applied sciences

MDPI

Review

Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance

Misael Sousa de Araujo [1,*], Bruna Aparecida Souza Machado [2,3] and Francisco Uchoa Passos [2]

[1] General Coordination of Information Technology Management, Oswaldo Cruz Foundation-Fiocruz, Rio de Janeiro 21040-900, Brazil
[2] Post-Graduate Program in Industrial Management and Technology, University Center SENAI CIMATEC, Salvador 41650-010, Brazil; brunam@fieb.org.br (B.A.S.M.); uchoapassos@gmail.com (F.U.P.)
[3] SENAI Institute of Innovation (ISI) in Health Advanced Systems (CIMATEC ISI SAS), SENAI CIMATEC, Salvador 41650-010, Brazil
* Correspondence: misael.araujo@fiocruz.br; Tel.: +55-21-3885-1724

Abstract: Cyber resilience is a topic of extreme relevance to organizations in the most diverse segments of activity, where the concept of resilience presents nuance in its different dimensions, in addition to the need to recognize and distinguish the different stages that characterize the state of cyber resilience. Thus, the aim of this article is to understand the various concepts of cyber resilience in its different contexts and dimensions. To this end, bibliographic research was carried out through the process of indirect documentation in articles, books, and publications on the subject. The main stages of resilience were mapped, and an analysis was produced of how these stages have evolved over the years. Finally, an updated proposal for standing for the stages of cyber resilience was presented, based on the consolidation of proposals from the entire framework studied in this work. This review emphasizes the importance of cyber resilience and understanding the stages that characterize cyber resilience, highlighting the need for its further integration into the organizations in the most diverse segments of activity management.

Keywords: resilience; cyber resilience; resilience stages; information security; cyber security

Citation: Araujo, M.S.d.; Machado, B.A.S.; Passos, F.U. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Appl. Sci.* **2024**, *14*, 2116. https://doi.org/10.3390/app14052116

Academic Editors: Chuanyi Liu, Xiaoyong Li, Chuankai Zhang and Peiyi Han

Received: 26 December 2023
Revised: 20 February 2024
Accepted: 25 February 2024
Published: 4 March 2024

1. Introduction

Cyber resilience is an interdisciplinary field of study, being investigated from multiple points of view [1]. Information and Communication Technology (ICT) has become strongly integrated into economies and societies, where most socio-technical systems are designed to function based on a stable environment [2]. The complexity of digital environments leaves organizations more exposed to cyber threats, where the issue of cyber resilience has grown in importance [3].

The digital transformation process has brought profound change to organizations and has significantly altered the user experience, markets, relationships, and cultural differences. The adoption of emerging technologies such as AI, big data, blockchain, among others, while driving the digital transformation process, has brought significant new security risks, highlighting the importance of cybersecurity as an essential component for business resilience [4]. Cyber threats can be considered a universal problem that affects all kinds of organizations [5]. Thus, the possible responses to security incidents are crucial security challenges in both the public and private sectors, as well as in people's private lives in general.

A report by the European Union Agency for Cybersecurity (ENISA) on the 2023 threat landscape points to a significant increase in both the variety and quantity of cyber-attacks. Partly influenced by the war in Ukraine, there is an expansion of hacktivism with the emergence of new groups and an increase in cases of ransomware, as well as other

threats such as malware, social engineering, threats against data, denial of service attacks, manipulation and interference of information, as well as attacks on the supply chain [6].

Cyber-attacks are considered to be one of the most serious threats to organizations and for those that rely heavily on Information Technology (IT), so generating value is not only about avoiding cyber-attacks, but also about being able to respond in order to minimize their disastrous effects on operations [7]. The challenge of keeping data secure is increasing at the same speed as the quantity and variety of data being stored exponentially over the years, requiring information security professionals to constantly seek alternatives to proactively test and evaluate the physical and technical vulnerabilities of organizational systems, to the extent that the defenses themselves increase the legal and reputational risks [8]. However, cyber vulnerabilities and incidents not only affect an organization's operations, but also constitute a growing threat to economic, democratic, and social resilience [9].

In the public sector, security incidents are frequently observed in public administration units in all countries, where the security of the state and its citizens depends on a cybersecurity culture to help ensure cyber resilience, especially in dynamic scenarios of strong change such as that caused by the COVID-19 pandemic [10]. However, cyber threats and security concerns also affect organizations in the private sector, where small- and medium-sized companies are generally less mature in terms of security and resilience and are more exposed to vulnerabilities [11].

Knowledge of factors associated with cyber resilience is increasing all the time, making it imperative to adapt quickly to changes in order to properly understand the topic. [12]. Integrating the aspects of capacity and resilience has become crucial to the success of business strategies, making the organization's operations capable of facing complex challenges and supporting the organization's long-term growth [13].

Thus, the goals of this article are: (a) to understand the various concepts of cyber resilience in their various contexts and dimensions; (b) to highlight the relevance of cyber resilience for organizations in the most diverse segments of activity; and to (c) present a proposal for representing the stages or phases that characterize the state of cyber resilience based on the research conducted on the various definitions presented by the authors. In this way, it is believed that the consolidation of the depiction of these stages will be useful in future academic studies, harmonizing the many approaches discovered in the literature by various writers.

2. Methods

The purpose of this research is to better comprehend the significance of numerous ideas linked to cyber resilience and to offer a consistent presentation of the stages that define cyber resilience.

The Web of Science and Science Direct databases were used to search for papers. The inclusion criteria were research articles, review articles, conferences, and book chapters; articles developed between 2015 and 2023 were also considered. The exclusion criteria were articles written in languages other than English; repeated papers; articles that were not related to the topic or were irrelevant to the research; and papers that did not clearly present resilience concepts or definitions of resilience stages. The descriptors (resilience, cyber resilience, concept, definition, phase, stage) were applied to the title, abstract, and keywords, yielding 189 publications. After reading the title, abstract, and introduction, 48 articles were chosen for further reading. After reading these articles, a further 14 articles were added after searching for works cited by the authors, making a total of 62 articles. In total, 141 articles were excluded.

To identify the various stages that describe the cyber resilience cycle, this study carried out an analysis of the different concepts presented by the various authors studied. Each term described in the author's definition of resilience was carefully identified, evaluated, and grouped with other terms that had the same meaning.

A schematic diagram illustrating the life cycle of cyber resilience has been constructed, incorporating the recognized stages of cyber resilience. These stages have been categorized into three distinct time periods: pre-crisis, crisis, and post-crisis.

3. Cyber Resilience: Fundamental Concepts

3.1. Concepts of Resilience in Its Various Contexts

The term resilience can be understood as the ability to maintain the necessary capacity in the face of adversity [14]. It can also be understood as the "ability to adapt and recover quickly from any known or unknown changes in the environment" [15] or even as "the capacity of a cyber-system to perform effectively, regardless of the hazards" [5].

Presidential Policy Directive No. 21, issued by the American Government on 12 February 2013, sets forth a national policy for the U.S. government about the security and resilience of critical infrastructure. Resilience, as defined in the directive, refers to "the ability to prepare for and adapt to changing conditions and to withstand and recover quickly from disruptions". Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or natural threats or incidents [16].

It can also be understood as the "ability to withstand, absorb, recover from or successfully adapt to adversity or a change in conditions", or in an expanded definition, it can also be understood as the "ability of systems, infrastructures, government, businesses and citizens to withstand, absorb, recover from or adapt to an adverse event that could cause damage, destruction or loss of national importance" [17].

Hollnagel et al. [18] defines resilience as the "intrinsic capacity of a system to adjust its functioning before, during or after changes and disturbances, so that it can sustain the necessary operations under expected and unexpected conditions".

3.1.1. Organizational Resilience

The International Organization for Standardization (ISO) defines organizational resilience as the ability to absorb and adapt to a changing environment to meet its goals. It also adds that more resilient organizations can anticipate and respond to threats and opportunities arising from sudden or gradual changes in their internal and external context, where increasing resilience can be a strategic organizational objective, the result of good business practices and effective risk management [19].

