information

MDPI

Article

Cybersecurity as a Contributor Toward Resilient Internet of Things (IoT) Infrastructure and Sustainable Economic Growth

Georgia Dede [1,2,†], Anastasia Maria Petsa [2,†], Stelios Kavalaris [2,†], Emmanouil Serrelis [3,†], Spyridon Evangelatos [2,†], Ioannis Oikonomidis [2] and Thomas Kamalakis [1,*]

[1] Department of Informatics and Telematics, Harokopio University of Athens, 17671 Athens, Greece; gdede@hua.gr or georgia.dede@netcompany.com
[2] Netcompany Intrasoft S.A., L-1253 Luxembourg, Luxembourg; anastasiamaria.petsa@netcompany.com (A.M.P.); stelios.kavalaris@netcompany.com (S.K.); spyros.evangelatos@netcompany.com (S.E.); yannis.oikonomidis@netcompany.com (I.O.)
[3] Alphabet Education (AKMI-Metropolitan) Group, 15125 Athens, Greece; eserrelis@mitropolitiko.edu.gr
* Correspondence: thkam@hua.gr
† These authors contributed equally to this work.

Abstract: This paper investigates the contribution of the various cybersecurity domains to the United Nations' Sustainable Development Goals (SDGs), emphasizing the critical role of cybersecurity in advancing sustainable economic growth and resilient IoT infrastructure. The paper also examines specific use cases on how cybersecurity measures and practices can contribute to achieving SDG 8 and SDG 9 focused on decent work and economic growth and industry, innovations, and infrastructure. In the context of SDG 8 the use case of a smart agriculture network was examined, whereas for SDG 9, the use case focuses on a smart factory processing raw materials. An analysis of the prioritization of the several cybersecurity domains following the MoSCoW method is also presented. This paper offers valuable insights and guidance for enhancing corporate resilience and economic benefits in the Internet of Things (IoT) aligning with the SDGs and contributing to a more sustainable and resilient future for the IoT.

Keywords: sustainability; cybersecurity; Sustainable Development Goals; economic growth; resilient infrastructure

Citation: Dede, G.; Petsa, A.M.; Kavalaris, S.; Serrelis, E.; Evangelatos, S.; Oikonomidis, I.; Kamalakis, T. Cybersecurity as a Contributor Toward Resilient Internet of Things (IoT) Infrastructure and Sustainable Economic Growth. *Information* **2024**, *15*, 798. https://doi.org/10.3390/info15120798

Academic Editor: Krzysztof Szczypiorski

Received: 31 August 2024
Revised: 31 October 2024
Accepted: 13 November 2024
Published: 11 December 2024

1. Introduction

The United Nations' 17 Sustainable Development Goals (SDGs) stand as a comprehensive framework aimed at addressing global challenges and fostering a sustainable, equitable, and resilient future [1]. Established in 2015, the SDGs encompass a range of objectives, from ending poverty and hunger to ensuring clean water, quality education, gender equality, and climate action, among others. The interconnected nature of these goals reflects a holistic approach to promoting social, economic, and environmental well-being on a global scale.

In the modern era, the pervasive integration of digital technologies and the increasing reliance on interconnected systems underscore the critical need for robust cybersecurity measures. As societies, economies, and critical infrastructure become more digitized, the potential risks and vulnerabilities associated with cyber threats have grown exponentially.

The digital age is marked by the widespread integration of technologies. This increasing reliance on interconnected systems has transformed societies and economies. While this digital transformation offers immense opportunities for progress, it also presents significant challenges, with cybersecurity emerging as a critical factor in realizing the SDGs. The exponential growth of Internet of Things (IoT) devices, coupled with the vulnerability of critical infrastructure, has heightened the risk of cyberattacks, which can undermine economic growth, hinder innovation, and exacerbate social inequalities.

Cybersecurity is no longer merely a technical concern but has evolved into a fundamental aspect of ensuring the stability, security, and sustainability of our interconnected world. Cyber threats, ranging from data breaches and ransomware attacks to disruptions in critical infrastructure, have the capacity to undermine progress toward achieving the SDGs. For instance, an attack on financial systems could affect the economic growth and resilience in IoT infrastructures, while a cyber incident targeting healthcare infrastructure could hinder efforts to promote good health and well-being.

Moreover, as the digital landscape expands, the need to secure data and information becomes paramount in achieving goals related to innovation, economic growth, and responsible consumption. Cybersecurity not only safeguards sensitive information but also facilitates trust in digital transactions and fosters an environment conducive to technological advancements that align with the SDGs.

In this context, the paper seeks to explore and elucidate the multifaceted relationship between the SDGs and cybersecurity. By identifying specific contributions of cybersecurity to each SDG and providing examples of good practices, the paper aims to underscore the integral role of cybersecurity in advancing the global agenda for sustainable development. As we navigate an era marked by rapid technological advancements, understanding and addressing cybersecurity challenges become essential for realizing the vision of a sustainable and inclusive future outlined by the SDGs. The analysis is based on the National Institute of Standards and Technology (NIST) 800-53 r5 cybersecurity framework [2]. By examining specific use cases, such as those related to SDG 8: Decent Work and Economic Growth [3] and SDG 9: Industry, Innovation, and Infrastructure [4], this research aims to demonstrate the impact of cybersecurity measures and practices on sustainable development. The paper further emphasizes the critical role of cybersecurity in building resilient IoT infrastructure and fostering sustainable economic growth. Ensuring the resilience of critical infrastructure, cybersecurity can minimize disruptions, protect livelihoods, and support sustainable industrial development. SDG 8 and SDG 9 constitute the SDGs' dimensions of economic and technological development focused on economic growth, sustainable industrialization and innovation.

The rest of the paper is organized as follows: In Section 2, the related work is analyzed. In Section 3, a background overview is presented. Section 4 summarizes the methodology followed in this paper. The results related to the general contribution of cybersecurity to the SDGs are presented in Section 5. Section 6 describes the specific results based on the use cases of SDG 8 and SDG 9. Finally, some future considerations and concluding remarks are presented in Section 7.

2. Related Work

Inspection of previous literature reveals that there are no research papers that have studied the contribution of cybersecurity to SDGs. More specifically, Ref. [5] analyzes the role of cybersecurity in enhancing economic growth, promoting social inclusivity, and safeguarding environmental sustainability in the context of the 17 SDGs. However, it only provides a high-level discussion without examining specific cybersecurity frameworks. Additionaly, Ref. [6] discusses how achieving the SDGs in cybersecurity using artificial intelligence of things (AIoT) for healthcare application. This work is focused on the specific area of healthcare and is not based on the analysis of specific cybersecurity measures under pub lished cybersecurity frameworks. Moreover, Ref. [7] examines the connection between cybersecurity and the sustainability and resilience capabilities of smart cities in the broader framework of SDG 11, in which the notion of a city's resilience and sustainability is stressed. Finally, Ref. [8] proposes a fuzzy set qualitative comparative analysis technique to identify combinations of security attacks that lead to achieving cybersecurity in connected and automated vehicles and studies its implications to SDGs.

It seems that there is an increasing interest among researchers in investigating cybersecurity aspects with respect to SDG implementa- tion, but our work is the first attempt to examine the security measures of a specific cybersecurity framework and analyze how

these measures may contribute to the achievement of the SDGs. The authors have previously tried to investigate the contribution of cybersecurity to SDGs but emphasized SDG 13, while the current paper focuses on SDG 8 and SDG 9, highlighting resilience in IoT infrastructure and sustainable economic growth. The analysis of the prioritization of cybersecurtiy domains toward their implementation is also examined in this paper.

However, there are also studies that investigate the intersection of cybersecurity and sustainability and the role of cybersecurity in economic growth and IoT resilience. The article [9] investigates the relationships between cybersecurity and sustainable development in the inter-organizational networks. Reference [10] discusses how cybersecurity strategies can align with the SDGs. The study [11] explores the critical intersection of cybersecurity measures and green technologies, aiming to assess their combined impact on sustainability goals and stakeholder implications. In [12], the role of cybersecurity as a major differentiator for organizations and an essential sustainable economic development factor is investigated. Ref. Regarding IoT infrastructure resilience, Ref. [13] presents a critical analysis of the most recent cybersecurity issues for IoT-based critical infrastructures in order to solve cybersecurity challenges. In [14], cybersecurity considerations for industrial automation and control systems that can be adopted in the critical infrastructure sector to implement IoT security were examined.

3. Background

3.1. Information Security Frameworks

In order to identify the potential cybersecurity domains that may contribute to maintaining sustainable development, several popular Information Security Frameworks that include categories of such domains have been examined. These are the Information Security Forum's (ISF) Standard of Good Practice (SoGP) [15], the NIST's CyberSecurity Framework (CSF) [16], the ISO 27002 Information Security Controls [17], and the NIST Special Publication 800-53r5 on "Security and Privacy Controls for Information Systems and Organizations".

All four frameworks (ISF SoGP, NIST CSF, ISO 27002, and NIST 800-53r5) provide guidelines and best practices for managing cybersecurity risks and protecting critical systems and infrastructure. Each of them has its own focus, strengths, and areas of coverage.

The ISF SoGP provides a holistic approach to information security, covering not only cybersecurity but also physical security, personnel security, and other related areas. It provides detailed guidance on security governance and management, technical security controls, and operations. It also includes a section on risk management and incident management.

The NIST CSF provides a risk-based approach to managing cybersecurity, with a focus on identifying, protecting, detecting, responding to, and recovering from cyber incidents. It is widely adopted by organizations across various industries and can be tailored to the specific needs and risk profile of an organization.

ISO 27002 provides a code of practice for information security management, covering security management principles, security management processes, and security management controls. It provides a comprehensive set of guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. NIST Special Publication 800-53r5 is a guideline for the security and privacy controls for federal information systems and organizations. It provides a comprehensive set of security controls, including both management and technical controls, that can be used to protect information systems and data. Based on the comparison of the above for aligning with UN SDGs, NIST 800-53 seems to be better suited for several reasons:

1. *Coverage*: NIST 800-53 provides a comprehensive set of security controls that cover a wide range of security domains that use a systematic ordering, also in terms of numbering and hierarchy. The framework is designed to address various aspects of information security, making it more likely to have controls relevant to different UN SDGs.

2. *Government and International Recognition*: NIST is a U.S. government agency, and NIST 800-53 is widely recognized and adopted not only within the U.S. but also internationally. This recognition can facilitate alignment with global initiatives such as the UN SDGs.
3. *Adaptability*: NIST 800-53 is designed to be adaptable to different organizational structures, sizes, and missions. This adaptability can make it easier to integrate with diverse organizations working toward UN SDGs, which vary widely in their focus and activities.
4. *Risk Management Focus*: NIST 800-53 emphasizes a risk management approach to cybersecurity. Aligning with UN SDGs involves managing risks related to information security that may impact the achievement of Sustainable Development Goals. NIST 800-53's risk-based approach can help organizations prioritize and address cybersecurity challenges in the context of their specific SDGs-related activities.
5. *Maturity Model*: NIST 800-53 includes a maturity model that allows organizations to assess and improve their cybersecurity practices over time. This can be beneficial for organizations working toward UN SDGs, as they can evolve their cybersecurity posture in line with their evolving sustainability initiatives.
6. *Interoperability*: NIST 800-53 is designed to be compatible and interoperable with other cybersecurity standards and frameworks. This flexibility makes it easier for organizations to integrate NIST 800-53 with existing processes and align with other international standards, including those related to sustainability.

