sustainability

MDPI

Article

Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework

Alessandro Annarelli and Giulia Palombi *

Department of Computer, Control and Management Engineering, Sapienza University of Rome, Via Ariosto 25, 00185 Rome, Italy; alessandro.annarelli@uniroma1.it
* Correspondence: giulia.palombi@uniroma1.it

Abstract: Digital transformation is currently an essential condition for companies to operate in most markets, since it provides a whole new set of competitive skills and strategic tools. On the other hand, the same digitalization puts companies in the face of a whole new series of threats coming from the cyber space. The foundation of business sustainability, which is the maintenance of competitiveness while securing business, is no longer a "plus" feature or a captivating sentence but a true and consistent need for all organizations. This article provides a literature analysis on approaches and models for cyber resilience, digitalization capabilities, and a conceptual framework showing how digitalization capabilities drive cyber resilience. Digitalization capabilities are involved in the plan/prepare phase and in the adaptation phase of the cyber resilience process. In particular, online informational capabilities can drive both these phases. Other capabilities such as the employment of heterogeneous resources and the promotion of continuous learning drive the plan/prepare phase, while the scanning of the evolution of the digital environment and a timely reconfiguration of resources drive the adaptation phase.

Keywords: digital transformation; digitization; cyber security; cyber resilience phases; dynamic capabilities

Citation: Annarelli, A.; Palombi, G. Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. *Sustainability* **2021**, *13*, 13065. https://doi.org/10.3390/su132313065

Academic Editors: Marc A. Rosen and Lucian-Ionel Cioca

Received: 21 July 2021
Accepted: 24 November 2021
Published: 25 November 2021

1. Introduction

The concept of survival and business sustainability has assumed an increasingly relevant role in recent years for organizations. The key is to design an organizational system aimed at enhancing so-called organizational resilience [1]. Currently, firms are required to face competition in the market while ensuring the sustainability of their operations from economic, environmental, and social points of view. Ensuring the sustainability of the environment and society can no longer be an option alongside business strategy and competitiveness (i.e., the sustainability of business).

The latest research developments show that one of the most promising answers to these pressing needs lies in the multifaceted possibilities offered by the digitalization of business [2]. Indeed, the growing level of digitalization is dramatically impacting the strategy and operations of today's organizations. It is evident how, in many sectors, digital interaction with customers is allowing organizations to provide a richer user experience [3].

Nevertheless, the complexity of the digitalized cyber environment causes cyber attacks to increase in frequency. Digitalization creates many opportunities but also a more complex cyber space, therefore making companies more exposed to cyber threats [4]. Hence, so-called cyber resilience, i.e., the ability of an organization to plan and prepare for, respond to, recover from, and adapt to a cyber attack, is growing in importance.

Cyber security management has become vital for organizations. Investments in cyber security and digitalization generate numerous advantages, but there is a tradeoff between the benefit deriving from these investments and their economic sustainability for companies [5]. In particular, small and medium-sized enterprises must consider how much and how to invest in these areas, considering their limited resources [6].

Digitalization capabilities are those organization capabilities that allow seizing numerous opportunities by combining digital assets and business resources, and by leveraging digital networks, to innovate products, services, and processes. These capabilities are considered important drivers of sustained competitive advantage through organizational learning, customer value creation, and innovation management [7].

To the best of our knowledge, there are very few contributions to the emerging topic of digitalization capabilities and their relationship with cyber resilience. This paper analyzes how digitalization capabilities drive cyber resilience. It provides a literature analysis on approaches and models for cyber resilience, digitalization capabilities, and the interactions between them. Finally, recent contributions on cyber resilience management [8] and digitalization capabilities [7] allowed us to formulate a conceptual framework. The framework clarifies the specific digitalization capabilities that concur to drive cyber resilience and in which phases.

This paper is structured as follows: the first section contains the introduction, the Section 2 summarizes approaches and models for cyber resilience, the Section 3 presents the research methodology, the Section 4 summarizes the literature on digitalization capabilities, the Section 5 contains the conceptual framework, and the sixth and last section contains the discussion and conclusions.

2. Approaches and Models for Cyber Resilience

In recent years, numerous studies have been proposed to guide organizations in being cyber resilient. The Cyber Resiliency Engineering Framework, proposed by [9] in the MITRE technical report, provides cyber resiliency goals, objectives, and practices. The cyber resiliency goals relate to adverse events and are Anticipate, Withstand, Recover, and Evolve. The last goal consists in changing missions/business functions and/or supporting cyber capabilities to minimize adverse impacts from actual or predicted adversary attacks.