The ability to develop organizational resilience is a key factor in the operations of organizations, as well as their ability to adapt and operate consistently over the long term [20]. Organizational resilience has a dynamic and contextual approach, since an organization's level of resilience can change over time depending on the importance the organization attaches to the topic (dynamic), as well as the specific needs that require organizations to take a tailor-made approach (contextual) [21].

Organizational resilience is linked not only to the survival of organizations—i.e., their ability to produce quick and effective responses in times of adversity, facing their strategic challenges and ensuring business continuity—but also to being able to contribute to the evolution and growth of the organization based on the learning produced by the adaptations and proactivity required in times of crisis, enabling the organization to acquire a competitive advantage in complex and challenging business environments [22–24].

3.1.2. Operational Resilience

The Gartner Information Technology Glossary presents a slightly broader concept of resilience, but one that also relates to security. The term operational resilience can be understood as initiatives that expand business continuity management programs with a focus on impacts, connected to risk appetite and tolerance levels in the event of an interruption in the delivery of products or services to internal and external stakeholders, such as employees, customers, citizens and partners [25].

CERT/SEI, a cybersecurity division of the Software Engineering Institute, defines operational resilience as the ability of an organization to continue to de-perform its mission in the face of stress and disturbances that do not exceed its operational limit [26].

3.1.3. Cyber Resilience

Cyber resilience is part of the concern of organizational resilience, since cyber incidents that jeopardize information security have the potential to damage the operation of organizations, jeopardize the achievement of their strategic goals and cause financial losses. "Organizational resilience refers to the ability of a system to adapt to change: a very contemporary concept that is finding increasing importance in our ever-changing society and is also taking on greater relevance in the cyber context. Therefore, the ability of organizations to react to cyber-attacks and to evolve to a new robustness after successful outbreaks recalls the concept of resilience and brings to the evolution of this concept that of cyber resilience" [27].

Cyber security can also be understood as "the ability of a cyber physical production system to respond to and recover from operational disturbances and risks" [28].

The Glossary of Information Security prepared by the Office of Institutional Security of the Brazilian Presidency of Republic defines resilience as the "ability of an organization or infrastructure to withstand the effects of an incident, attack or disaster and return to normal operations" [29].

The NIST Computer Security Resource Center Glossary defines cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises in systems that use or are enabled by cyber resources. Cyber resilience is intended to enable mission or business objectives that rely on cyber resources to be achieved in a contested cyber environment" [30].

Another definition is presented by the World Economic Forum, where cyber resilience is understood as "the ability of systems and organizations to withstand cyber events, measured by the combination of 'mean time to failure' and 'mean time to recovery" [31].

Other authors define cyber resilience as "the ability to continuously deliver the expected outcome despite adverse cyber events" [32] or as "the ability of a system to protect itself from incidents of cyber-attacks and maintain an acceptable level of performance, maintaining critical functionality and the timely restoration of the quality of services to the level that existed before the incident" [33].

3.2. The Relevance of Cyber Resilience in Various Segments

In the literature, there are several studies on the cyber resilience of organizations, whether they are public or private and in a wide range of segments: aviation, critical infrastructure, the financial system, health, industry, supply chains, among others. In recent years, there has been an increase in the number of cyber-attacks targeting Industrial Control Systems, which are also used in critical infrastructure systems [34]. Cyber threats represent a strategic risk and require joint work between the IT and business areas to make effective decisions, since many failures stem from organizational issues rather than technical problems [5].

3.2.1. Civil and Military Aviation

Cyber security and cyber resilience are emerging and urgent issues in next-generation air traffic surveillance systems, where critical air navigation systems in civil aviation can negatively affect the economic and political sectors, to the point that the International Civil Aviation Organization—ICAO considers cyber security and cyber resilience as emerging issues in the field of aviation worldwide [35]. In military aviation, cyber and electromagnetic activities have become prevalent on today's battlefields and the armed forces are witnessing the introduction of increasingly complex and interconnected weapons systems, to the point where US military doctrine classifies cyberspace as the fifth dimension of the battlefield [36,37].

3.2.2. Critical Infrastructures

Another segment where resilience is viewed with strong concern is critical infrastructures such as electricity, water treatment, and transportation. The growing adoption of cyber-physical systems in modern industrial plants for water treatment and distribution must consider the perspective of cyber resilience as a way of complementing a traditional assessment of physical resilience, this point of view being a central issue for critical infrastructures, considering the potential social and economic consequences that a disturbance can represent [38]. Risks associated with the integration of the computational, communication and physical aspects of critical cyber infrastructures, whose potential risks associated with failures affect the guarantee of resilience [39]. As the world becomes increasingly interconnected, the use of and dependence on Internet of Things (IoT) technology and other self-adaptive systems increases, requiring greater cyber resilience of critical infrastructures, at the risk of catastrophic impacts on society as a whole, due to society's growing dependence on these systems [40]. Detecting, preventing, and mitigating cyber threats is a concern for most organizations, especially those in critical infrastructure sectors [41].

3.2.3. Electricity

Power generation and distribution systems are critical infrastructures operated under the control of intelligent devices and interrelated to cyber-physical processes characterized by vulnerability to cyber-attacks [42]. Strengthening cyber security and resilience in the electricity sector has become a global necessity [43]. The use of intelligent energy networks (known as Smart Grids) makes it possible to automate, monitor, and control energy consumption, offering extremely reliable energy systems. Conversely, the use of smart grids for communication increases the probability of attacks on these grids. These attacks can lead to disruptions, such as inaccurate meter readings, false electricity demands, and impaired protective mechanisms. Consequently, a resilient communications network that can withstand cyber threats is necessary [44]. Still, on the subject of the electricity sector, the concept of the microgrid—widely used for integrating distributed generation units (e.g., photovoltaic units, diesel engines and wind turbines)—is capable of providing improved services, but the cyber and physical structures of microgrids are more prone to cyber and physical attacks [45].

3.2.4. Transport

In the transport sector, while advances in information technology and interconnectivity have improved the efficiency of the transport infrastructure, they have also created greater risk associated with cyber systems [46]. With the advance of new technologies and applications, such as wireless technologies, mobile applications, cloud computing, artificial intelligence, the internet of things, etc., cyber security is becoming increasingly important, making it essential to build an environment conducive to increasing cyber resilience at all levels and reacting to cyber-attacks when they occur [47].Even in maritime navigation, cyber resilience has been a growing concern, where studies have been carried out to examine the properties of cyber resilience from three elements: combining information from multiple sensors, diagnosing non-normal behavior and detecting changes [48].

3.2.5. Industry

In the industry sector, there are several studies that relate the concern between security and cyber resilience. One approach is cyber security and resilience mechanisms for manufacturing applications using software-defined networks (SDN) [49]. Another approach refers to resilience in the context of the cyber-physical system, based on approaches focused on the application domain and organizational aspects [50]. Industrial Control Systems (ICSs), despite their great capacity for interconnection and adaptability, are considered highly vulnerable, and attention needs to be paid to ICSs that deal with critical infrastructure assets [51]. The study of resilience, especially when related to physical infrastructure, has been extensively re-examined within risk analysis [52]. Industry 4.0

comes with the promise of reconciling performance and agility, but with the expected improvements also come new cyber threats, since there is a greater attack surface and number of access connections [53].

3.2.6. Supply Chains

Attacks on supply chains have always been a source of concern for organizations, but since 2020 we have seen a greater number of attacks and in a more organized way. This can be explained in part by the fact that organizations have more robust security protections in place and attackers are focusing on suppliers. Attacks on supply chains have a cascading effect, since a successful attack on one supplier has the potential to affect a large number of client companies, causing consequences such as system downtime, monetary losses and damage to organizations' reputations [54]. The advancement of emerging technologies such as IoT and AI has led to changes in the relationships between supplier and consumer organizations, since the most modern supply chains make massive use of technologies to satisfy customer demands, compared to traditional supply chains, imposing new security concerns due to co-connection networks and shared data [55]. Assessing the cyber resilience of a supply chain becomes a crucial task to make organizations competitive and resilient to invasions [56].