3.2. Cybersecurity Domains of NIST 800-53r5

The NIST Special Publication 800-53 Revision 5 (NIST 800-53 r5) is a framework that provides guidelines for securing information systems and managing cybersecurity risk within federal agencies and organizations. The framework is organized into families, each representing a set of security controls that address specific aspects of information security. The controls are categorized into cybersecurity domains, which are crucial components for creating a comprehensive and robust cybersecurity posture. The NIST 800-53 r5 cybersecurity domains include the following families as presented in Table 1.

Table 1. NIST 800-53r5 family controls.

ID	Family	ID	Family
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contigency Plan	RA	Risk Assessment
IA	Identification and Authentication	SA	Systems and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

These cybersecurity domains and controls are designed to help organizations establish a strong cybersecurity foundation, manage risk effectively, and ensure the confidentiality, integrity, and availability of their information systems and data. The NIST 800-53 r5 framework is widely recognized and used not only in the U.S. federal entities but also worldwide by private sector organizations seeking to enhance their cybersecurity practices.

3.3. The United Nations' SDGs

The United Nations' SDGs, officially known as the 2030 Agenda for Sustainable Development, represent a universal call to action to end poverty, protect the planet, and ensure prosperity for all. Adopted by all 193 member states of the United Nations in September

2015, the SDGs provide a comprehensive framework addressing a wide range of global challenges. The goals aim to guide collective efforts toward a sustainable, equitable, and resilient future for people and the planet by the year 2030.

Each SDG consists of specific targets and indicators, and achieving these goals requires collaboration and concerted efforts at the national and international levels. The SDGs represent a holistic and interconnected approach to addressing global challenges, emphasizing the need for social, economic, and environmental sustainability to create a better future for present and future generations. The 17 SDGs are presented in Figure 1.

Figure 1. Sustainable Development Goals [1].

4. Methodology

This paper's methodology, aiming to identify the link between the NIST 800-53r5 and the UN's SDGs through a systematic and comprehensive approach, includes the following steps.

1. *Investigation of Cybersecurity Frameworks*: In an attempt to identify the potential cybersecurity domains that may contribute to maintaining sustainable development, several Information Security Frameworks that include categories of such domains have been examined. The analysis and the choice of the NIST 800-53r5 are presented in Section II.A.
2. *Mapping of NIST 800-53r5 Controls to SDGs*: The process began by mapping the specific security controls outlined in NIST 800-53r5 to the corresponding SDGs. This involved identifying the controls that address issues directly related to poverty alleviation, hunger, health, education, gender equality, clean water, sustainable energy, economic growth, and other key SDG themes.
3. *Cross-Reference with SDG Targets and Indicators*: This step included cross-referencing the mapped NIST controls with the specific targets and indicators associated with each SDG. This step ensured a granular understanding of how cybersecurity measures contributed to achieving the measurable outcomes outlined by the SDGs targets.
4. *Case Studies*: This step includes the collection and analysis of case studies and best practices related to the implementation of NIST 800-53r5 controls in alignment with SDGs. This qualitative aspect of the methodology provides insights into the practical application of cybersecurity measures on sustainable development. The case studies presented in this paper are SDG 8 (Decent Work and Economic Growth), which has as

its mission to promote sustained, inclusive, and sustainable economic growth; full and productive employment; and decent work for all, and SDG 9 (Industry, Innovation and Infrastructure), which aims at building resilient infrastructure, promoting inclusive and sustainable industrialization, and fostering innovation. Moreover, the last step contains the evaluation of the NIST800-53r5 domains toward their implementation for the achievement of the SDGs. More specifically, the NIST800-53r5 cybersecurity domains are prioritized in terms of their contribution to the achievement of SDG 8 and SDG 9, taking into account that the objective is the fostering of sustainable economic growth as well as the resilience of IoT infrastructure. The MoSCoW method [18] is used for this analysis.

5. Cybersecurity Contribution to SDGs

To illustrate how each NIST 800-53r5 cybersecurity domain contributes to each United Nations SDG toward the resilience of IoT critical infrastructure and economic growth, an elaboration for each pairing is included. Due to the complexity and space constraints, this paper presents a simplified example, which can be extended for a more comprehensive analysis. Table 2 below also summarizes the main contributions per SDG.

Table 2 provides a starting point for understanding the potential contributions of each NIST 800-53r5 domain to specific UN SDGs, presenting sample contributions. In a more detailed analysis, one would delve into the specific controls within each domain and how they align with the targets and indicators of each SDG. It is crucial to consider the context of each organization, as the impact may vary based on industry, geographical location, and organizational structure.

Table 2. NIST 800-53r5 domains and SDGs.

NIST 800-53r5 Domain	SDGs	Contribution
Access Control	8, 9, 11, 12	AC controls protects critical infrastructure assets, ensuring authorized access to IoT devices and data. This fosters innovation, economic growth, and sustainability by preventing unauthorized access, data breaches and system/services disruptions, which can hinder economic activities and damage public trust.
Awareness and Training	8, 9, 11	AT controls raise awareness and train people on cybersecurity risks in order to be able to contribute to resilient IoT infrastructure and services by reducing human error, detecting threats early, and implementing effective measures. This fosters a secure business environment promoting economic growth.
Audit and Accountability	8, 9, 12, 16	AU controls monitor and log IoT system activities, detecting any anomalies. With robust AU controls organizations may build trust with their stakeholders contributing to a stable business environment, essential for sustainable economic growth.
Identification and Authentication	8, 9, 11	IA manages user identities, preventing unauthorized access, protecting sensitive and critical data, and enabling secure IoT operations. This builds trust of digital services, enabling investments and thus contributing to economic growth.
Contingency Planning	8, 9, 11	CP builds plans for responding to cyber incidents, minimizing disruptions, protecting critical IoT infrastructure, and ensuring business continuity. Effective CP reduces the impact of cyberattacks, protecting assets and revenues. This builds resilience and confidence in the digital economy, fostering sustainable economic growth.
Configuration Management	8, 9	CM controls in IoT devices may reduce vulnerabilities, ensuring system integrity, and optimizing system performance and hence contributing to resilient IoT infrastructure supporting cost-effective operations.
Incident Response	8, 9, 11	IR detects, analyzes, and responds to cyber incidents. An effective IR team can mitigate the impact of cyberattacks, protecting IoT critical infrastructure and ensuring business continuity. This builds trust and confidence in the IoT digital ecosystem, fostering economic growth.

Table 2. *Cont.*

NIST 800-53r5 Domain	SDGs	Contribution
Maintenance	8, 9	MA controls for IoT systems may ensure continuous operation, security, and reliability. Regular system maintenance and updates reduce vulnerabilities and system downtime, ensuring optimal performance and efficiency. This contributes to resilient IoT infrastructure and supports sustainable economic growth.
Risk Assessment	8, 9, 12	RA identifies and assesses cybersecurity risks. By understanding potential risks, threats and vulnerabilities, organizations can prioritize investments in cybersecurity measures, reducing risks and hence contributing to resilient IoT critical infrastructure and supporting sustainable economic growth.
System and Communications Protection	8, 9, 11	SC protects system and communication components, ensuring the cybersecurity triad of confidentiality, integrity, and availability of data, systems, and services. By protecting these assets, organizations may ensure business continuity, which contributes to economic growth.
System and Information Integrity	8, 9, 11, 12	SI ensures the accuracy and reliability of IoT systems and data. Ensuring data integrity is important for innovation and trust in IoT systems, contributing to sustainable economic growth.

Inspection of the results presented in Table 2 reveals that cybersecurity is a critical factor for resilient IoT infrastructure and sustainable economic growth. Safeguarding critical assets and protecting sensitive data are important to build a secure environment favorable for innovation and investment, contributing to SDG 8 (Decent Work and Economic Growth).

Cybersecurity builds resilient IoT infrastructure by preventing cyberattacks, minimizing disruptions, and protecting critical assets. For instance, robust Access Control mechanisms safeguard IoT devices from unauthorized access, preventing service outages and data breaches and hence supporting SDG 11 (Sustainable Cities and Communities). Effective Incident Response plans enable rapid recovery from security incidents, minimizing downtime and financial losses, thereby contributing to SDG 9 (Industry, Innovation, and Infrastructure). By protecting system and communication components, organizations ensure the reliable operation of IoT systems and services, supporting critical infrastructure like power grids, transportation networks, and healthcare facilities, aligning, for example, with SDG 7 (Affordable and Clean Energy).

Cybersecurity is also a crucial contributor to sustainable economic growth by fostering innovation and attracting investments. Security and privacy controls protect intellectual property and consumer data, building trust and encouraging innovation, contributing to SDG 9. Access Control and Identity and Authentication mechanisms may ensure secure online transactions, supporting e-commerce and economic growth, aligning with SDG 8. Moreover, reducing cyber risks may help organizations reduce their operational costs and allocate resources to other business activities, such as research and development, which drive innovation and competitiveness and hence support SDG 9.

The analysis of NIST 800-53r5 cybersecurity domains in relation to the SDGs underscores the critical role of cybersecurity in fostering and enhancing resilient IoT infrastructure and sustainable economic growth. By integrating cybersecurity controls, organizations can build a secure digital ecosystem that drives innovation, creates jobs, and contributes to sustainable economic stability and growth.

6. Aligning NIST 800-53r5 Domains with SDG 8 and SDG 9

This section focuses on the analytical examination of cybersecurity's contribution toward the achievement of SDG 8 and SDG 9, aiming at the enhancement of economic growth in relation to the resilience of the IoT critical infrastructure. SDG 8 and SDG 9 constitute the dimensions of economic and technological development focused on economic growth, sustainable industrialization, and innovation.