A model for strategic and tactical resiliency against threats to ubiquitous systems (STRATUS) was developed by [10]. This model adopts an ontological point of view that takes into account different elements, which include, for instance, vulnerability and reliability levels for hardware and software resources and the role of physical and/or network proximity in determining levels of vulnerability.

Linkov et al. [11] designed a resilient matrix framework based on a four-stage life cycle model, divided into Plan/Prepare, Absorb, Recover, and Adapt phases. These phases are jointly considered in the matrix with the four domains of the Network-Centric Operations doctrine, which are: physical, information, cognitive, and social [12]. From the intersection of phases and domains, resilience metrics were derived and further considered into a second study authored by [13], who integrated and better detailed these metrics with quantitative and qualitative measures emerging from the literature.

Further, cyber resilience models have begun to increasingly take into account the dynamic nature of cyber threats, highlighting the relevance of preparation and recovery phases, for what concerns known and unknown threats as well. The framework developed by [14] goes exactly in this direction, showing how risk-based standards can move beyond risk assessment to create systems that are more resilient to dynamic threats. In this context, the ability of an organization to understand the surrounding environment and learn/absorb knowledge from it becomes an essential element of cyber resilience, with the aim of building specific capabilities to exploit opportunities and manage threats more effectively [15]. Therefore, it is becoming essential to build cyber resilience with the characteristics of dynamic capabilities in mind, fostering both a reactive and a proactive capacity.

Jensen et al. [16] outlines actions to undertake to realize cyber resilience for the efficient functioning of the maritime industry: informational campaigns directed at companies showing the cyber risks they face; pressure from customers who are made increasingly aware of the risk they face in cases the companies lack cyber defenses; and, finally, "cyber premiums" on insurance policies that reflect the degree to which companies adhere to voluntary guidelines.

Di Mase et al. [17], in their cyber physical systems security framework (CPSS), suggest ten areas that enable a complete analysis concerning the "health status" of cyber security systems. These areas include data and information security (to ensure information sharing and reporting), as well as physical security and control of physical accesses, anticounterfeit measures, forensics and prognostics analyses, and recovery plans. Similarly, the model detailed by [18] takes into account the quality and integrity of data, the need for physical and virtual control, and the importance of ensuring continuity through security and safety.

Objective, intention, approach, architecture, and scope are the five aspects of cyber resilience identified by [19]. According to them, the *objective* consists in ensuring business delivery, so they recommend keeping business goals intact, rather than IT systems, during adverse cyber events. The *intention* should be "safe-to-fail", meaning that resilient systems should be designed to be able to fail in a controlled way, rather than being designed to solely protect against failure. The *approach* should "build security from within", which means that resilience should be incorporated into organizations and IT systems, rather than added as separate functions or teams. The *architecture* should contain multilayered protection, meaning that a resilient architecture contains several layers, each capable of protection and recovery, rather than having a single layer of protection. Finally, the *scope* should be holistic and consider the entire network of organizations.

The Cyber Resilience Recovery Model (CRRM) was developed by [20] with the aim of contrasting zero-day malware attacks. To do so, the authors provide insights into the strengths and weaknesses of current recovery processes while presenting cyber security solutions that rely on, for instance, awareness training and isolation of "infected" machines.

Annarelli et al. [8], conducting a multiple case study analysis, proposes the managerial *cyber resilience framework* and the *context-based managerial cyber resilience framework.* The frameworks guide organizations in the implementation of the right managerial actions and investment to implement to enhance cyber resilience. According to the literature review on cyber resilience conducted by [21], the most important category is pre-event knowledge management, followed by security, velocity, ability, and adapt.

Annarelli et al. [22], through a qualitative study on the managerial practices for cyber resilience, shed light on the effectiveness and the way practices are implemented in the Italian context.

An ambidextrous approach to cyber security has been outlined by [23], adopting a balanced scorecard, multistage approach under a 7Ps stage-gate model (Patient, Persistent, Persevering, Proactive, Predictive, Preventive, and Preemptive) to enhance cyber resilience.

According to [24], measuring cyber resilience is in its infancy. Decisions on converting knowledge and intuition regarding the recovery and adaptation of cyber systems in response to threats into management decisions and policy will rely on a growing volume of increasingly diverse measurements.