3.2.7. Financial System

The financial system has also been a frequent target of attacks for various reasons, such as the potential financial gains from a successful attack; obtaining resources to finance terrorist actions; or causing the collapse of national and global financial markets [57]. Data protection has sought to use reliable and user-friendly digital identification systems to provide protection mechanisms that are secure and robust enough to guarantee the resilience of various organizations, including banks [58]. Financial institutions are increasingly dependent on digital technologies and are exposed to cyber-attacks, technical failures, human error and natural disasters, so cyber resilience is becoming an urgent necessity [59].

3.2.8. Digital Health

The increased adoption of medical equipment and smart mobile devices has made healthcare organizations more exposed to threats, especially the threat of Ransomware, where the size and complexity of operations added to the numerous legacy and incompatible systems bring enormous challenges in implementing effective security measures, requiring an in-depth study of the sector for its resilience [60]. The literature on resilience in the field of health [61,62] highlights that the healthcare sector makes use of various information technology resources that are considered critical infrastructures. These critical infrastructures are the subject of security and resilience concerns, since cyber criminals are attracted by the monetary potential of personal and health data stored by hospitals and due to the growing number of incidents in the health sector in recent years. There is also widespread adoption of information technology resources that integrate healthcare systems and networks of connected medical devices, coupled with an increasing number of cyber threats. It is therefore essential to ensure that these critical infrastructures are protected, available and resilient against threats so that they can adequately support the areas that make use of these technologies. Another concern in the field of Digital Health is related to data privacy, especially due to regulations in recent years, for example GDPR in the European Union. If an organization is not sufficiently resilient from a cyber point of view, this can lead to the leakage of its patients' personal data. Patient data privacy must be properly managed in the digital transformation of healthcare systems, enabling better organizational governance of healthcare organizations [4].

3.3. Typifying the Stages of the Cyber Resilience Cycle

The literature review shows that the various authors studied describe cyber resilience in a dynamic represented by a cycle characterized by gradual stages of resilience, which

can be summarized as follows: PR = Preparation | DT = Detection | RT = Resistance | RP = Response | AD = Adaptation | RC = Recovery | LN = Learning.

A mapping was made of the various definitions found in the literature on the concept of resilience, as well as the stages that characterize this resilience, as shown in Table 1.

Table 1. Mapping the stages of resilience in the reviewed literature.

Title	Category	Author	Year	PR	DT	RT	RP	AD	RC	LN
Understanding the management of cyber resilient systems	Cyber resilience	[27]	2020				X			X
Organizational Cyber Resilience: Management perspectives	Stages of cyber resilience	[5]	2023	X		X		X	X	
Cyber Resilience—Fundamentals for a Definition	Cyber resilience	[32]	2015					X		
Information Security Glossary	Cyber resilience	[29]	2019			X			X	
Cyber Resilience Progression Model	Phases of cyber resilience	[63]	2020	X	X	X	X		X	X
Department of Homeland Security Risk Lexicon	Resilience	[17]	2008			X		X	X	
ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems	Cyber resilience	[33]	2019			X	X			
Resilience engineering in practice: a guidebook	Resilience	[18]	2011	X		X		X		
Security and resilience—Organizational resilience—Principles and attributes	Organizational resilience	[19]	2022		X	X	X	X		
Does applying a circular business model lead to organizational resilience? Mediating effects of industry 4.0 and customers integration	Organizational resilience	[20]	2023			X		X		
Cyber resilience models of systems for monitoring and operational dispatch control of electric power systems	Stages of cyber resilience	[42]	2022			X	X	X	X	
The relationship between slack resources and organizational resilience: The moderating role of dual learning	Organizational resilience	[22]	2023			X			X	X
Social media use, corporate entrepreneurship, and organizational resilience: A recipe for SMEs success in a post-COVID scenario	Organizational resilience	[23]	2023				X	X	X	X
A Maturity Framework for Operational Resilience and Its Application to Production Control	Operational resilience	[28]	2018				X		X	
Developing Cyber-Resilient Systems: A Systems Security Engineering Approach	Cyber resilience	[30]	2021		X	X		X	X	
CERT Resilience Management Model	Operational resilience	[26]	2016			X				
Presidential Policy Directive–Critical Infrastructure—Security and Resilience	Resilience	[16]	2013	X		X		X	X	
Cyber resilience recovery model to combat zero-day malware attacks	Stages of cyber resilience	[64]	2020	X	X		X		X	X
Resilience in the Cyberworld: Definitions, Features and Models	Stages of cyber resilience	[65]	2021	X	X	X		X	X	
Systems engineering handbook: a guide for system life cycle processes and activities	Resilience	[14]	2015			X	X			
Partnering for Cyber Resilience: Risk and Responsibility in a Hyper connected World—Principles and Guidelines	Cyber resilience	[31]	2012			X				
Introduction to the Security Engineering Risk Analysis (SERA) Framework	Stages of cyber resilience	[66]	2019	X	X			X	X	
How can new-energy vehicle companies use organizational resilience to build business ecological advantages? The role of ecological niche and resource orchestration	Organizational resilience	[24]	2023				X			
Cyber-physical resilience modeling and assessment of urban roadway system interrupted by rainfall	Stages of cyber resilience	[67]	2020			X		X	X	

PR = Preparation | DT = Detection | RT = Resistance | RP = Response | AD = Adaptation | RC = Recovery | LN = Learning.

4. Main Stages and Research Aims

This section of the article is a follow-up to Section 3.3, where the main concepts of resilience presented by the authors studied were consolidated in Table 1. As can be seen in Section 3.1, there are various concepts of resilience with different definitions. Investigating

the concept of cyber resilience reveals nuances in its definition. The question then arises as to what it really means for an organization to have cyber resilience.

Based on the various definitions of resilience brought by the authors in Table 1, different verbs that demonstrate capabilities such as responding, recovering, adapting, etc., were identified in the text. These capabilities can be observed at different moments (here called phases/stages) in a timeline in the face of an adverse event—a cyber incident, for example—that puts the organization's operations at risk if it does not have adequate cyber resilience. Thus, the research question proposed for this study is to understand which stages characterize cyber resilience.

Based on the concepts researched by the authors studied and consolidated in Table 1, it was possible to map out seven stages used to characterize a resilience cycle: preparation, detection, resistance, response, adaptation, recovery, and learning. The number of citations for each stage can be seen in Figure 1, where the stages of resistance, response, adaptation, and recovery are most frequently cited by the authors as stages that characterize a state of resilience, while fewer authors present preparation, detection, and learning.