6.1. Analytical Examination of SDG 8

This section examines the critical role of cybersecurity in achieving SDG 8 (Decent Work and Economic Growth). By examining the alignment between NIST 800-53r5 cybersecurity domains and the specific targets of SDG 8, this analysis seeks to understand how cybersecurity can contribute to sustainable economic growth, promoting full and productive employment and ensuring decent work. The focus will be on identifying cybersecurity measures and controls that can contribute to attaining the SDG 8 targets toward sustainable economic growth and resilient IoT infrastructure. The subtargets of SDG 8 can be categorized as follows:

- T8.1: Sustain per capita economic growth in accordance with national circumstances, and, in particular, at least 7 percent gross domestic product (GDP) growth per annum in the least developed countries.
- T8.2: Achieve higher levels of economic productivity through diversification, technological upgrading, and innovation, including a focus on high-value-added and labor-intensive sectors.
- T8.3: Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity, and innovation and encourage the formalization and growth of micro-, small- and medium-sized enterprises, including through access to financial services.
- T8.4: Improve progressively, through 2030, global resource efficiency in consumption and production and endeavor to decouple economic growth from environmental degradation, in accordance with the 10-Year Framework of Programmes on Sustainable Consumption and Production, with developed countries taking the lead.
- T8.5: By 2030, achieve full and productive employment and decent work for all women and men, including for young people and persons with disabilities, and equal pay for work of equal value.
- T8.6: By 2020, substantially reduce the proportion of youth not in employment, education, or training.
- T8.7: Take immediate and effective measures to eradicate forced labor, end modern slavery and human trafficking, and secure the prohibition and elimination of the worst forms of child labor, including the recruitment and use of child soldiers, and by 2025 end child labor in all its forms.
- T8.8: Protect labor rights and promote safe and secure working environments for all workers, including migrant workers, particularly women migrants, and those in precarious employment.
- T8.9: By 2030, devise and implement policies to promote sustainable tourism that creates jobs and promotes local culture and products.
- T8.10: Strengthen the capacity of domestic financial institutions to encourage and expand access to banking, insurance, and financial services for all.
- T8.a: Increase Aid for Trade support for developing countries, particularly the least developed countries, including through the Enhanced Integrated Framework for Trade-Related Technical Assistance to Least Developed Countries.
- T8.b: By 2020, develop and operationalize a global strategy for youth employment and implement the Global Jobs Pact of the International Labor Organization.

The examined use case scenario is the development of a smart agriculture network. More specifically, a smart agriculture network is developed in a developing country, aiming at enhancing the productivity, efficiency, and sustainability of the agricultural sector. This network requires, among other things, the integration of IoT systems and devices, artificial intelligence mechanisms and analytics, precision agriculture technologies, cloud platforms, and monitoring and management systems for crops, livestock, resources etc. The role of cybersecurity is investigated in this scenario as a contributor toward sustainable economic growth, food security, and resilient IoT systems.

Table 3 and the related analysis of the results show and describe how the various NIST 800-53r5 domains can contribute to the achievement of SDG 8 in the context of the examined scenario, aiming at sustainable economic growth and resilient IoT infrastructure.

Table 3. Applicability of the NIST 800-53r5 domains to SDG 8 targets.

NIST 800-53r5 Domain	**8.1**	**8.2**	**8.3**	**8.4**	**8.5**	**8.6**	**8.7**	**8.8**	**8.9**	**8.10**	**8.a**	**8.b**
Access Control (AC)	x	x			x	x				x	x	
Awareness and Training (AT)		x	x	x	x	x	x	x	x	x	x	x
Audit and Accountability (AU)	x	x			x	x	x	x	x	x	x	x
Assessment, Authorization and Monitoring (CA)	x	x			x	x				x	x	
Configuration Management (CM)	x	x			x	x				x	x	
Contingency Planning (CP)	x	x			x	x				x	x	
Identification and Authentication (IA)	x	x			x	x				x	x	
Incident Response (IR)	x	x			x	x				x	x	
Maintenance (MA)	x	x			x	x				x	x	
Media Protection (MP)			x				x	x	x			
Physical and Environmental Protection (PE)						x						
Planning (PL)			x	x	x	x	x		x			x
Program Management (PM)												
Personnel Security (PS)	x	x	x	x	x	x	x	x	x	x	x	x
PII Processing and Transparency (PT)						x	x	x	x	x		x
Risk Assessment (RA)	x	x	x	x	x	x	x	x	x	x	x	x
System and Services Acquisition (SA)	x	x			x	x				x	x	
System and Communications Protection (SC)	x	x			x	x				x	x	
System & Information Integrity (SI)	x	x			x	x				x	x	
Supply Chain Risk Management (SR)	x	x			x	x				x	x	

It seems that Access Control (AC), System and Services Acquisition (SA), and Supply Chain Risk Management (SR) controls may play a crucial role in fostering economic growth in many targets, such as T8.1 and T8.2. Access Control ensures that only authorized personnel have access to critical agricultural systems and data, which is crucial for the integrity of technological innovations, thereby supporting operational efficiency and supporting economic growth. A practical example may be the implementation of fine-grained Access Controls for IoT devices in the smart agriculture network, allowing different users to have varying levels of access to different data and functions. This prevents unauthorized access to sensitive information and critical infrastructure. AC safeguards sensitive data and technological assets, preventing unauthorized access that could lead to cyberattacks, data breaches, or operational disruptions. Ensuring secure access to IoT devices, cloud platforms, and AI tools promotes innovation and operational efficiency, which drive economic productivity (T8.2) and growth (T8.1). This protection also secures the financial operations and transactions related to agriculture, aligning with SDG 8.10, which seeks to strengthen financial institutions. By securing data integrity and access, AC fosters a reliable environment for economic diversification through innovative agricultural technologies, such as AI-driven analytics, precision farming tools, and IoT sensors. These technologies improve resource management, boost crop yields, and enhance food security, which indirectly creates more

job opportunities in the agricultural sector (T8.5) and helps reduce unemployment (T8.6). Furthermore, in developing countries, AC ensures the safe integration of international aid, promoting trade and supporting economic development (T8.a).

SA helps in the strategic procurement and integration of advanced technologies. A practical example may be when procuring IoT devices and components for the smart agriculture network, to prioritize vendors with strong cybersecurity practices and a proven track record of delivering reliable and secure products. The SA domain focuses on procuring and integrating technologies and services securely and efficiently. In a smart agriculture scenario, SA ensures the adoption of advanced technologies (e.g., IoT, AI, and cloud-based analytics) that boost productivity and operational efficiency, aligning with T8.1 and T8.2 by sustaining economic growth through technological innovation. By managing the acquisition of resilient and scalable systems, SA helps ensure that the agricultural workforce has access to tools that enable productivity, directly contributing to full employment (T8.5). It also plays a role in reducing youth unemployment (T8.6) by facilitating the integration of modern technologies that create job opportunities in technology-based agriculture. For developing countries, SA strengthens financial institutions (T8.10) by ensuring secure systems are in place to manage agricultural data and transactions. It also enhances Aid for Trade (T8.a) programs by providing secure platforms to track and manage aid flows, supporting sustainable trade practices and economic growth.

Furthermore, SR manages cyber risks related to technology providers, ensuring that technologies and services remain secure and resilient. A practical example may be the implementation of a vendor risk assessment process to evaluate the security practices of suppliers who provide IoT devices and components for the smart agriculture network. SR addresses the vulnerabilities associated with the procurement and integration of third-party systems and technologies in smart agriculture. Managing risks in the supply chain ensures that agricultural enterprises can rely on secure, resilient technologies, which support continuous production and economic growth (T8.1). In addition, ensuring that the supply chain is free from compromised components enhances productivity by allowing for uninterrupted technological upgrades (T8.2). Effective SR controls also provide job security (T8.5), as disruptions to the supply chain can result in lost productivity and job losses. In a smart agriculture network, the failure of critical IoT devices or data analytics platforms due to compromised supply chain components could result in significant operational downtimes. By managing these risks, SR controls help sustain employment and reduce youth unemployment (T8.6) by ensuring the stability of agriculture-related jobs. Moreover, resilient supply chains contribute to the strength of financial institutions (T8.10), as secure supply chains reduce the risk of financial losses due to supply chain failures. This resilience is particularly important for developing countries relying on international trade support programs (T8.a), as secure supply chains ensure the integrity of imported technologies and services.

Configuration Management (CM) and Contingency Planning (CP) are also integral parts of sustainable resource management, which is in line with targets such as T8.4 in the smart agriculture network scenario. CM ensures that system configurations are managed effectively, which enhances system performance, reduces resource wastage, and thereby supports the efficient use of resources. A practical example may be the establishment of baseline configurations for all IoT devices in the smart agriculture network to ensure consistency and security. CM ensures the secure and efficient operation of systems and devices in smart agriculture networks by managing system configurations, patches, and updates. This control contributes to achieving economic growth (T8.1) by preventing disruptions and reducing downtime, thus ensuring continuous operations in agricultural production. By ensuring proper system configurations, CM improves resource efficiency (T8.4), helping to reduce waste in water usage, energy consumption, and other agricultural inputs. This is critical for sustainable practices, particularly in regions where resources are scarce. Moreover, secure and reliable configurations create a conducive environment for technological upgrading (T8.2), supporting productivity growth. CM also promotes

job creation and skill development (T8.5), as managing advanced systems requires a trained workforce. Reducing risks through effective Configuration Management indirectly contributes to reducing unemployment (T8.6), especially among younger workers who are skilled in maintaining complex technological systems. The control also ensures that financial operations within the smart agriculture network are secure, aligning with T8.10 and supporting developing economies through Aid for Trade mechanisms (T8.a).

Moreover, CP prepares the network for unexpected events by outlining strategies to ensure business continuity and effective resource management, thus promoting sustainability. A practical example may be the development of a disaster recovery plan for a smart agriculture network, including procedures for restoring operations in the event of a natural disaster or cyberattack. CP ensures that smart agriculture networks can maintain operations during unexpected disruptions, such as cyberattacks, natural disasters, or system failures. This resilience is essential for sustaining economic growth (T8.1) and supporting the continuous use of innovative technologies that drive productivity (T8.2). CP also facilitates business continuity, ensuring resource efficiency (T8.4) and minimizing wastage during crises. The ability to swiftly recover from disruptions ensures job security and helps protect employment levels (T8.5), as well as providing opportunities for the workforce to learn and engage with contingency procedures. For younger workers (T8.6), skills in business continuity and disaster recovery planning offer valuable job opportunities, especially in technologically dependent sectors like smart agriculture. CP also secures financial transactions, aligning with T8.10 and supporting the resilience of aid mechanisms (T8.a).

Furthermore, Awareness and Training (AT) and Personnel Security (PS) influence the development of job opportunities and skills in urban agriculture, which is aligned with targets such as T8.5 and T8.6 and is vital for economic growth and resilience. With AT, people build the appropriate skills, thus supporting job creation and economic growth. A practical example may be to provide cybersecurity awareness training to all employees involved in the smart agriculture network, tailored to their specific roles and responsibilities. This training should cover topics such as identifying and reporting phishing attempts, recognizing social engineering tactics, and understanding the importance of strong passwords. Awareness and Training (AT) can directly support the workforce's capacity to adapt to advanced technologies, thus promoting technological upgrading and economic productivity (T8.2). In smart agriculture, proper training on IoT systems, cybersecurity protocols, and AI-based tools enables workers to optimize operations, fostering innovation and productivity. Through training, farmers and agricultural workers can efficiently adopt resource-efficient technologies, helping to decouple economic growth from environmental degradation (T8.4). AT also contributes to achieving full and productive employment (T8.5) by equipping workers with the necessary skills to operate and maintain advanced agricultural technologies. This aligns with reducing youth unemployment (T8.6), as young workers gain expertise in emerging tech-driven industries. The focus on cybersecurity training ensures that labor rights are protected and workplaces are safe (T8.8), especially in digitalized sectors. Additionally, AT helps local agricultural businesses access international markets by ensuring compliance with global cybersecurity and financial standards, which strengthens domestic institutions (T8.10) and aids developing countries in their trade efforts (T8.a).

