67. Sidibé, A.; Olabisi, L.S.; Doumbia, H.; Touré, K.; Niamba, C.A. Barriers and enablers of the use of digital technologies for sustainable agricultural development and food security. *Elem. Sci. Anthr.* **2021**, *9*, 00106. [CrossRef]
68. Polverini, D.; Ardente, F.; Sanchez, I.; Mathieux, F.; Tecchio, P.; Beslay, L. Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process. *Comput. Secur.* **2018**, *76*, 295–310. [CrossRef]
69. Shackelford, S. Shoul cybersecurity be a human right? Exploring the Shared responsibillity of cyberpeace. In *Music, Business and Peacebuilding*; Routledge: London, UK, 2021; pp. 174–197.
70. Cui, Y.; Kara, S.; Chan, K. Manufacturing big data ecosystem: A systematic literature review. *Robot. Comput.-Integr. Manuf.* **2020**, *62*, 101861. [CrossRef]
71. Ganji, K.; Afshan, N. A bibliometric review of Internet of Things (IoT) on cybersecurity issues. *J. Sci. Technol. Policy Manag.* **2024**, *ahead-of-print*. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.