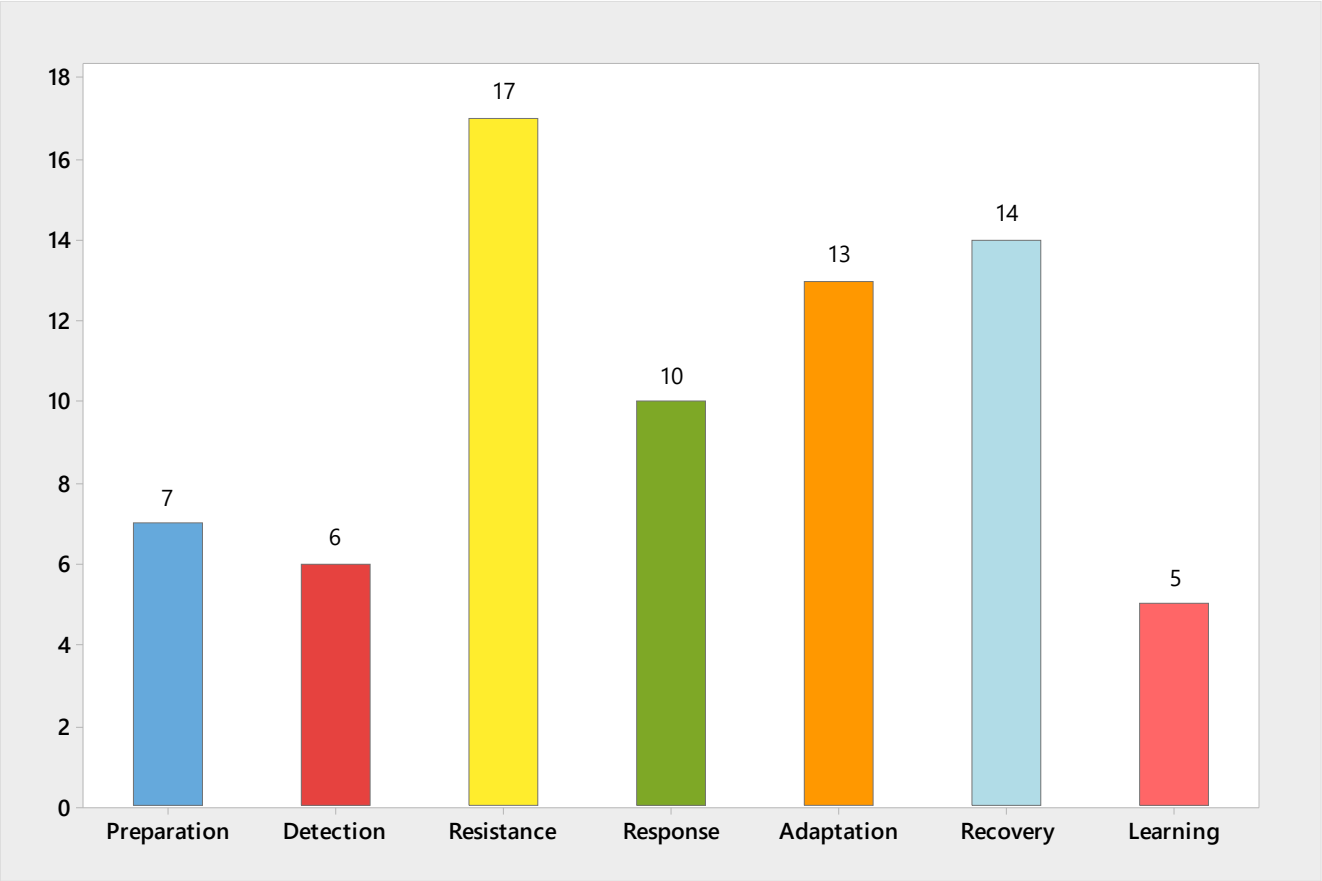

Figure 1. Number of citations to the stages of resilience.

Analyzing the authors that specifically address the subject of cyber resilience reveals a modest variation, with resistance, adaptation, and recovery being the most referenced stages, while preparation, detection, response, and learning are less cited, as shown in Figure 2.

However, it is important to highlight that these concepts are evolving over time as our understanding of the stages of cyber resilience evolves and new terms are adopted.

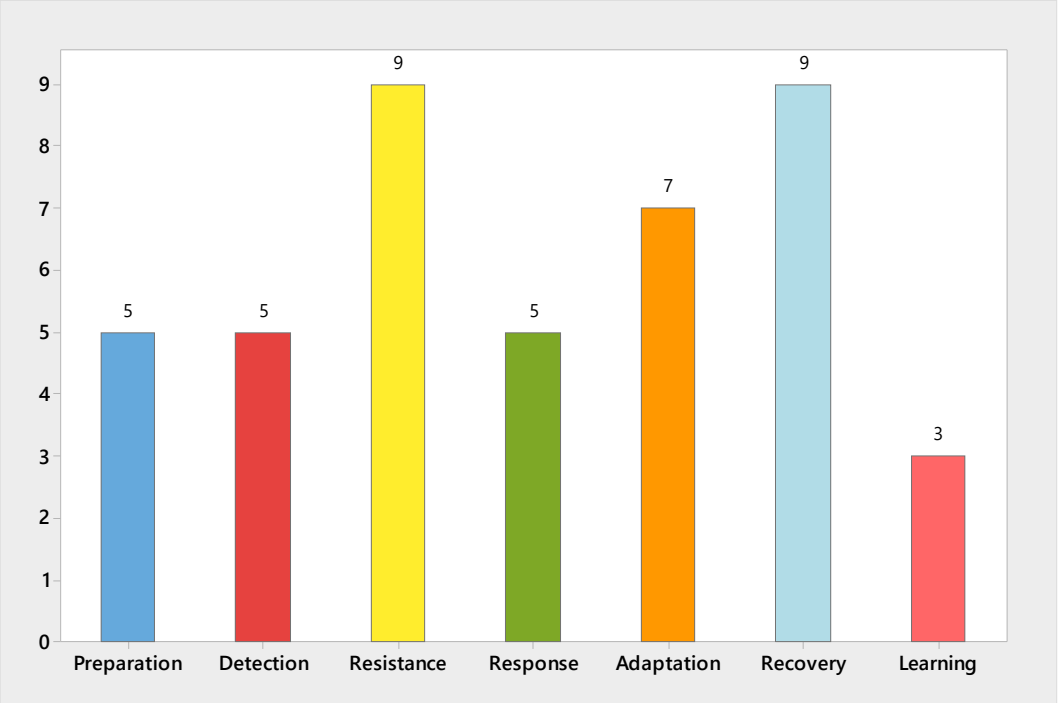

Figure 2. Main citations to the stages of cyber resilience.

Figure 3 shows how the concept of resilience has evolved over the years. Based on the authors studied, resilience was initially understood as resistance, adaptation, and recovery, and over the years and the progress of studies on the subject, other stages have been added, allowing the characterization of new stages such as detection and learning, which are more frequently found in the literature researched from 2020 onwards.

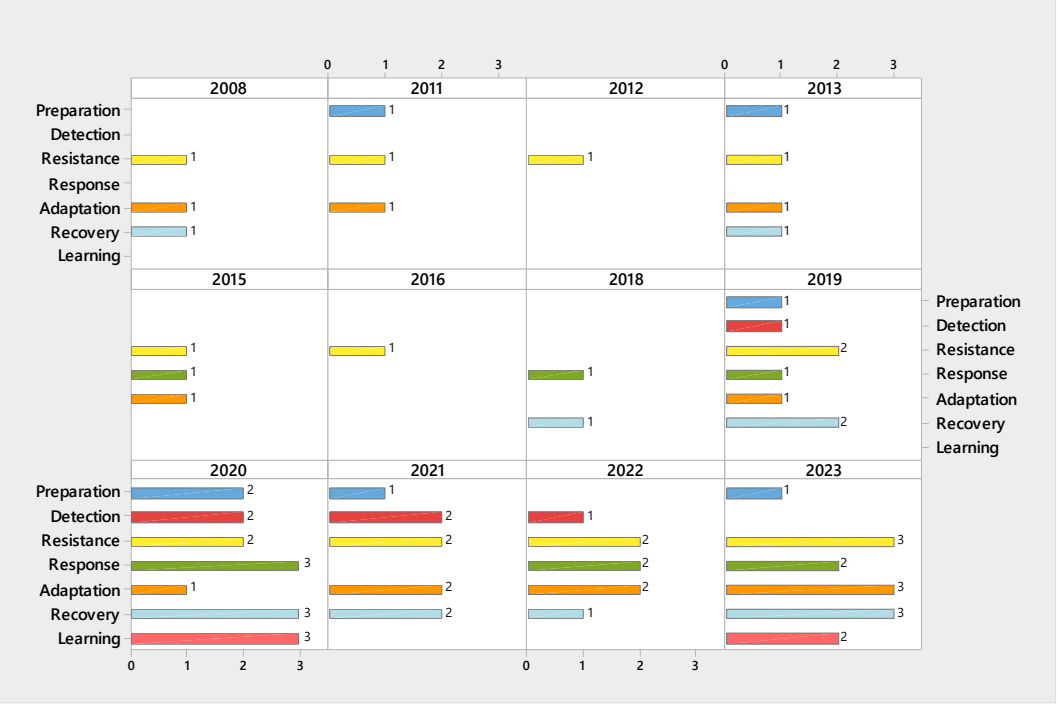

Figure 3. Characterization of the stages of resilience over the years.

Also based on the authors studied shown in Table 1, some of the stages in their definitions have overlapping concepts. A regrouping of these stages is therefore proposed by the authors of this work, trying to optimize the representation of cyber resilience, particularly for the purpose of measuring cyber resilience in future field works (Figure 4).