On the other hand, PS ensures that employees are protected and hence contributes to job stability and resilience. A practical example may be to conduct background checks on all employees who have access to IoT devices and systems in the smart agriculture network to identify potential security risks. PS focuses on ensuring that individuals granted access to smart agriculture systems are properly vetted and monitored to prevent insider threats. By ensuring the integrity and reliability of the workforce, PS contributes to sustained economic growth (T8.1) and higher productivity (T8.2) by mitigating risks posed by internal actors, which could otherwise lead to system failures or data breaches. PS also plays a key role in protecting labor rights and ensuring safe working environments (T8.8). By conducting background checks and continuous monitoring, PS helps eliminate forced

labor and trafficking (T8.7), ensuring that individuals working in the agriculture sector are employed voluntarily and under fair conditions. Additionally, PS contributes to reducing youth unemployment (T8.6) by ensuring that young workers entering the sector are appropriately trained, vetted, and supported. In developing countries, where agriculture forms a significant portion of the economy, PS controls help safeguard international trade and aid programs (T8.a) by ensuring that personnel involved in these programs adhere to ethical and legal standards. This, in turn, strengthens financial institutions (T8.10) by promoting trust in their operations.

System and Communications Protection (SC) and System and Information Integrity (SI) may enhance the resilience of the urban food supply, which is in line with targets such as SDG 8.10, 8.a. SC safeguards the confidentiality, integrity, and availability of communications and systems and financial operations conducted in urban agriculture. This protection is crucial for ensuring a resilient food supply system and financial systems that can withstand disruptions and cyber threats. A practical example may be the encryption of data transmitted between IoT devices and the cloud platform in the smart agriculture network to protect it from unauthorized access. SC is critical for ensuring the confidentiality, integrity, and availability of data transmitted across smart agriculture networks. By protecting communication channels, SC prevents cyberattacks and data breaches that could disrupt operations, safeguarding productivity (T8.1, T8.2). In a sector that relies on real-time data from IoT devices to optimize irrigation, fertilization, and harvest schedules, secure communication systems are paramount for maintaining operational efficiency and economic growth. SC also ensures that employment opportunities created by the adoption of advanced technologies are sustained (T8.5), as a secure technological environment fosters the development of new jobs in cybersecurity, data management, and system maintenance. By reducing the risk of cyber disruptions, SC contributes to job stability and encourages further technological upgrading, which in turn stimulates productivity and growth. Additionally, secure communications are crucial for financial operations in agriculture, especially in developing countries, where strong digital financial systems are necessary for international trade support (T8.a) and financial institution capacity-building (T8.10). Reliable protection ensures that agricultural enterprises can conduct secure transactions and participate in global markets, thereby promoting economic development.

SI ensures that the data used are accurate and reliable. A practical example may be the implementation of data validation checks to ensure that the data collected by IoT sensors in the smart agriculture network are accurate and reliable. This helps prevent errors in decision-making and ensures the integrity of agricultural operations. SI controls ensure that the data generated and used by smart agriculture networks are accurate, reliable, and secure. Data integrity is crucial for ensuring that decisions made in precision agriculture—such as when to irrigate, fertilize, or harvest—are based on accurate information, which enhances productivity (T8.2) and promotes sustained economic growth (T8.1). Secure and accurate data also facilitate technological upgrades by fostering trust in new systems and innovations. In the context of employment (T8.5, T8.6), SI controls create opportunities for jobs related to data security, analytics, and system monitoring. As agricultural systems increasingly rely on real-time data, ensuring that this data are not corrupted or manipulated is key to maintaining system performance and, consequently, job stability. SI controls also support financial institutions (T8.10) by ensuring that financial data and transactions remain secure, preventing fraud and enhancing the credibility of financial systems in agriculture. In developing countries, SI controls help ensure the successful implementation of trade and aid support programs (T8.a) by protecting data integrity in international transactions.

Audit and Accountability (AU) and Security Assessment and Authorization (CA) can support local economies and small enterprises in the context of the smart agriculture network. AU can provide mechanisms for tracking and data management and hence ensuring accountability, supporting the resilient operation and growth of small and medium enterprises. A practical example may be considered the regular audits of the smart agricul-

ture network's IoT infrastructure to identify vulnerabilities and ensure compliance with security standards. Another example is implementing continuous monitoring of system logs and user activity to detect suspicious behavior. With AU it is ensured that the activities performed comply with the related policies and regulations. AU controls ensure that system activities, user actions, and system changes are traceable and meet legal, regulatory, and operational requirements. This capability is essential for transparency and integrity in agricultural operations. In the context of smart agriculture, auditing processes ensure that systems are functioning correctly, data are accurate, and financial transactions are secure, which supports continuous economic growth (T8.1) and productivity (T8.2). AU also plays a vital role in protecting labor rights and promoting safe working environments (T8.8), as regular auditing can ensure that systems are in compliance with safety regulations, reducing risks to workers who interact with IoT devices and machinery. Additionally, audits provide accountability mechanisms to monitor efforts aimed at eliminating forced labor or human trafficking in supply chains (T8.7). The control family supports resilient financial institutions (T8.10) by ensuring that transactions and financial operations in agriculture are transparent and secure. Furthermore, audits help verify that international trade and aid support mechanisms (T8.a) are being used appropriately in developing countries, fostering trust and investment. By ensuring systems and transactions are secure and accountable, AU contributes to job creation (T8.5, T8.6) by promoting a secure environment where small enterprises can grow, thereby reducing unemployment. The alignment of these controls with broader global strategies for youth employment (T8.b) further supports inclusive economic growth and workforce development.

CA can evaluate and authorize new technologies, ensuring their security and effectiveness. By integrating secure technologies, local businesses are supported to securely grow and be competitive. A practical example may be the continuous monitoring tools to detect anomalies in IoT sensors used to monitor crop health, soil conditions, and weather patterns. The CA domain is essential for establishing a secure environment in which smart agriculture systems can operate. By conducting thorough assessments and ensuring that all systems and processes are authorized, CA mitigates risks associated with unauthorized access or security breaches. This contributes directly to sustained economic growth (T8.1) by maintaining the integrity of critical agricultural operations. CA supports higher levels of productivity (T8.2) through the continuous monitoring and assessment of technologies deployed in agriculture. By ensuring that systems are operating efficiently and securely, CA allows organizations to adapt and innovate, promoting technological advancements essential for agricultural productivity. In terms of employment, CA plays a vital role in ensuring that the workforce has access to secure systems that support their roles, thus contributing to full and productive employment (T8.5). It also helps reduce barriers for younger workers (T8.6) by ensuring that the systems they engage with are secure, allowing them to gain the necessary skills and experience in a safe environment. By implementing secure and reliable systems for monitoring and assessment, CA reinforces financial institutions (T8.10). It ensures that data integrity is maintained, which is critical for trust in financial transactions related to agriculture. For developing countries, CA supports Aid for Trade (T8.a) by ensuring that the technologies and systems used in trade operations are secure and compliant with relevant standards, fostering sustainable practices in agricultural trade.

6.2. Analytical Examination of SDG 9

This section examines the critical role of cybersecurity in achieving SDG 9 (Industry, Innovation, and Infrastructure). More specifically, it investigates how the NIST cybersecurity domains may contribute to the achievement of SDG 9, fostering sustainable economic growth and resilient IoT infrastructure. The focus will be on identifying cybersecurity measures that can support sustainable industrialization, promote innovation, and develop resilient critical infrastructure while enhancing economic growth. The targets of SDG 9 are presented below:

- T9.1: Develop quality, reliable, sustainable, and resilient infrastructure, including regional and trans-border infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all.
- T9.2: Promote inclusive and sustainable industrialization and, by 2030, significantly raise industry's share of employment and gross domestic product, in line with national circumstances, and double its share in the least developed countries.
- T9.3: Increase the access of small-scale industrial and other enterprises, in particular in developing countries, to financial services, including affordable credit, and their integration into value chains and markets.
- T9.4: By 2030, upgrade infrastructure and retrofit industries to make them sustainable, with increased resource-use efficiency and greater adoption of clean and environmentally sound technologies and industrial processes, with all countries taking action in accordance with their respective capabilities.
- T9.5: Enhance scientific research, upgrade the technological capabilities of industrial sectors in all countries, in particular developing countries, including, by 2030, encouraging innovation and substantially increasing the number of research and development workers per 1 million people and public and private research and development spending.
- T9.a: Facilitate sustainable and resilient infrastructure development in developing countries through enhanced financial, technological and technical support to African countries, least developed countries, landlocked developing countries, and small island developing states.
- T9.b: Support domestic technology development, research, and innovation in developing countries, including by ensuring a conducive policy environment for, inter alia, industrial diversification and value addition to commodities.
- T9.c: Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in the least developed countries by 2020.

The principal use case scenario for this examination is the following: A company decides to establish a new smart factory dedicated to processing raw materials used in construction, such as aggregates, cement, and other building materials. This factory is strategically located in a local area experiencing significant demand for construction materials due to ongoing infrastructure development projects, such as roads, bridges, residential complexes, and commercial buildings. To enhance operational efficiency, the factory integrates IoT technologies, including smart sensors and automated systems, to monitor equipment performance, track inventory in real time, and optimize the supply chain.

As shown in Table 4, Access Control has a significant role in the SDG 9 targets by safeguarding critical infrastructure and ensuring that only authorized personnel have access to critical systems and data. A practical example of AC may be that a smart factory implements Role-Based Access Control (RBAC) to restrict access to IoT devices based on employee roles. This prevents unauthorized access to sensitive data and production controls. AC contributes to the development and maintenance of resilient infrastructures. For instance, it enhances T9.1 (Resilient Infrastructure) by protecting critical infrastructure from unauthorized access and breaches, which can cause costly disruptions and economic losses. By protecting assets, AC enhances investor confidence, fostering sustainable economic growth. In the context of T9.2 (Sustainable Industrialization), secure access management supports the integrity and reliability of industrial processes. This not only promotes operational efficiency but also supports economic sustainability by reducing waste and inefficiencies. AC also encourages innovation by creating a secure environment for new technologies (T9.3-Fostering Innovation) by ensuring that innovative systems and technologies are used in a secure manner only by authorized individuals. This can lead to economic diversification and increased employment opportunities. Regarding T9.4 (Upgrade Infrastructure), AC mechanisms manage upgrades and changes in a secure way, thereby enhancing IoT systems and critical infrastructure resilience, preventing costly

downtime, and hence contributing to the maintenance of economic stability. For T9.5 (Research and Technological Development), AC may protect sensitive research data and technological solutions in order not to be compromised. Protecting sensitive research data encourages innovation, which is critical for economic growth. Concerning T9.a, T9.b, and T9.c (Supporting Small and Medium Enterprises, Innovation, and Technology), AC may contribute to a secure environment that fosters technological advancement and investments, especially for small enterprises.