A recent contribution is that of [25], who discuss the extent to which cyber physical systems contribute to the resilience of sociotechnical systems.

As clearly emerges from the analysis of cyber security literature, there is a lack of contributions investigating and highlighting the relationship between cyber resilience and digitalization capabilities. Nevertheless, elements and characteristics of digitalization capabilities can be retrieved in the above-cited contributions. Therefore, we performed a literature analysis, focusing on the stream of research of digitalization capabilities, to better understand if there is any evidence in academic production supporting this relationship.

3. Research Procedure

To investigate the relationship between digitalization capabilities and cyber resilience, we conducted a literature analysis.

We considered the digitalization capabilities reviewed by [7] and also included new pertinent contributions by replicating the search using the following search-string on Scopus: "(capabilit* OR abilit* OR capacit* OR process* OR routine*) AND (organization* OR firm* OR compan* OR enterprise*" and "digital*)". To conduct the search, we opted

for the Scopus online database because, compared to other sources, and as evidenced by [26], it is particularly good for works published after 1995, and it has a wide range of subjects and journals. For the definition of inclusion/exclusion criteria, we followed the recommendations and criteria already adopted by [7].

Among the digitalization capabilities identified (and summarized in Section 4), we considered those having a relationship with cyber resilience, then organized logically their interplay in a conceptual framework presented in Section 5.

4. Digitalization Capabilities

Companies need to develop capabilities oriented at managing digital ecosystem partnerships by the integration of their physical, financial, and information flows with their supply chain partners [27]; they also need to develop digital innovation capabilities for the process of searching for and redeeming capabilities in digital ecosystems [28].

Firms should also seize their own digitalization capabilities, considering the deployment of IT as drivers of digital competitiveness [29]. Rather than studying in detail their nature, other contributions studied how digitalization capabilities should be embraced by the employment of heterogeneous resources that enable digital solutions, looking at different stages of business processes [28,30].

Digitalization capabilities are of significant importance in information exchange and also digitalization capabilities to automate tasks [31,32]. It is important to reconfigure firms' digital resources and routines. The timely reconfiguration of resources appears to be a key capability, especially for what concerns securing digital innovation efforts.

Wheeler [33], moving from the concept of digital integration capabilities, conceptualized the dynamic capability of net enablement, which in turn allows processing and managing multiple and concurrent innovations at a given point in time. This is closely related to the work of [3], who formalized the importance of the scanning evolution of the digital environment in seeking opportunities for digital innovation. This is a key aspect, particularly for its link with improvisational capabilities, discussed in the same paper. According to the authors, "the malleability of digital technologies affords a higher degree of improvisation than their analog counterparts" (p. 65). The same topic and its relevance were studied more in detail by [34,35]. Improvisational capabilities can be defined as "the ability to spontaneously reconfigure existing resources to build new operational capabilities to address urgent, unpredictable, and novel environmental situations" [34]. Similarly, Ref [36] stressed the importance of adaptive capabilities in the context of digital marketing.

Finally, Ref [37] provided guidance on digital technology adoption in practice, helping scholars and managers to understand the potential impact of digital technologies on supply chains.

Among the digitalization capabilities reviewed by [7], those involved in the cyber resilience process considering the above-mentioned contributions are:

- Employing heterogeneous resources [30];
- Improvisational capabilities [34,35];
- Online informational capabilities [27,38];
- Promoting continuous learning [3];
- Scanning evolution of digital environment [3];
- Timely reconfiguration of resources [33].

These digitalization capabilities have been included in the conceptual framework described in detail in the next section.

5. Digitalization Capabilities and Cyber Resilience

According to [15], the combined use of dynamic capabilities, which include ordinary-defensive, dynamic-resilience, and extraordinary capabilities, leads to increasing levels of maturity in the area of computer (cyber) resilience. Recently, [23] recalled these aspects by highlighting the need for an adaptive process of dynamic intangible organizational assets, resources, and capabilities across a performance frontier to enhance cyber resilience.

To contribute theoretically and practically in this research direction, we want to analytically show that each digitalization capability drives cyber resilience consequences.

Considering the identified digitalization capabilities [7,30,34,38] and the cyber resilience phases by [11] lately organized in managerial practices in the managerial cyber resilience framework proposed by [8], we found an interesting common ground between digitalization capabilities and cyber resilience practices.