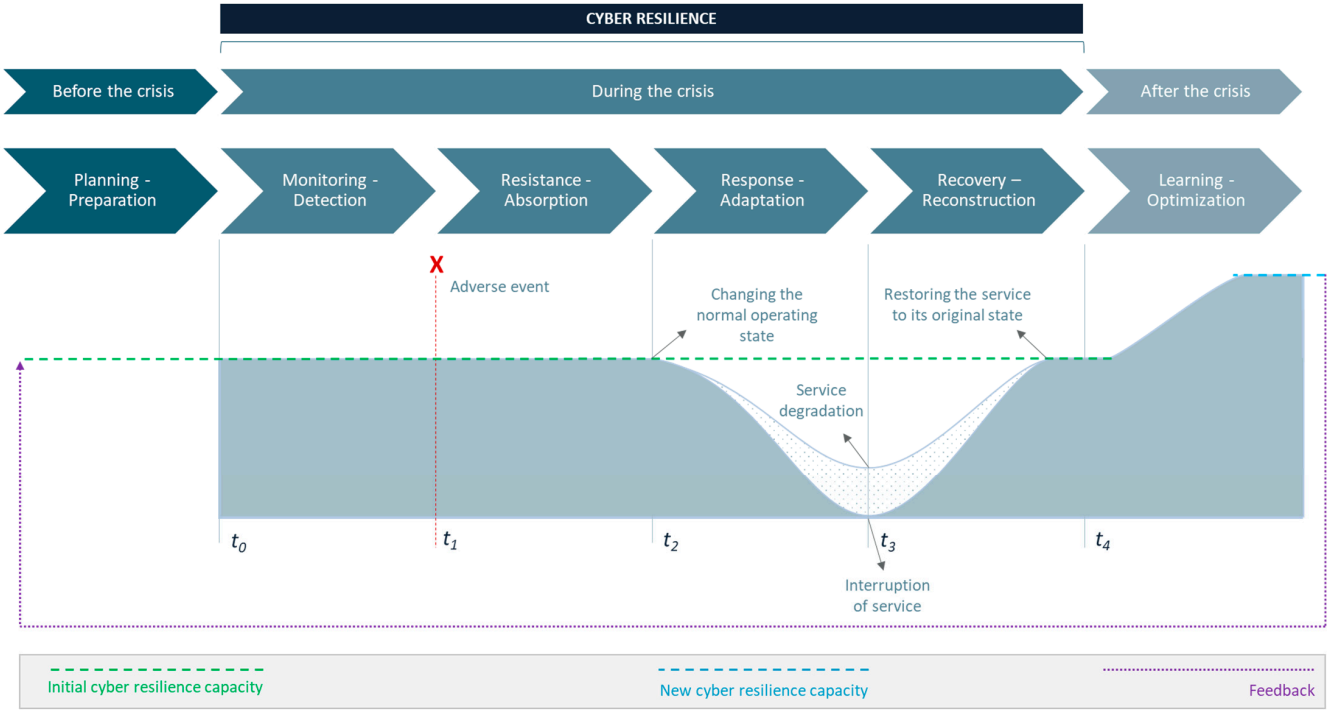

Figure 4. Representation of the stages of cyber resilience.

Figure 4 presents the mentioned proposal for cyber resilience states based on the mapping carried out with the authors studied, suggesting 4 stages of cyber resilience: Monitoring–Detection; Resistance–Absorption; Response–Adaptation; and Recovery–Reconstruction.

The 'Monitoring–Detection' and 'Resistance–Absorption' stages are not always consciously perceived by management, particularly in cases where the system is technically self-sufficient to automatically monitor, detect, resist, and absorb a given adverse event. Therefore, empirical assessments of these two stages would be subjective in nature. It should also be noted that the 'Monitoring–Detection' stage is a process that is carried out continuously and that its execution may overlap in different phases, i.e., monitoring/detection will take place before, during and after a crisis. However, for the purposes of representing cyber resilience, 'Monitoring–Detection' is the first stage of cyber resilience. Empirical assessments of the 'Response–Adaptation' and 'Recovery–Reconstruction' stages, on the other hand, could be made with reasonable objectivity since they are conducted by management.

It is important to highlight too that the two other stages (Planning–Preparation and Learning–Optimization) which, although they are not characterized as stages of resilience per se (Figure 4), are equally relevant to resilience. One of them is the planning and preparation stage—which precedes a crisis scenario—and is essential for achieving an effective response to the four stages of resilience presented. Another important stage is that of learning and optimization, since once a service has recovered and stabilized to the initial conditions, the learning produced by an event can be considered to improve the resilience system, adding this new knowledge to prepare an even more resilient system.

In this way, we have an initial time (t_0) where a particular IT service is observed in operation, when this service is monitored to identify adverse events (incidents) that could impact its availability/capacity, i.e., its security.

Once an adverse event (time t_1) has been detected—based on the monitoring and detection capacity of the previous stage—the resistance and absorption stage begin, where the security systems can respond in an automated way or by human decision and intervention to maintain their operating capacity, resisting and absorbing any negative impact produced by this event.

However, in some situations, there may be a degradation of the service (time t_2), where there is a partial loss or complete failure of its operating capacity. In this way, the response and adaptation stage begin, i.e., actions are taken to contain the event and ensure the continuity of operations (even with reduced capacity).

Finally, activities are carried out to recover and rebuild the environment/service (time t_3) to re-establish the initial operating conditions.

Table 2 below provides a brief explanation of each of the stages that characterize cyber resilience.

Table 2. Defining the stages of cyber resilience.

Stage	Scenario	Explanation
Planning–Preparation	Before the crisis	It includes the structuring and implementation of cyber security management processes to establish resilience capabilities in the operation of IT services.
Monitoring–Detection	During the crisis	It aims to provide automated tools capable of monitoring the availability and capacity of IT services, as well as identifying anomalies in operations and alerting the responsible parties.
Resistance–Absorption		This refers to the ability of established security systems to deal with a large volume of adverse events without impacting IT operations.
Response–Adaptation		It relates to the ability of systems to contain malicious events and reconfigure themselves in such a way as to preserve resources for maintaining IT operations at satisfactory levels.
Recovery–Reconstruction		It implements measures to restore or rebuild the affected IT services to satisfactory operating levels whenever there is a degradation or even an interruption of these services.
Learning–Optimization	After the crisis	It refers to the use of knowledge generated by previous cyber incidents to promote improvements in processes, staff training and the configuration of security solutions, improving the capacity of the whole cyber security system to deal with adverse situations.

5. Challenges and Future Directions

Cyber resilience has been the subject of numerous studies over time, but various aspects related to this subject still pose challenges and require more in-depth research. The following are issues related to the study of resilience from the point of view of some researchers.

The digital transformation, driven by the COVID-19 pandemic, has opened up space for cybercriminals to exploit vulnerabilities [4], while the assessment of cyber resilience has not advanced and is still in its infancy, requiring studies to develop robust and systematic assessment methods, traditionally anchored in two types of approaches: metrics-based and model-based [68].

Developing resilience requires a transition from conventional security measures to evolutionary and predictive approaches. While the conventional approach is based on static security measures, an evolutionary approach makes it possible to constantly improve cyber resilience based on adaptive defense tactics, allowing organizations, based on the history of previous incidents, to better understand their risks and evolve in the prevention of cyber-attacks. The predictive approach, on the other hand, will allow an organization to use data and analysis to predict potential threats, allowing the organization to adapt to new scenarios and provide more effective responses [13].

Adversarial training has proven to be an effective defense approach in training deep learning models to increase adversary robustness and can thus be improved and used to deal with attacks in general [69]. This is because, unlike conventional models, an additional step is added to the training of the model, where in addition to clean data, contradictory data is also used, increasing the robustness of the model against adversarial attacks [70,71]. Thus, the concept of adversarial training can also be used in cyber defense systems, increasing the resilience of these defense systems in the Monitoring–Detection, Resistance–Absorption, Response–Adaptation phases and especially in the Learning–Optimization phase. However, learning algorithms for cyber-attacks based on adversarial training still need to be explored [72].