Table 4. Applicability of NIST 800-53r5 domains to SDG 9 targets.

NIST 800-53r5 Domain	9.1	9.2	9.3	9.4	9.5	9.a	9.b	9.c
Access Control (AC)	x	x	x	x	x	x	x	x
Awareness and Training (AT)	x	x	x	x	x	x	x	x
Audit and Accountability (AU)	x	x	x	x	x	x	x	x
Assessment, Authorization, and Monitoring (CA)				x	x	x		x
Configuration Management (CM)	x	x	x	x	x	x	x	x
Contingency Planning (CP)	x	x	x	x	x	x	x	x
Identification and Authentication (IA)	x	x	x	x	x	x	x	x
Incident Response (IR)	x	x	x	x	x	x	x	x
Maintenance (MA)	x	x	x	x	x	x	x	x
Media Protection (MP)								
Physical and Environmental Protection (PE)	x	x	x	x	x	x	x	x
Planning (PL)								
Program Management (PM)								
Personnel Security (PS)	x	x	x	x	x	x	x	x
Personally Identifiable Information Processing and Transparency (PT)								
Risk Assessment (RA)	x	x	x	x	x	x	x	x
System and Services Acquisition (SA)	x	x	x	x	x	x	x	x
System and Communications Protection (SC)	x	x	x	x	x	x	x	x
System and Information Integrity (SI)	x	x	x	x	x	x	x	x
Supply Chain Risk Management (SR)	x	x	x	x	x	x	x	x

Awareness and Training are essential in order for personnel to be aware of security practices and operations. promoting industrialisation and impacting several SDG 9 targets. A practical example may be the case that cybersecurity awareness training is provided to all the smart factory employees who have access to IoT devices, including information on how to identify and report phishing attempts. Security awareness training provides training modules on identifying and responding to security risks for personnel at all levels, including operators of critical IoT devices in the smart factory. In developing countries where cybersecurity skills might be limited, using Role-Based Security Training may help tailor training specifically for roles with access to sensitive areas. For T9.1, AT improves the ability of personnel to manage and maintain the systems and data securely. Empowering

employees to identify and mitigate risks may help thus reducing potential economic losses from security incidents. In relation to T9.2, training in sustainable industrial practices fosters a culture of efficiency, promoting economic growth through resource conservation and waste reduction. In T9.3, AT encourages innovation and adaptability, which are crucial for small businesses seeking to remain competitive in a dynamic market. Regarding T9.4, AT ensures that infrastructure upgrades are handled correctly, reducing errors and enhancing system resilience, minimizing operational disruptions that could impact economic stability. For T9.5, well-trained personnel are essential for effective research and development, leading to technological advancements that drive economic growth.

Audit and Accountability are crucial for tracking and reviewing system activities to ensure compliance with security policies and hence secure industrial operations. Regular audits may significantly contribute to SDG 9 targets. A potential practical example may be to conduct regular audits of the factory's IoT infrastructure to identify vulnerabilities and ensure compliance with security standards. Moreover, implementing Audit Events enables the logging of all access and modification events within the smart factory, creating a comprehensive record of actions that can be audited for compliance. In addition, Audit Generation establishes protocols for recording and analyzing audit data, which is significant in identifying patterns that may indicate potential security risks. In developing countries, these measures provide transparency and build trust among stakeholders, attracting investment and supporting small enterprises since they ensure consistent security across operations. In the context of T9.1, audits help identify vulnerabilities and address potential security issues before they impact the IoT critical infrastructure. This may also help prevent incidents that can lead to significant economic losses. For T9.2, AU ensures that industrial operations adhere to sustainability standards and practices, which can enhance brand reputation and customer loyalty, ultimately contributing to economic growth. AU also supports T9.3 by providing transparency and accountability in innovation processes, which foster trust and investment, essential for economic development, particularly in small enterprises. T9.4 may be positively impacted by audits through the proper management of infrastructure upgrades and changes to enhance resilience and protect against costly failures. Regarding T9.5, regular accountability checks may contribute to securing research and technological development processes and activities ensuring the integrity of innovations that drive economic growth. Furthermore, AU also aligns with T9.a, T9.b, and T9.c by ensuring the technology ecosystem remains transparent and accountable, fostering an environment favorable for innovation and enterprise growth, which is crucial for sustainable economic development.

Assessment, Authorization, and Monitoring are also important for several SDG 9 targets. As a practical example, we may consider using continuous monitoring tools to detect anomalies in IoT sensors used to monitor equipment performance and inventory levels in the smart factory. Controls such as continuous monitoring are important since they apply automated tools to monitor IoT systems in real time, detecting anomalies that might signal equipment malfunction or cyber threats. Moreover, Control Assessment ensures regular reviews of controls applied to smart factory infrastructure, verifying that all mechanisms are up to date and effective in preventing unauthorized access. In terms of T9.4, CA manages infrastructure upgrades and changes, thereby supporting resilience. CA ensures that all upgrades are properly evaluated, minimizing the risk of disruptions that can have economic repercussions. CA provides insights into the system's performance and also areas for improvement, which fosters innovation. For T9.5, regular assessments ensure that research and development activities meet security and performance standards, fostering an environment fertile for innovation. This is vital for driving economic growth through new technologies. CA also contributes to Target 9.a by ensuring that infrastructure improvements are sustainable and compliant with regulations, which is crucial for attracting investments. Additionally, supporting Target 9.c, CA helps maintain compliance across technological processes, which is essential for sustaining economic development and encouraging enterprise growth.

Configuration Management ensures that systems are set up and maintained according to predefined standards and hence may standardize industrialization. A practical example is the establishment of baseline configurations for all IoT devices in the factory to ensure consistency and security. Baseline Configuration ensures that the IoT devices of the smart factory adhere to an approved configuration baseline and hence reduce potential vulnerabilities. Configuration Settings can further enforce secure settings on IoT devices, making it harder for unauthorized changes to be made. CM supports several SDG 9 targets by ensuring system resilience and operational consistency. For T9.1, CM enhances infrastructure resilience by maintaining system stability and preventing failures. A stable environment reduces the likelihood of failures that can lead to economic losses. It contributes to T9.2 by ensuring that industrial systems operate efficiently and consistently over time, which directly translates to cost savings and sustainability, promoting economic growth. The domain supports T9.3 by providing a stable foundation for innovation and technological development, allowing businesses to adapt and grow economically. Effective configuration management also aids in T9.4 by managing infrastructure upgrades systematically, thus improving resilience. For T9.5, maintaining consistent configurations ensures a stable environment for research and development, driving technological advancements that bolster economic growth. Additionally, T9.a, T9.b, and T9.c benefit from standardized configurations that support technological development and the growth of small and medium enterprises enhancing their economic impact.

Contingency Planning seems to be essential for several SDG 9 targets by enhancing infrastructure resilience and business continuity. In practice, an example may be the development of a disaster recovery plan for the smart factory's IoT infrastructure, including procedures for restoring operations in the event of a natural disaster or cyberattack. Contingency Planning outlines clear procedures for responding to various incidents, ensuring that a smart factory's operations may resume quickly after a failure. System Recovery and Reconstitution provide specific protocols for restoring IoT system functionality and hence allowing faster recovery times. In developing countries, where resources are limited, these plans are important for minimizing economic losses and promoting uninterrupted industrial growth by ensuring that systems can quickly return to full operational capacity after an incident. For T9.1, effective CP ensures that infrastructure can recover quickly from disruptions, thus enhancing resilience, minimizing economic losses, and maintaining investor confidence. CP also facilitates T9.2, T9.3 by ensuring that innovation can continue despite disruptions, ensuring that disruptions do not stifle small-scale industries. In relation to T9.4, robust planning helps manage infrastructure upgrades and changes effectively, minimizing downtime that could impact economic stability. For T9.5, CP protects research and development activities by ensuring that they can recover from disruptions. In addition, T9.a, T9.b, and T9.c are supported by effective CP, which ensures that systems and services remain operational during unexpected events, thus supporting small and medium enterprises' growth and their contributions to the economy.

Identification and Authentication involve verifying the identity of users and systems and can support the resilience of the industrial environment. A practical example is the implementation of multi-factor authentication for access to IoT-enabled systems in the factory, requiring users to provide a password, a security token, and biometric verification. In developing countries where cyberthreats are increasingly prevalent, such multi-layered authentication processes can prevent unauthorized access, safeguarding industrial assets and reducing potential disruptions. IA mechanisms are essential for preventing unauthorized access, directly impacting T9.1 by safeguarding against potential breaches that could lead to significant economic disruptions and also fostering the resilience of the infrastructure. Regarding T9.2, IA supports secure industrial processes by ensuring that only authorized users can access critical systems, promoting operational reliability and reducing costs associated with breaches. Concerning T9.3, strong IA fosters an innovative environment where small-scale industries can confidently develop new technologies, contributing to economic growth. For T9.4, identification and authentication manage access during infrastructure

upgrades and changes, enhancing resilience. In relation to T9.5, IA protects research and development processes by ensuring that only authorized individuals can access sensitive information. Additional benefits also stand for T9.a, T9.b, and T9.c.

Incident Response involves managing and addressing security incidents and can deal with disruptive events during operations, which is vital for several SDG 9 targets, as it ensures quick recovery from disruptions. In practice, we may consider indicatively the case to establish an Incident Response team that is trained to handle cyberattacks on the smart factory's IoT infrastructure. Moreover, the implementation of Incident Handling is important to define protocols for addressing security incidents in the smart factory, particularly around critical IoT systems. Additionally, Incident Reporting sets a standard for promptly reporting security incidents, ensuring immediate attention and reducing the impact on smart factory operations. In developing countries where security resources may be limited, such predefined response protocols enhance organizational capacity to handle and recover from incidents, supporting continued growth and stability against cyberthreats. For T9.1, an IR plan enhances IoT critical infrastructure resilience by addressing breaches promptly. In T9.2, effective IR may significantly reduce the impact of disruptions. In the same way, the other SDG 9 targets also benefit from effective IR, which ensures that organizations and enterprises can handle and recover from security incidents that may affect the IoT critical infrastructure.