Among all the approaches and models for cyber resilience summarized in Section 2, we chose the managerial cyber resilience framework for its focus on managerial practices. Moreover, it recalls concepts, such as planning and preparing through competencies, adaptation to the context, and learning by the experience, typical of digitalization capabilities.

In Table 1, each digitalization capability is presented with its definition, together with the cyber resilience phase and practice it belongs to.

Table 1. Digitalization capabilities driving cyber resilience.

Digitalization Capabilities		Cyber Resilience Practice	Cyber Resilience Phase
Employing heterogeneous resources	Employing heterogeneous distributed resources to use digital solutions to different extents and in different stages of the business processes. There can be a distinction between digital capabilities to exchange and process information and digital capabilities to automate tasks [30]	Prevention; Training	Plan/Prepare
Improvisational capabilities	Ability to spontaneously reconfigure existing resources to build new operational capabilities to address urgent, unpredictable, and novel environmental situations, through IT-enabled capability, i.e., the effective use of digital IT systems [34]	Update	Adapt
	Capabilities that enable spontaneous change, are best suited for extremely turbulent environments, characterized by sudden changes in demand and unexpected technological breakthroughs [35]		
Online informational capabilities	The ability of a firm to exchange strategic and tactical information through the integration of IT resources and processes [27,38]	Prevention; Review	Plan/Prepare; Adapt
Promoting continuous learning	Firms should promote continuous learning of the unique properties of digital technologies, by acquiring new skills both internally and externally while establishing new digital roles [3]	Training	Plan/Prepare
Scanning evolution of digital environment	To identify opportunities, firms need to scan their digital environment to foresee and understand key changes [3]	Context	Adapt
Timely reconfiguration of resources	Net enablement capability as a dynamic capability to turn timely the business innovations enabled by digital networks into customer value [33]	Context	Adapt

Employing heterogeneous resources means employing heterogeneous distributed resources to use digital solutions to different extents and in different stages of business processes [32,39]. For instance, the digital capabilities needed to exchange and process information and those used to automate tasks can be very different [30]. The plan/prepare phase, and in particular the prevention and training category, best matches this capability. In fact, investments in heterogeneous human resources and activities of recruiting and retention are essential, and it has been highlighted that a key security challenge for organizations is the lack of communication, collaboration, and sharing between IT teams and teams belonging to other functions [40].

Improvisational capabilities, i.e., the ability to spontaneously reconfigure existing resources to build new operational capabilities to address urgent, unpredictable, and novel environmental situations [34], suited for extremely turbulent environments [35], is included in the phase called Adapt. In this case, the adaptation relates to the Update practice since, even if automatically, it implies the reconfiguration/updating of the digital environment and related cyber security actions.

The literature shows that improvisation is inevitable during crises. In some cases, employees will not have built up a routine for the situation before them, or their routine simply does not work [41].

Online informational capabilities, which, according to [38], consists in the ability of a firm to exchange strategic and tactical information through the integration of IT resources and processes, can contribute to the practices called Prevention and Review, respectively, included in the Plan/Prepare and Adapt phases. In fact, it is essential to organize data protection for instance by the use of cryptography and to review the effectiveness of the secure transferring of knowledge, especially if it is tacit, nonproprietary, and technological [42].

The digitalization capability named Scanning evolution of digital environment, which, according to [3], consists in the ability to identify opportunities, since firms need to scan their digital environment to foresee and understand key changes, is significantly important in the Adapt phase and in particular in the adaptation to the Context. The digital environment can imply new competitive opportunities but also new threats and vulnerabilities. It is therefore essential to evaluate this tradeoff between smartness and resilience and smartness and economic sustainability, since the same investments and level of digitalization can be sustainable and reasonable for a particular organization but not for another [43].

Timely reconfiguration of resources, i.e., the net enablement capability as a dynamic capability to timely transform the business innovations enabled by digital networks into customer value [33], similarly to the previous phase, consists in the Adapt phase and in particular the adaptation to the Context. Being aware of the cyber security consequences of this enablement is vital. The key is building cyber security into the business value chain and enabling new technological operating platforms that combine many innovations [4].

As emerges from the definitions provided in Table 1, digitalization capabilities are not totally mutually exclusive or totally mutually inclusive and present similar traits, e.g., improvisational capabilities with employing heterogeneous resources and/or online informational capabilities. This suggests the existence of potential synergies among the simultaneous adoption and development of more capabilities at once.

In Figure 1, the digitalization capabilities driving the Cyber Resilience Framework are provided.