Security and resilience in Industry 4.0 is also a challenge and requires an approach not only from a management point of view but also from an IT point of view, taking into account the three layers of exposure of cyber-physical systems: physical, network and computing [73]. Another cause for concern and one that requires more advanced studies are technologies that are considered radically new, such as AI, 5G, and 6G, the use of the cloud, high-performance computing, IoT and quantum computing [9]. Therefore, in order to make an organization more resilient, it is necessary to advance in the combination of cyber resilience and cyber security [5]. The cybersecurity capability framework also merits future research, in order to investigate the measurement of resilience levels of organizations' critical infrastructures from a socio-technical systems perspective to study the interrelationships between non-technical cybersecurity practices, human factors, and technical cybersecurity practices [74].

The resilience of electrical networks against possible cyber-attacks requires the implementation of algorithms and architectures in real-time simulation environments in order to optimize the performance of the cyber physical system in a cloud environment [75]. It is also necessary to advance the resilience perspective of cyber-physical systems to the detriment of traditional risk-based approaches, focusing research not only on investigating resilience from a technical perspective, but also from a socio-technical dimension [50]. One opportunity to improve the resilience of cyber-physical systems is to include natural disasters in the planning of such systems and to improve defense strategies [76].

In the healthcare field, cybersecurity is essential to ensure the privacy of patient data and the safety of medical devices. The adoption of emerging technologies, such as artificial intelligence (AI), big data, blockchain and cloud computing, has boosted digital transformation just as it has brought security risks. As such, organizations need to be fully aware of the threats that arise throughout the digital transformation process in order to provide greater resilience to healthcare organizations [4]. However, implementing security in the health sector remains a significant challenge due to the difficulty of implementation in the health sector, and more research is needed to understand this difficulty, not limited to issues related to the technology required, as well as the adoption of a sustainable and systematic approach to safety management [77]. Digital transformation in the health sector is becoming increasingly important in a post-industrial and knowledge-based society, where radical innovations in information technology necessitate effective management in terms of cybersecurity and resilience, despite the fact that there is still a lack of a comprehensive understanding of the factors that drive resilient and sustainable digital transformation in the health domain [78].

The complexity, breadth, and persistence of cyber-attacks means that there is a need for comprehensive research on the subject and not just from the perspective of a single discipline, i.e., there is a need for collaborative and interdisciplinary research [79].

In addition to the contributions made by this article, there are many other challenges related to the study of cyber resilience. Some of these challenges have already been listed above by the authors studied and others could be the subject of more in-depth studies proposed for future work. In addition, the authors of this article highlight the following gaps and challenges:

- How can we achieve a unified approach to managing an organization's risks, bringing organizational risk management closer to cyber risk management? In other words, how can cyber resilience issues be aligned with organizational resilience?
- How can we assess an organization's maturity in terms of its cyber resilience management processes? Which model should be chosen from the many available, or even in which cases should such a model be developed given a particular segment or sector?
- If a model needs to be developed, which reference documents (frameworks, guides, standards, etc.) should be adopted? Which scales (descriptors, levels, etc.) are most appropriate?
- What factors (human, political, cultural, etc.) can directly or indirectly influence cyber resilience?
- How can the government and academia contribute to raising awareness and improving the cyber resilience of organizations?
- How can resources such as automation and artificial intelligence (AI) help organizations' cyber resilience processes?

6. Conclusions

The study of resilience has been a highly relevant area of knowledge for organizations in all sectors, whether public or private, because resilience is required to ensure the continuity of an organization's services in unexpected circumstances and its survival in crisis scenarios. Section 3.1 presented the most varied definitions of resilience found in the literature for several concepts of resilience (organizational resilience, operational resilience, and cyber resilience).

Section 3.2 also looked at cyber resilience is one of the factors that concern organizations and demands focus for its appropriate understanding, planning, and effective adoption, considering the strong dependence of organizations on digital technologies to carry out their business, independent of their sector (industry, aviation, finance, etc.).

The analysis of cyber resilience concepts reveals that, in general, there is agreement that cyber resilience can be defined as the ability to resist, respond, and adapt in crisis situations. Section 3.3 mapped the definition of resilience given by the authors studied and consolidated it in Table 1. Section 4 analyzed these different proposed stages and their evolution over the years and presented a proposed representation of the stages of cyber resilience (Figure 4).

Thus, cyber resilience can therefore be characterized in four basic stages, in response to a crisis: Monitoring–Detection, Resistance–Absorption, Response–Adaptation, and Recovery–Reconstruction. In addition, there is also a Preparation–Planning stage (before a crisis) and a Learning–Optimization stage (after a crisis) (Table 2).

Although there is no consensus in the literature about the stages of resilience planning and post-crisis learning, in general, the Preparation–Planning stage is more concerned with information security management, i.e., the efforts needed to structure and improve security actions, while the Learning–Optimization stage is more concerned with improving the resilience system.

Finally, it is important to note that this study will serve as a basis for evaluations of resilience in organizations, as part of an empirical study that the authors of this paper are preparing. Although the proposed model for representing the stages of cyber resilience may still present nuances related to the interpretation of the literature review, we are confident that such kind of empirical study brings consistent contributions to the cyber resilience field.

Author Contributions: Conceptualization, M.S.d.A.; methodology, M.S.d.A.; software, M.S.d.A.; validation, F.U.P.; formal analysis, F.U.P.; investigation, M.S.d.A.; resources, M.S.d.A.; data curation, M.S.d.A.; writing—original draft preparation, M.S.d.A.; writing—review and editing, M.S.d.A., B.A.S.M. and F.U.P.; visualization, M.S.d.A.; supervision, F.U.P.; project administration, M.S.d.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Acknowledgments: The authors are grateful to University Center SENAI/CIMATEC (National Service for Industrial Training), Oswaldo Cruz Foundation-Fiocruz, and CNPq (B.A.S.M. is a Technological fellow from CNPq 306041/2021-9).