Maintenance maintains IoT systems and critical infrastructure in order for them to operate properly and reliably. A practical example is the scheduling of regular maintenance on the smart factory's IoT sensors and equipment to ensure their proper functioning and prevent failures. Indicatively, the control of Non-local Maintenance mandates secures the maintenance of devices even when remote support is needed, which is particularly beneficial in rural or resource-limited areas. By ensuring the ongoing functionality of IoT devices, particularly in high-demand sectors like construction, this control enhances system reliability and prevents costly failures, supporting economic sustainability. This domain is important for the applied SDG 9 targets since regular maintenance prevents failures and addresses issues before they become significant, thereby enhancing IoT critical infrastructure resilience.

Overall, the NIST 800-53r5 domains contribute to achieving SDG 9 targets by enhancing the resilience of infrastructure, supporting sustainable industrialization, fostering innovation, and protecting technological development. Each domain plays a critical role in supporting, which is important sustainable economic growth and technological advancement.

6.3. Evaluation of NIST Cybersecurity Domains' Contributions to SDGs

This section describes and evaluates the positive impacts of cybersecurity on SDG 8 and SDG 9. In order to further analyze and evaluate the impacts, a set of impact criteria is defined, and the MoSCow method is followed to prioritize the most immediate criteria per SDG.

6.3.1. Prioritization Approach

The MoSCoW method is a type of numerical assignment technique. In this context, four priority groups are defined, more specifically, "Must Have", "Should Have", "Could Have" and "Won't Have". To prioritize the NIST cybersecurity domains, experts were asked to classify each domain into one of the aforementioned categories based on their importance to the achievement of the overall goal.

- "Must Have" is related to cybersecurity domains that seem to be mandatory. NIST cybersecurity domains are essential for ensuring the resilience of IoT systems and infrastructure and immediate economic impacts.
- "Should Have" includes important initiatives that are not vital but add significant value. Cybersecurity control refers to families that play an important role but have a slightly less urgent or direct impact on economic growth and IoT infrastructure resilience.

- "Could Have" concerns nice-to-have initiatives that will have a small impact if left out. These domains are beneficial in the long term but not immediately critical.
- "Won't Have" means domains with a lower priority in comparison with the previous groups. Domains with little or no immediate impact on economic growth or IoT resilience in the short term.

In this context, twelve experts with expertise in cybersecurity and IoT technoeconomics were gathered to provide their feedback and categorize the NIST 800-53r5 domains as per the contribution to the achievement of SDG 8 and SDG 9. The main objective was sustainable economic growth and the resilience of IoT infrastructure. The experts evaluated each cybersecurity domain based on impact criterion C_k, where k is an integer in the interval [1 N] with N as the total number of criteria. The criteria are the criticality to IoT infrastructure resilience (C_1) and the relevance to economic productivity (C_2), which are further explained in Sections 6.3.2 and 6.3.3.

Each NIST control family i was evaluated by each expert m $(1 \leq m \leq M)$ for each criterion with a value $v_{ik}^{(m)}$ from 1 to 5, and then the average value was estimated by all the experts as v_{ik}. Then, the average score of the NIST control family i for both criteria was evaluated as v_i. The control families within the interval [4 5] are categorized in the Must Have category. If $3 \leq v_i < 4$, then it is categorized in the Should Have category. A v_i that falls into the interval [2 3) belongs to the Could Have, whereas the rest values classify the control family in the Won't Have category for the short term.

6.3.2. Evaluation of Cybersecurity Contribution to SDG 8

The MoSCoW method is used to prioritize cybersecurity domains based on their relevance and impact on the smart agriculture network use case scenario in the context of achieving SDG 8 targets. The experts evaluated each cybersecurity domain based on the following impact criteria:

- Criticality to IoT infrastructure resilience (C_1): Ensuring the stability, continuity, and security of IoT systems and infrastructure in the smart agriculture network.
- Relevance to economic productivity (C_2): Reducing risks to agricultural operations and ensuring continuous improvement in productivity and efficiency.

The results of the MoSCow prioritization for SDG 8 are presented in Figure 2. This prioritization may constitute a helpful guide for the implementation of the cybersecurity domains and controls toward the achievement of the SDG 8 targets and indicators, aiming at sustainable economic growth.

In the "Must Have" category, we find the cybersecurity domain of Risk Assessment. RA is essential for identifying potential threats and vulnerabilities in IoT systems and networks. In the context of the smart agricultural network, suitable controls may be implemented to mitigate these issues, preventing disruptions of services that could lead to financial losses and reduced productivity. The Access Control domain is also important to prevent unauthorized access to sensitive data and critical systems and infrastructure, which could lead to data breaches and/or operational disruptions. System and Communications Protection is also a Must Have domain since data from IoT devices and cloud platforms are constantly exchanged, and ensuring secure communication channels seems to be crucial to enable accurate and timely decision-making enhancing productivity. Incident Response is another crucial domain, since quick and effective response to incidents may reduce downtime and ensure that, e.g., agricultural operations continue without significant disruption. This is vital for maintaining economic stability and resilience. Awareness and Training is also a crucial horizontal measure to be applied.

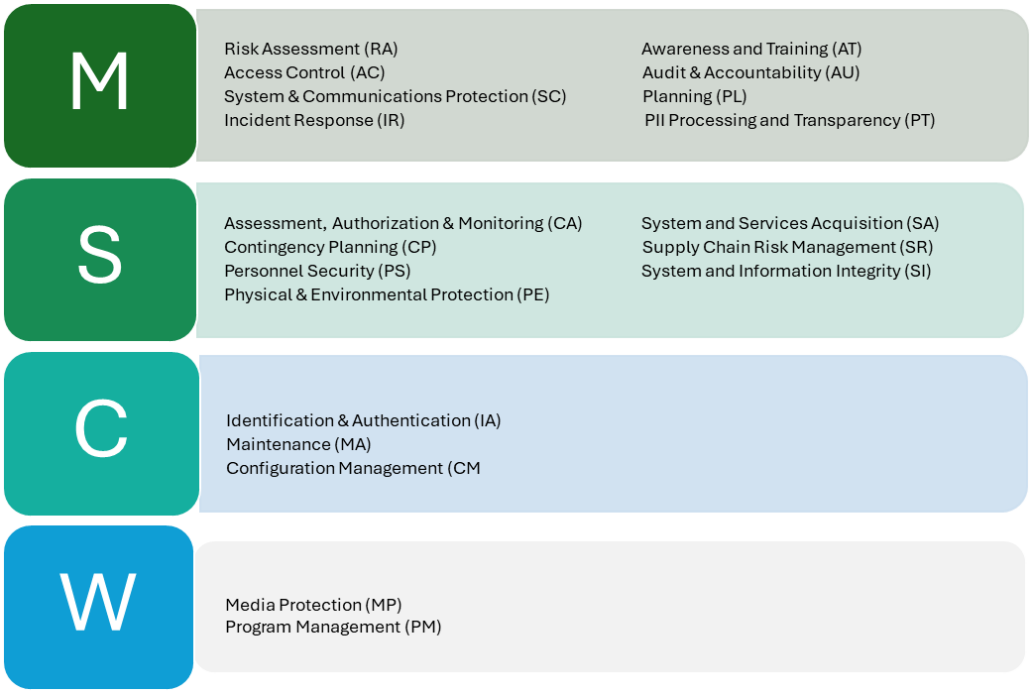

Figure 2. NIST domains prioritization for SDG 8.

In the "Should Have" category, there are the important cybersecurity domains of System and Information Integrity, Security Assessment and Authorization, Supply Chain Risk Management, and Contingency Planning. SI ensures the accuracy of data, which is critical for decision-making in crop management, livestock monitoring, and resource allocation, e.g., for an agriculture network. In the context of CA, security assessments and systems' authorization may ensure that the network's security controls remain effective over time. Moreover, SR controls ensure that all components are secure and reliable, which seems to be crucial, as compromised supply chains can introduce vulnerabilities. CP is also significant since it ensures that the systems and network continue operating during and/or after disruptions, such as natural disasters or cyberattacks. For example, for a smart agriculture network, this is useful for food production maintenance and supply chain continuity, which are essential for economic stability and growth.

Regarding the "Could Have" category, there are domains such that, even if they enhance cybersecurity and resilience, they are not directly related to sustainable economic growth. Identification and Authentication, Maintenance, and Configuration Management may not be immediately critical, but they indirectly contribute to long-term trust and reliability, which are important for sustaining economic productivity.

In the last category of "Won't Have", Media Protection and Program Management are domains that may not directly impact economic growth in the short term but could be considered in later stages.

Overall, maintaining robust security controls enhances the support of continuous operations and hence protects the potential investments contributing to sustainable economic growth.

6.3.3. Evaluation of Cybersecurity's Contribution to SDG 9

The prioritization of cybersecurity domains concerns the use case scenario examined above for SDG 9 and more specifically supports the goal of smart factories to contribute to resilient infrastructure, sustainable economic growth, and IoT system stability. The classification of the NIST domains into the four MoSCoW categories was performed based on the feedback of the experts taking into account the following impact criteria:

- Criticality to infrastructure resilience (C_1): Importance of each domain in ensuring the integrity and continuity of IoT systems in the smart factory.
- Relevance to economic growth (C_2): The degree to which the domain impacts the factory's ability to meet market demands and support local economic development.

The outcomes of the MoSCow prioritization for SDG 9 are presented in Figure 3. This prioritization may serve as a helpful guideline for the implementation of the cybersecurity controls toward the achievement of the SDG 9 targets and indicators, aiming at resilient IoT infrastructure and sustainable economic growth.

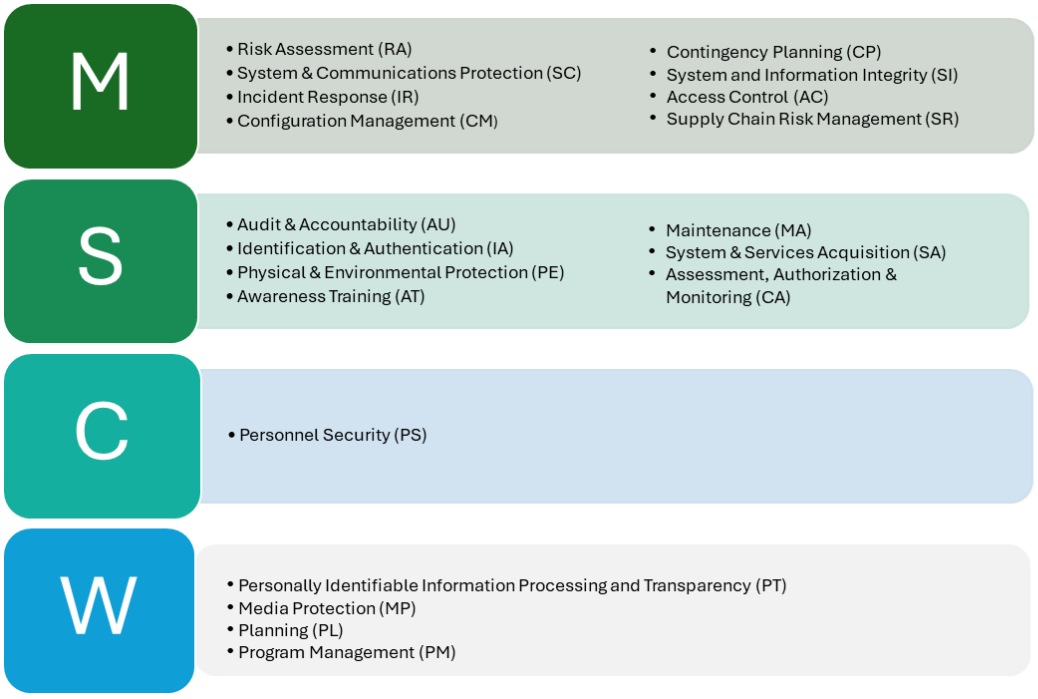

Figure 3. NIST domain prioritization for SDG 9.