In this framework, digitalization capabilities are reported according to the phase in which we recognized they are involved according to the literature.

In fact, employing heterogeneous resources and promoting continuous learning have been recognized as drivers in the Plan/Prepare phase, online informational capabilities has been associated with both the Plan/Prepare and Adapt phases, while scanning the evolution of digital environment and timely reconfiguration of resources relate to the Adapt phase.

The practices recognized are also specified in correspondence with each capability: from the practice of prevention and training in which the employing of heterogeneous

resources plays a crucial role, to that of the adaptations to the context for which the timely reconfiguration of resources is essential.

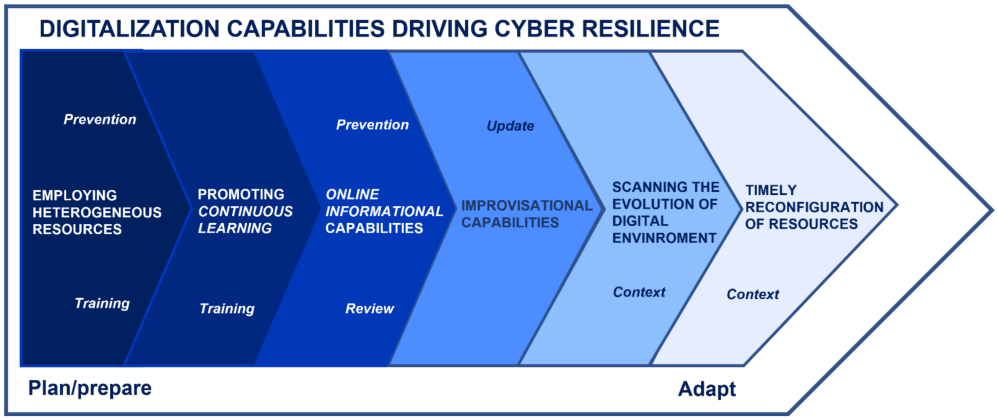

Figure 1. Digitalization capabilities driving the Cyber Resilience Framework.

6. Discussion and Conclusions

According to what was reported in the previous section, we conceptualize the following insights:

- Employing heterogeneous resources is a driver of prevention and training practices that belongs to the plan/prepare phase of the managerial cyber resilience process.
- Promoting continuous learning is a driver of the practice of training, belonging to the plan/prepare phase of the managerial cyber resilience process.
- Online informational capabilities are drivers of prevention and review practices, respectively belonging to the Plan/Prepare and Adapt phases of the managerial cyber resilience process.
- Improvisational capabilities are drivers of the Update practice, which belongs to the Adapt phase of the managerial cyber resilience process.
- Scanning the evolution of the digital environment and Timely reconfiguration of resources are drivers of the adaptation to the context that belongs to the Adapt phase of the managerial cyber resilience process.

These insights might be confirmed empirically through future studies of quantitative and qualitative nature.

Moreover, we can state that the study of digitalization capabilities should not be limited to competitiveness and strategic insights but rather encompass a much larger perspective to fully understand their potential. As a matter of fact, digitalization capabilities inherit several characteristics from organizational and dynamic capabilities, considering that they allow sensing and seizing opportunities and threats while allowing a reconfiguration of resources and routines in the context of digital transformation [7,44]. On the other hand, the vast universe of digitalization is causing companies to constantly face more serious threats in the cyber world, hence the importance, in the last years, of the concept of cyber resilience. Maintaining competitiveness while at the same time ensuring safety and security is no longer an option, a feature for highly competitive markets, nor a "catchphrase". Through this work, our aim was to show that there is a strong link between these needs and that digitalization capabilities might be the answer for both scholars and practitioners. Maintaining a set of heterogeneous and diversified resources, while being able to reconfigure the allocation of said resources when needed, can be both a key strategic and a resilient move. What might change is the purpose and way of employment, but the maintenance and timely exploitation of these resources rely on the same set of capabilities, therefore being an invariant. The same thinking can be replicated for improvisational capabilities, the promotion of continuous learning, and all the other capabilities detailed in the previous sections, which can foster cyber resilience and business strategies at the

same time. Furthermore, this study only considered this benefit as acting in one way, but a deeper study of cyber resilience practices might uncover a new set of digitalization capabilities as well. There is a clear and strong need for practitioners and researchers to focus more on the multibeneficial relationship between digitalization capabilities and cyber resilience, since this might represent a key turning point in mastering once and for all the digital transformation of business.