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

References

1. Attajer, A.; Chaabane, S.; Darmoul, S.; Sallez, Y.; Riane, F. Evaluation of Operational Resilience in Cyber-Physical Production Systems: Literature Review. *IFAC-Pap.* **2022**, *55*, 2264–2269. [CrossRef]
2. Neeme, S. Cyber Resilience: A Global Challenge. *Technol. Forecast. Soc. Chang.* **2022**, *184*, 122013. [CrossRef]
3. Annarelli, A.; Palombi, G. Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. *Sustainability* **2021**, *13*, 13065. [CrossRef]
4. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors* **2023**, *23*, 6666. [CrossRef]
5. Bagheri, S.; Ridley, G.; Williams, B. Organisational Cyber Resilience: Management Perspectives. *Australas. J. Inf. Syst.* **2023**, *27*. [CrossRef]
6. ENISA. *ENISA Threat Landscape 2023*; ENISA: Athens, Greece, 2023. [CrossRef]
7. Sepúlveda Estay, D.A.; Sahay, R.; Barfod, M.B.; Jensen, C.D. A Systematic Review of Cyber-Resilience Assessment Frameworks. *Comput. Secur.* **2020**, *97*, 101996. [CrossRef]
8. DeMarco, J.V. An Approach to Minimizing Legal and Reputational Risk in Red Team Hacking Exercises. *Comput. Law Secur. Rev.* **2018**, *34*, 908–911. [CrossRef]
9. Timmers, P. *Cybersecurity and Resilience from a Strategic Autonomy Perspective*, 1st ed.; Techno-Politics Series; European Liberal Forum: Brussels, Belgium, 2022; ISBN 978-2-39067-033-9.
10. Ubowska, A.; Królikowski, T. Building a Cybersecurity Culture of Public Administration System in Poland. *Procedia Comput. Sci.* **2022**, *207*, 1242–1250. [CrossRef]
11. Benz, M.; Chatterjee, D. Calculated Risk? A Cybersecurity Evaluation Tool for SMEs. *Bus. Horiz.* **2020**, *63*, 531–540. [CrossRef]
12. Mishra, D.K.; Ray, P.K.; Li, L.; Zhang, J.; Hossain, M.J.; Mohanty, A. Resilient Control Based Frequency Regulation Scheme of Isolated Microgrids Considering Cyber Attack and Parameter Uncertainties. *Appl. Energy* **2022**, *306*, 118054. [CrossRef]
13. Safitra, M.F.; Lubis, M.; Fakhrurroja, H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability* **2023**, *15*, 13369. [CrossRef]
14. INCOSE. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, 4th ed.; Walden, D.D., Roedler, G.J., Forsberg, K., Hamelin, R.D., Shortell, T.M., International Council on Systems Engineering, Eds.; Wiley: Hoboken, NJ, USA, 2015; ISBN 978-1-118-99941-7.
15. NIST. *Contingency Planning Guide for Federal Information Systems*; NIST: Gaithersburg, MD, USA, 2010.
16. The White House Office of the P.S. Presidential Policy Directive—Critical Infrastructure Security and Resilience. Available online: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed on 13 March 2022).
17. DHS. *DHS Risk Lexicon*; DHS: Washington, DC, USA, 2008.
18. Hollnagel, E.; Pariès, J.; Woods, D.D.; Wreathall, J. (Eds.) *Resilience Engineering in Practice: A Guidebook*; Ashgate studies in resilience engineering; Ashgate: Farnham, UK, 2011; ISBN 978-1-4724-2074-9.
19. *ISO 22316:2017(En)*; Security and Resilience—Organizational Resilience—Principles and Attributes. ISO: Geneva, Switzerland, 2017. Available online: https://www.iso.org/obp/ui#iso:std:iso:22316:ed-1:v1:en (accessed on 12 December 2022).
20. Jabbour, A.B.L.d.S.; Latan, H.; Chiappetta Jabbour, C.J.; Seles, B.M.R.P. Does Applying a Circular Business Model Lead to Organizational Resilience? Mediating Effects of Industry 4.0 and Customers Integration. *Technol. Forecast. Soc. Chang.* **2023**, *194*, 122672. [CrossRef]
21. Seville, E. *Resilient Organizations: How to Survive, Thrive and Create Opportunities through Crisis and Change*; Kogan Page Limited: London, UK, 2017; ISBN 978-0-7494-7855-1.
22. Mao, Y.; Li, P.; Li, Y. The Relationship between Slack Resources and Organizational Resilience: The Moderating Role of Dual Learning. *Heliyon* **2023**, *9*, e14044. [CrossRef]
23. Martín-Rojas, R.; Garrido-Moreno, A.; García-Morales, V.J. Social Media Use, Corporate Entrepreneurship and Organizational Resilience: A Recipe for SMEs Success in a Post-Covid Scenario. *Technol. Forecast. Soc. Chang.* **2023**, *190*, 122421. [CrossRef]

24. Xie, Y.; Chen, R.; Cheng, J. How Can New-Energy Vehicle Companies Use Organizational Resilience to Build Business Ecological Advantages? The Role of Ecological Niche and Resource Orchestration. *J. Clean. Prod.* **2023**, *415*, 137765. [CrossRef]
25. Gartner Definition of Operational Resilience—Gartner Information Technology Glossary. Available online: https://www.gartner.com/en/information-technology/glossary/operational-resilience (accessed on 20 November 2022).
26. SEI. CERT Resilience Management Model (CERT-RMM) Version 1.2. Available online: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084 (accessed on 22 August 2021).
27. Annarelli, A.; Nonino, F.; Palombi, G. Understanding the Management of Cyber Resilient Systems. *Comput. Ind. Eng.* **2020**, *149*, 106829. [CrossRef]
28. McFarlane, D.; Srinivasan, R.; Puchkova, A.; Thorne, A.; Brintrup, A. A Maturity Framework for Operational Resilience and Its Application to Production Control. In *Service Orientation in Holonic and Multi-Agent Manufacturing*; Springer: Cham, Switzerland, 2018; pp. 51–62. [CrossRef]
29. Brasil Glossário de Segurança da Informação. 2019. Available online: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663 (accessed on 5 October 2021).
30. NIST. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021; p. 76. [CrossRef]
31. WEF. *Partnering for Cyber Resilience: Risk and Responsibility in a Hyper Connected World—Principles and Guidelines*; WEF: Geneva, Switzerland, 2012; p. 16.
32. Björck, F.; Henkel, M.; Stirna, J.; Zdravkovic, J. Cyber Resilience—Fundamentals for a Definition. In *New Contributions in Information Systems and Technologies*; Rocha, A., Correia, A.M., Costanzo, S., Reis, L.P., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 311–316.
33. Haque, M.A.; Shetty, S.; Krishnappa, B. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. In Proceedings of the 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 27–29 May 2019; IEEE: Washington, DC, USA, 2019.
34. Ota, Y.; Mizuno, E.; Aoyama, T.; Hashimoto, Y.; Koshijima, I.; Asai, H.; Taniuchi, S. Designing Framework for Tabletop Exercise to Promote Resilience Against Cyber Attacks. In *Computer Aided Chemical Engineering*; Yamashita, Y., Kano, M., Eds.; Elsevier: Amsterdam, The Netherlands, 2022; Volume 49, pp. 1471–1476, ISBN 1570-7946.
35. Elmarady, A.A.; Rahouma, K. Actual TDoA-Based Augmentation System for Enhancing Cybersecurity in ADS-B. *Chin. J. Aeronaut.* **2021**, *34*, 217–228. [CrossRef]
36. De Santo, D.; Malavenda, C.S.; Romano, S.P.; Vecchio, C. Exploiting the MIL-STD-1553 Avionic Data Bus with an Active Cyber Device. *Comput. Secur.* **2021**, *100*, 102097. [CrossRef]
37. Lees, M.J.; Crawford, M.; Jansen, C. Towards Industrial Cybersecurity Resilience of Multinational Corporations. *IFAC-Pap.* **2018**, *51*, 756–761. [CrossRef]
38. Patriarca, R.; Simone, F.; Di Gravio, G. Modelling Cyber Resilience in a Water Treatment and Distribution System. *Reliab. Eng. Syst. Saf.* **2022**, *226*, 108653. [CrossRef]
39. Salvi, A.; Spagnoletti, P.; Noori, N.S. Cyber-Resilience of Critical Cyber Infrastructures: Integrating Digital Twins in the Electric Power Ecosystem. *Comput. Secur.* **2022**, *112*, 102507. [CrossRef]
40. Koelemeijer, D. Enhancing the Cyber Resilience of Critical Infrastructures through an Evaluation Methodology Based on Assurance Cases. *Procedia Comput. Sci.* **2018**, *126*, 1779–1791. [CrossRef]
41. Zohuri, B.; McDaniel, P. (Eds.) Chapter 14—Cyber Resilience and Future of Electric Power System. In *Introduction to Energy Essentials*; Academic Press: Cambridge, MA, USA, 2021; pp. 509–548, ISBN 978-0-323-90152-9.
42. Kolosok, I.; Gurina, L. Cyber Resilience Models of Systems for Monitoring and Operational Dispatch Control of Electric Power Systems. *IFAC-Pap.* **2022**, *55*, 485–490. [CrossRef]
43. Heymann, F.; Henry, S.; Galus, M. Cybersecurity and Resilience in the Swiss Electricity Sector: Status and Policy Options. *Util. Policy* **2022**, *79*, 101432. [CrossRef]
44. Maziku, H.; Shetty, S.; Nicol, D.M. Security Risk Assessment for SDN-Enabled Smart Grids. *Comput. Commun.* **2019**, *133*, 1–11. [CrossRef]
45. Ye, Z.; Yang, H.; Zheng, M. Using Modified Prediction Interval-Based Machine Learning Model to Mitigate Data Attack in Microgrid. *Int. J. Electr. Power Energy Syst.* **2021**, *129*, 106847. [CrossRef]
46. Tonn, G.; Kesan, J.P.; Zhang, L.; Czajkowski, J. Cyber Risk and Insurance for Transportation Infrastructure. *Transp. Policy* **2019**, *79*, 103–114. [CrossRef]
47. Tonhauser, M.; Ristvej, J. Disruptive Acts in Cyberspace, Steps to Improve Cyber Resilience at National Level. *Transp. Res. Procedia* **2019**, *40*, 1591–1596. [CrossRef]
48. Dagdilelis, D.; Blanke, M.; Andersen, R.H.; Galeazzi, R. Cyber-Resilience for Marine Navigation by Information Fusion and Change Detection. *Ocean Eng.* **2022**, *266*, 112605. [CrossRef]
49. Babiceanu, R.F.; Seker, R. Cyber Resilience Protection for Industrial Internet of Things: A Software-Defined Networking Approach. *Comput. Ind.* **2019**, *104*, 47–58. [CrossRef]
50. Colabianchi, S.; Costantino, F.; Di Gravio, G.; Nonino, F.; Patriarca, R. Discussing Resilience in the Context of Cyber Physical Systems. *Comput. Ind. Eng.* **2021**, *160*, 107534. [CrossRef]