In the context of the "Must Have" category, the Risk Assessment seems to be fundamental to identifying potential threats to the IoT infrastructure. This can be critical for both the economic stability and resilience of infrastructures since the associated risks may undermine operations, leading to economic losses and disruptions of services. System and Communications Protection is also important for achieving SDG 9 since it helps protect the communication channels and systems within the IoT infrastructure. A potential breach may compromise entire networks, disrupt services, and hence impact economic growth. Regarding Incident Response, the ability to respond quickly and effectively to cybersecurity incidents is crucial for maintaining operational continuity in the context of IoT infrastructure and services. An effective Incident Response may prevent an issue of low importance from escalating into a major disruption, hence safeguarding both economic stability and IoT infrastructure resilience. Moreover, Proper Configuration Management ensures that systems are set up securely and consistently, which is essential for both maintaining resilient IoT infrastructures and ensuring that associated economic activities and services are not disrupted. Contingency Planning is also crucial, since a robust contingency plan is vital for ensuring that IoT infrastructure can recover quickly, hence preventing economic issues and losses that may occur by minimizing downtime. System and Information Integrity is also important since it contributes to the protection of the integrity of information within IoT systems. Access Control ensures that only authorized users can access critical IoT systems, which is fundamental to prevent unauthorized activities that may compromise the IoT infrastructure and affect economic stability. Supply Chain Risk Management can address risks in the supply chain for IoT components and systems, ensuring their availabil-

ity and security, which is crucial for maintaining resilient infrastructure and supporting economic growth.

Regarding the "Should Have" category, the cybersecurity domain of Audit and Accountability ensures that all actions within IoT systems are monitored and are accountable, which seems to be of secondary priority for implementation toward achieving SDG 9. Identification and Authentication controls, Physical and Environmental Protection, Awareness and Training, Maintenance of IoT systems, Systems and Services acquisition, Assessment, Authorization, and Monitoring seem to be important for maintaining resilient operations but less directly related to economic growth in the context of SDG 9 compared to the "Must Have" category.

Personnel Security is categorized in the "Could Have" group, since it is beneficial but not essential, with a less significant impact on infrastructure resilience and economic growth.

In the last category of "Won't Have," the controls related to PII Processing and Transparency, Media Protection, and Planning and Project Management are included. These seem to have less direct impact on economic growth and infrastructure resilience.

The outcomes of the above subsections for SDG 8 and SDG 9 may serve as an important guide for implementing the cybersecurity domains toward the achievement of SDG 8 and SDG 9, keeping in mind the fostering of economic growth and ensuring resilient IoT infrastructure and services. The prioritization seems to be crucial in order for all the involved parts, from the designers to the implementers, to be aware of the hierarchy of implementation toward the achievement of the SDG targets and indicators. Since the budget and the available resources are crucial criteria for the implementation of a series of beneficial cybersecurity controls, it is of paramount importance to follow a useful and effective guide of prioritization.

6.4. Relevant Cybersecurity Threats and Incidents

It seems that there are many cybersecurity threats [19] that have a distinct set of challenges for both SDG 8 and SDG 9, and the proposed cybersecurity controls analyzed in the previous subsections aim to deal with these threats and minimize the possibility of potential cybersecurity incidents. An analysis of relevant threats is presented in this section. For smart agriculture in SDG 8, threats like malware, data breaches, and DoS attacks could reduce productivity, harm economic stability, and undermine food security. In the context of SDG 9, focused on industrial resilience, such threats can impede infrastructure projects, increase costs, and disrupt supply chains, slowing economic growth and development.

Malware attacks is a threat for both SDGs. Malware can corrupt data from IoT sensors monitoring crops and livestock, disrupt precision agriculture systems, and compromise the AI-driven analytics used for resource management. This may lead to downtime in agricultural operations, reduced crop yields, and financial losses, directly affecting economic productivity and food security. The efficiency and sustainability goals of the smart agriculture system would be undermined, slowing economic growth in a developing region. On the other hand, for SDG 9, in smart factory processing construction materials, malware could target IoT systems that monitor equipment performance, manage inventory or optimize supply chains. This could cause downtime, leading to delayed projects, increased costs, and loss of productivity in infrastructure development. It could also impact the availability of construction materials in a high-demand region, compromising economic growth and infrastructure resilience.

Data breaches could also impact SDG 8 and SDG 9. A data breach could expose sensitive farm operation data, such as proprietary crop management techniques, soil data, and livestock information. This could lead to competitive disadvantages for local farmers and economic entities, potentially slowing the modernization of agriculture and negatively impacting sustainable economic growth. Additionally, if data about resource management are altered, it could cause inefficient use of resources, undermining agricultural productivity. Regarding SDG 9, in a smart factory, a data breach could expose confidential

supply chain information or critical design plans, leading to competitive disadvantages or even corporate espionage. The leak of sensitive information might result in supply chain disruptions or material shortages, impeding infrastructure projects and negatively impacting local economic development. Moreover, a breach in IoT systems that controls equipment performance could lead to inefficient operations, increasing maintenance costs and reducing operational efficiency.

Denial of Service (DoS) attacks are also crucial for both SDGs. A DoS attack could render IoT sensors and monitoring systems inaccessible, halting the flow of real-time data on crop conditions, weather, or livestock health. This would severely impair precision agriculture and the ability to make timely decisions, leading to reduced crop yields, wasted resources, and economic losses. The agricultural network's goal of increasing productivity through IoT-based efficiency would be jeopardized, slowing economic growth in developing countries. As per SDG 9, in a smart factory, a DoS attack could interrupt critical real-time systems monitoring equipment performance, halting production and preventing inventory tracking. This could delay infrastructure projects due to material shortages, increasing costs and negatively impacting regional economic growth. Such attacks could also erode trust in the factory's operational resilience, reducing investor confidence and slowing industrial development in the area.

Phishing and social engineering could also affect SDGs 8 and 9. A successful phishing attack could allow malicious actors to gain control over critical farming operations, including access to systems controlling irrigation, fertilization, or livestock feeding. The misuse of these systems could lead to resource mismanagement, reduced productivity, and ultimately financial losses for local farmers, reducing sustainable economic growth in the agricultural sector. As far as SDG 9 is concerned, phishing attacks targeting factory employees could result in unauthorized access to systems managing production lines or inventory systems. This could lead to operational disruptions or manipulation of the supply chain, causing delays in construction projects, increasing costs, and slowing infrastructure development. Moreover, unauthorized access to industrial control systems could compromise factory safety, affecting both infrastructure resilience and economic stability.

Supply chain attacks are another threat that impacts both SDGs. For SDG 8, a supply chain attack on the IoT components used in a smart agriculture network could introduce vulnerabilities, leading to malfunctioning devices or sensors. Compromised IoT devices might provide incorrect data about crops, leading to poor resource management decisions. Such attacks could disrupt precision farming operations, hinder crop yields, and affect overall economic growth in the agricultural sector. In the context of SDG 9 in a smart factory, a supply chain attack could target third-party IoT components or software used to monitor and manage production processes. This could compromise the reliability and safety of the factory's equipment, leading to production delays, increased costs, and a higher likelihood of system failures. Disruptions in the supply chain could reduce the availability of construction materials, negatively impacting infrastructure projects and hindering sustainable economic growth.

Unauthorized access and insider threats are other threats to be considered. For SDG 8, insider threats or unauthorized access to IoT systems managing agricultural operations could result in the manipulation or sabotage of critical systems, such as irrigation, crop monitoring, or livestock tracking. This could lead to resource misallocation, damaging crop yields or livestock health, ultimately slowing economic productivity and food security in the region. For SDG 9, unauthorized access could allow individuals to manipulate industrial systems, shut down production lines, or tamper with inventory management systems, leading to delays and inefficiencies in construction material supply. Such attacks would compromise infrastructure development and impact regional economic growth, undermining both the factory's and the local construction industry's resilience.

There are also additional threats that may affect the achievement of SDG 8 and SDG 9. For example, in the context of SDG 8, additional threats such as ransomware, advanced persistent threats, zero-day exploits, and data tampering could undermine the ability of

smart agricultural networks to maintain productivity, resource efficiency, and sustainable economic growth. Similarly, in terms of SDG 9, threats like man-in-the-middle attacks, botnet-driven DDoS attacks, and insider threats could compromise production efficiency, supply chains, and the resilience of IoT infrastructure.

Since there is a large number of potential cybersecurity threats that may threaten the achievement of SDG 8 and SDG 9, an analysis of indicative related cybersecurity incidents has been performed and is presented below. The Ukraine Power Grid Cyberattack was conducted in December 2023 [20]. Cyberattacks targeted Ukraine's power grid during a critical winter period, aiming to disrupt energy supplies amid ongoing geopolitical tensions. This attack highlighted the vulnerabilities of smart grid technologies, which rely on IoT systems for monitoring and managing power distribution. Moreover, the Colonial Pipeline Ransomware Attack occurred in May 2021 [21]. A ransomware attack by the DarkSide group targeted Colonial Pipeline, a major U.S. fuel pipeline operator. The attack caused significant disruptions in fuel supplies across the East Coast. Furthermore, in March 2021, hackers breached Verkada [22], a company providing IoT-based security cameras for industrial facilities, healthcare, and public spaces. The hackers accessed over 150,000 cameras in hospitals, factories, prisons, and schools by using a publicly exposed admin login found online. The breach allowed unauthorized viewing of sensitive areas, including factories, which impacted industries directly. In April 2022, the Costa Rica government suffered a major ransomware attack attributed to the Conti ransomware gang [23]. The attack targeted the country's Ministry of Finance and later spread to other government agencies, including customs services and social security systems. This led to significant disruption in the country's economy and public services, including delays in imports and exports due to customs system failures. Moreover, the world's largest meat processing company, JBS Foods [24], was hit by a ransomware attack in 2021 that disrupted its operations in the U.S., Australia, and Canada. The attack impacted the global meat supply chain, raising food prices and disrupting markets, which affected economic stability, especially for developing countries reliant on agricultural exports.

Based on the analysis presented in this section it seems that it is of paramount importance to implement cybersecurity controls in order to minimize the likelihood that a cybersecurity incident occurs and significantly affects the operations and the infrastructure in the context of the SDGs achievement. As global reliance on interconnected devices and systems grows, so does the potential for cybersecurity threats, such as data breaches, system disruptions, and cyberattacks targeting critical infrastructure. These threats can significantly undermine economic stability, disrupt supply chains, and jeopardize essential services, thereby threatening food security and industrial productivity. By implementing robust cybersecurity measures, organizations can mitigate these risks, ensuring the continuous operation of IoT systems that enhance productivity and efficiency in sectors like agriculture and manufacturing that are examined in the use case scenarios of this paper. The intersection of cybersecurity and sustainable economic growth becomes increasingly evident, as the protection of digital assets and infrastructure not only supports existing operations but also contributes to a more resilient and sustainable future.

7. Future Considerations

The work presented in this paper is the first attempt to address the contribution of cybersecurity domains into the achievement of the SDGs. SDG 8 and SDG 9 have been chosen to be examined as two indicative case studies for economic growth and IoT infrastructure resilience. For sure, there are also other SDGs of great interest and relevance to be analyzed and investigated such as SDG 11 (Sustainable Cities and Communities). Performing a preliminary analysis of SDG 11 shows that many NIST family controls may contribute to the achievement of SDG 11's targets respecting the sustainable economic growth and the resilience of IoT infrastructure. For example, strong Access Controls for smart transportation systems can prevent unauthorized access and disruptions, ensuring the efficient movement of people and goods, which is essential for sustainable economic

growth. By preventing unauthorized access, AC helps maintain the integrity and reliability of IoT infrastructure, enhancing its resilience to cyberattacks and other threats. Moreover, regular audits of smart grid infrastructure can identify potential security risks and ensure the reliable delivery of electricity, supporting sustainable economic growth. Proactive monitoring and auditing help identify and address security risks before they lead to significant disruptions, ensuring the reliability and availability of IoT infrastructure. Furthermore, well-configured IoT systems are more resistant to attacks and less likely to experience unexpected failures, ensuring the reliability and availability of critical infrastructure. This supports sustainable economic growth by enabling efficient and uninterrupted operations. Additional SDGs could be analyzed as an extension of this work in future research.

8. Discussion and Conclusions

In conclusion, cybersecurity plays a crucial role in achieving the United Nations' SDGs for a sustainable future. Our study focused on the contribution of cybersecurity to SDGs, based on the NIST 800-53r5 framework, leading to key findings that underscore the role of cybersecurity in advancing global sustainability in line with sustainable economic growth and resilient IoT critical infrastructure. In this paper, two use case scenarios were also examined and analyzed, focused on SDG 8 (decent work and economic growth) and SDG 9 (industry, innovations, and infrastructure). An analysis of the prioritization of the several cybersecurity domains following the MoSCoW method was also presented.

The analytical examination of NIST 800-53r5 cybersecurity domains reveals their significant contribution toward achieving SDG 8 and SDG 9. The alignment between these cybersecurity controls and the specific targets of SDG 8 and SDG 9 underscores the critical role that robust cybersecurity measures play in fostering sustainable economic growth, promoting innovation, and ensuring resilient critical infrastructure, particularly within IoT environments.

In the context of SDG 8, there are important cybersecurity measures like Access Control, System and Services Acquisition, and Supply Chain Risk Management that contribute to economic productivity, job creation, and resilient IoT systems in sectors like smart agriculture. These controls support targets such as improving resource efficiency, securing employment, and fostering innovation. Similarly, for SDG 9, cybersecurity domains enhance infrastructure resilience, support sustainable industrialization, and foster innovation. Controls such as Access Control, Configuration Management, and Contingency Planning are vital in securing critical infrastructure, managing technological upgrades, and ensuring business continuity. These measures contribute directly to the development of resilient industrial systems, the protection of research and innovation, and the integration of small and medium-sized enterprises into the global economy.

Overall, the comprehensive analysis highlights that the integration of NIST 800-53r5 cybersecurity controls not only enhances the security and resilience of IoT systems but also directly supports the broader objectives of sustainable development as outlined in SDG 8 and SDG 9. By effectively implementing these controls, organizations can contribute to a secure and sustainable economic future, driving innovation, protecting critical infrastructure, and ensuring inclusive and sustainable growth. While the direct impact of NIST control families on specific SDGs may vary, correlations between cybersecurity practices and sustainable development objectives are evident. The alignment of NIST control families with SDGs offers a structured approach for organizations to address cybersecurity in the context of broader sustainability goals. By recognizing and leveraging these correlations, stakeholders can enhance both security and sustainability efforts, contributing to a more resilient and equitable global society with economic stability. Cybersecurity is vital for fostering sustainable economic growth by safeguarding a digital infrastructure that supports economic activities, ensuring the security of digital fundraising initiatives for sustainable development, and protecting the financial sector along with other crucial areas essential to economic progress. This research offers key insights into the necessity of incorporating cybersecurity strategies within the framework of the SDGs to advance sustainable economic

development. As the digital landscape evolves, the role of cybersecurity in creating a secure and resilient digital environment will be increasingly important for driving sustainable economic growth and fulfilling the broader goals of the SDGs.

Author Contributions: Conceptualization, G.D.; Methodology, G.D., A.M.P., S.K. and E.S.; Validation, S.E.; Investigation, data curation, S.E., T.K. and G.D.; Writing—original draft, G.D.; writing—review and editing, G.D., E.S., A.M.P., S.K. and I.O.; Visualization, G.D.; Supervision, T.K.; Project administration, S.E. and T.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work has received funding from the European Union's—HORIZON-CL3-2021-INFRA-01 through ATLANTIS (https://www.atlantis-horizon.eu/, accessed on 12 November 2024) project under grant agreement No. 101073909.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: Authors Georgia Dede, Anastasia Maria Petsa, Stelios Kavalaris, Spyridon Evangelatos and Ioannis Oikonomidis were employed by the company Netcompany Intrasoft S.A. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. United Nations. Available online: https://sdgs.un.org/goals (accessed on 12 November 2024).
2. R. 5. NIST Special Publication 800-53, Security and Privacy Controls for Informations Systems and Organizations. 2020. Available online: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (accessed on 12 November 2024).
3. Bilek-Steindl, S.; Kettner, C.; Mayrhuber, C. Sustainability, Work and Growth in the Context of SDG 8. *Empirica* **2022**, *49*, 277–279. [CrossRef] [PubMed]
4. Kynčlová, P.; Upadhyaya, S.; Nice, T. Composite index as a measure on achieving Sustainable Development Goal 9 (SDG-9) industry-related targets: The SDG-9 index. *Appl. Energy* **2020**, *265*, 114755. [CrossRef]
5. Odumesi, J.O.; Sanusi, B.S. Achieving Sustainable Development Goals from a Cybersecurity Perspective. In Proceedings of the Cybersecure Nigeria Conference, Abuja, Nigeria, 11–12 July 2023.
6. Vijarania, M.; Gupta, S.; Agrawal, A.; Misra, S. Achieving Sustainable Development Goals in Cyber Security Using AIoT for Healthcare Application. In *Artificial Intelligence of Things for Achieving Sustainable Development Goals*; Springer Nature: Cham, Switzerland, 2024; pp. 207–231.
7. Andrade, R.O.; Yoo, S.G.; Tello-Oquendo, L.; Ortiz-Garcés, I. Cybersecurity, sustainability, and resilience capabilities of a smart city. In *Smart Cities and the UN SDGs*; Elsevier: Amsterdam, The Netherlands, 2021; pp. 181–193.
8. Karuppiah, K.; Sankaranarayanan, B.; Ali, S.M.; Priyanka, R. A fsQCA-Based Framework for Cybersecurity of Connected and Automated Vehicles: Implications for Sustainable Development Goals. *Vehicles* **2024**, *6*, 484–508. [CrossRef]
9. Sulich, A.; Rutkowska, M.; Krawczyk-Jezierska, A.; Jezierski, J.; Zema, T. Cybersecurity and sustainable development. *Procedia Comput. Sci.* **2021**, *192*, 20–28. [CrossRef]
10. Ige, A.B.; Kupa, E.; Ilori, O. Aligning Sustainable Development Goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Adv. Res. Rev.* **2024**, *19*, 344–360.
11. Chukwurah, E.G.; Okeke, C.D.; Ekechi, C.C. Innovation green technology in the age of cybersecurity: Balancing sustainability goals with security concerns. *Comput. Sci. IT Res. J.* **2024**, *5*, 1048–1075. [CrossRef]
12. Vasiu, I.; Vasiu, L. Cybersecurity as an essential sustainable economic development factor. *Eur. J. Sustain. Dev.* **2018**, *7*, 171–178. [CrossRef]
13. Djenna, A.; Harous, S.; Saidouni, D.E. Internet of things meet Internet of threats: New concern cyber security issues of critical cyber infrastructure. *Appl. Sci.* **2021**, *11*, 4580. [CrossRef]
14. Priya, N. Cybersecurity considerations for industrial IoT in critical infrastructure sector. *Int. J. Comput. Organ. Trends* **2022**, *12*, 27–36. [CrossRef]
15. Information Security Forum. Available online: https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security/ (accessed on 12 November 2024).
16. NIST. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf (accessed on 12 November 2024).
17. ISO. Available online: https://www.iso.org/standard/75652.html (accessed on 12 November 2024).
18. Kravchenko, T.; Bogdanova, T.; Shevgunov, T. Ranking requirements using MoSCoW methodology in practice. In *Computer Science On-Line Conference*; Springer International Publishing: Cham, Switzerland, 2022; pp. 188–199.
19. ENISA Threat Landscape 2024. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (accessed on 12 November 2024).

20. Case, D.U. *Analysis of the Cyber Attack on the Ukrainian Power Grid*; Electricity Information Sharing and Analysis Center (E-ISAC): Atlanta, GA, USA, 2016; Volume 388, p. 3.
21. Beerman, J.; Berent, D.; Falter, Z.; Bhunia, S. A review of colonial pipeline ransomware attack. In Proceedings of the 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), Bangalore, India, 1–4 May 2023; pp. 8–15.
22. Al Allaf, A.; Totonji, W. Exploring IoT Security Threats and Forensic Challenges: A LiteratureReview and Survey Study. 2023. Available online: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1764110&dswid=5555 (accessed on 12 November 2024).
23. Datta, P.M.; Acton, T. Ransomware and Costa Rica's national emergency: A defense framework and teaching case. *J. Inf. Technol. Teach. Cases* **2024**, *14*, 56–67. [CrossRef]
24. Usmani, M.A.; Usmani, K.A.; Kaleem, A.; Samiuddin, M. Cyber Threat Migration: Perpetuating in the Healthcare Sector and Agriculture and Food Industries. In *Advances in Cyberology and the Advent of the Next-Gen Information Revolution*; IGI Global: Hershey, PA, USA, 2023; pp. 62–85.