51. González, S.G.; Dormido Canto, S.; Sánchez Moreno, J. Obtaining High Preventive and Resilience Capacities in Critical Infrastructure by Industrial Automation Cells. *Int. J. Crit. Infrastruct. Prot.* **2020**, *29*, 100355. [CrossRef]
52. Hausken, K. Cyber Resilience in Firms, Organizations and Societies. *Internet Things* **2020**, *11*, 100204. [CrossRef]
53. Theron, P. Through-Life Cyber Resilience in Future Smart Manufacturing Environments. A Research Programme. *Procedia Manuf.* **2018**, *16*, 193–207. [CrossRef]
54. ENISA. *ENISA Threat Landscape for Supply Chain Attacks*; ENISA: Athens, Greece, 2021; ISBN 978-92-9204-509-8.
55. Wong, L.-W.; Lee, V.-H.; Tan, G.W.-H.; Ooi, K.-B.; Sohal, A. The Role of Cybersecurity and Policy Awareness in Shifting Employee Compliance Attitudes: Building Supply Chain Capabilities. *Int. J. Inf. Manag.* **2022**, *66*, 102520. [CrossRef]
56. Rahman, S.; Hossain, N.U.I.; Govindan, K.; Nur, F.; Bappy, M. Assessing Cyber Resilience of Additive Manufacturing Supply Chain Leveraging Data Fusion Technique: A Model to Generate Cyber Resilience Index of a Supply Chain. *CIRP J. Manuf. Sci. Technol.* **2021**, *35*, 911–928. [CrossRef]
57. Hua, J.; Chen, Y.; Luo, X. Are We Ready for Cyberterrorist Attacks?—Examining the Role of Individual Resilience. *Inf. Manag.* **2018**, *55*, 928–938. [CrossRef]
58. Sule, M.-J.; Zennaro, M.; Thomas, G. Cybersecurity through the Lens of Digital Identity and Data Protection: Issues and Trends. *Technol. Soc.* **2021**, *67*, 101734. [CrossRef]
59. Dupont, B. The Cyber-Resilience of Financial Institutions: Significance and Applicability. *J. Cybersecur.* **2019**, *5*, tyz013. [CrossRef]
60. Abraham, C.; Chatterjee, D.; Sims, R.R. Muddling through Cybersecurity: Insights from the U.S. Healthcare Industry. *Bus. Horiz.* **2019**, *62*, 539–548. [CrossRef]
61. Nwaiwu, F.; Mbelu, S. Digital Transformation in Healthcare and Surveillance Capitalism: Comparative Assessment of Data and Privacy Protection Compliance across the European Union. *SSRN J.* **2020**, 3. [CrossRef]
62. Markopoulou, D.; Papakonstantinou, V. The Regulatory Framework for the Protection of Critical Infrastructures against Cyberthreats: Identifying Shortcomings and Addressing Future Challenges: The Case of the Health Sector in Particular. *Comput. Law Secur. Rev.* **2021**, *41*, 105502. [CrossRef]
63. Carías, J.F.; Arrizabalaga, S.; Labaka, L.; Hernantes, J. Cyber Resilience Progression Model. *Appl. Sci.* **2020**, *10*, 7393. [CrossRef]
64. Tran, H.; Campos-Nanez, E.; Fomin, P.; Wasek, J. Cyber Resilience Recovery Model to Combat Zero-Day Malware Attacks. *Comput. Secur.* **2016**, *61*, 19–31. [CrossRef]
65. Vogel, E.; Dyka, Z.; Klann, D.; Langendörfer, P. Resilience in the Cyberworld: Definitions, Features and Models. *Future Internet* **2021**, *13*, 293. [CrossRef]
66. Alberts, C.; Wood, C.; Dorofee, A. *Introduction to the Security Engineering Risk Analysis (SERA) Framework*; Software Engineering Institute: Arlington, VA, USA, 2014.
67. Zhu, C.; Wu, J.; Liu, M.; Luan, J.; Li, T.; Hu, K. Cyber-Physical Resilience Modelling and Assessment of Urban Roadway System Interrupted by Rainfall. *Reliab. Eng. Syst. Saf.* **2020**, *204*, 107095. [CrossRef]
68. Zou, B.; Choobchian, P.; Rozenberg, J. Cyber Resilience of Autonomous Mobility Systems: Cyber-Attacks and Resilience-Enhancing Strategies. *J. Transp. Secur.* **2021**, *14*, 137–155. [CrossRef]
69. Bai, T.; Luo, J.; Zhao, J.; Wen, B.; Wang, Q. Recent Advances in Adversarial Training for Adversarial Robustness. In Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence Survey Track, Montreal, QC, Canada, 19–26 August 2021; pp. 4312–4321.
70. Athalye, A.; Carlini, N. On the Robustness of the CVPR 2018 White-Box Adversarial Example Defenses. *arXiv* **2018**. [CrossRef]
71. Zhao, W.; Alwidian, S.; Mahmoud, Q.H. Adversarial Training Methods for Deep Learning: A Systematic Review. *Algorithms* **2022**, *15*, 283. [CrossRef]
72. Zeng, L.; Qiu, D.; Sun, M. Resilience Enhancement of Multi-Agent Reinforcement Learning-Based Demand Response against Adversarial Attacks. *Appl. Energy* **2022**, *324*, 119688. [CrossRef]
73. Ghelani, D. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *Authorea* **2022**. [CrossRef]
74. Malatji, M.; Marnewick, A.L.; Von Solms, S. Cybersecurity Capabilities for Critical Infrastructure Resilience. *Inf. Comput. Secur.* **2022**, *30*, 255–279. [CrossRef]
75. Liang, X.; Konstantinou, C.; Shetty, S.; Bandara, E.; Sun, R. Decentralizing Cyber Physical Systems for Resilience: An Innovative Case Study from A Cybersecurity Perspective. *Comput. Secur.* **2023**, *124*, 102953. [CrossRef]
76. Xu, L.; Guo, Q.; Sheng, Y.; Muyeen, S.M.; Sun, H. On the Resilience of Modern Power Systems: A Comprehensive Review from the Cyber-Physical Perspective. *Renew. Sustain. Energy Rev.* **2021**, *152*, 111642. [CrossRef]
77. Fischer-Hübner, S.; Alcaraz, C.; Ferreira, A.; Fernandez-Gago, C.; Lopez, J.; Markatos, E.; Islami, L.; Akil, M. Stakeholder Perspectives and Requirements on Cybersecurity in Europe. *J. Inf. Secur. Appl.* **2021**, *61*, 102916. [CrossRef]
78. Garcia-Perez, A.; Cegarra-Navarro, J.G.; Sallos, M.P.; Martinez-Caro, E.; Chinnaswamy, A. Resilience in Healthcare Systems: Cyber Security and Digital Transformation. *Technovation* **2022**, *121*, 102583. [CrossRef]
79. Trim, P.R.J.; Lee, Y.-I. Managing Cybersecurity Threats and Increasing Organizational Resilience. *Big Data Cogn. Comput.* **2023**, *7*, 177. [CrossRef]