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

Funding: This work is supported by the fund "Progetto di Eccellenza" of the Department of Computer, Control and Management Engineering "Antonio Ruberti" of Sapienza University of Rome. The department has been designated by the Italian Ministry of Education (MIUR) for being a "Department of Excellence" in advanced training programs in the field of cyber security.

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

References

1. Annarelli, A.; Battistella, C.; Nonino, F. A framework to evaluate the effects of organizational resilience on service quality. *Sustainability* **2020**, *12*, 958. [CrossRef]
2. Vial, G. Understanding digital transformation: A review and a research agenda. *J. Strateg. Inf. Syst.* **2019**, *28*, 118–144. [CrossRef]
3. Nylén, D.; Holmström, J. Digital innovation strategy: A framework for diagnosing and improving digital product and service innovation. *Bus. Horiz.* **2015**, *58*, 57–67. [CrossRef]
4. Kaplan, J.; Ritcher, W.; Ware, D. Cybersecurity: Linchpin of the Digital Enterprise | McKinsey. McKinsey Co., no. July. 2019. Available online: https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-linchpin-of-the-digital-enterprise# (accessed on 1 July 2021).
5. Khan, O.; Estay, D.A.S. Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. *Technol. Innov. Manag. Rev.* **2015**, *5*, 6–12. [CrossRef]
6. Armenia, S.; Angelini, M.; Nonino, F.; Palombi, G.; Schlitzer, M.F. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decis. Support Syst.* **2021**, *147*, 113580. [CrossRef]
7. Annarelli, A.; Battistella, C.; Nonino, F.; Parida, V.; Pessot, E. Literature review on digitalization capabilities: Co-citation analysis of antecedents, conceptualization and consequences. *Technol. Forecast. Soc. Chang.* **2021**, *166*, 120635. [CrossRef]
8. Annarelli, A.; Nonino, F.; Palombi, G. Understanding the management of cyber resilient systems. *Comput. Ind. Eng.* **2020**, *149*, 106829. [CrossRef]
9. Bodeau, D.; Graubart, R.; Picciotto, J.; McQuaid, R. Cyber Resiliency Engineering Framework. 2011. Available online: http://www.mitre.org/work/tech_papers/2012/11_4436/%5Cnpapers2://publication/uuid/F03D9287-780F-4B61-AC47-E77BEDC3F939 (accessed on 1 July 2021).
10. BBurstein, M.; Goldman, R.; Robertson, P.; Laddaga, R.; Balzer, R.; Goldman, N.; Geib, C.; Kuter, U.; Mcdonald, D.; Maraist, J.; et al. STRATUS: Strategic and tactical resiliency against threats to ubiquitous systems. In Proceedings of the 2012 IEEE Sixth International Conference on Self-Adaptive and Self-Organizing Systems Workshops, Lyon, France, 10–14 September 2012; pp. 47–54. [CrossRef]
11. Linkov, I.; Eisenberg, D.A.; Bates, M.E.; Chang, D.; Convertino, M.; Allen, J.H.; Flynn, S.E.; Seager, T.P. Measurable resilience for actionable policy. *Environ. Sci. Technol.* **2013**, *47*, 10108–10110. [CrossRef] [PubMed]
12. Alberts, D.S.; Hayes, R.E. *Power to the Edge: Command . . . Control . . . in the Information Age*; Office of the Assistant Secretary of Defense Washington DC Command and Control Research Program (CCRP): Washington, DC, USA, 2003.
13. Linkov, I.; Eisenberg, D.A.; Plourde, K.; Seager, T.P.; Allen, J.; Kott, A. Resilience metrics for cyber systems. *Environ. Syst. Decis.* **2013**, *33*, 471–476. [CrossRef]
14. Collier, Z.A.; Dimase, D.; Walters, S.; Tehranipoor, M.M.; Lambert, J.H.; Linkov, I. Cybersecurity standards: Managing risk and creating resilience. *Computer (Long. Beach. Calif.)* **2014**, *47*, 70–76. [CrossRef]
15. Ferdinand, J. Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. *J. Bus. Contin. Emerg. Plan.* **2015**, *9*, 185–195.
16. Jensen, L. Challenges in Maritime Cyber-Resilience. *Technol. Innov. Manag. Rev.* **2015**, *5*, 35–39. [CrossRef]
17. Di Mase, D.; Collier, Z.A.; Heffner, K.; Linkov, I. Systems engineering framework for cyber physical security and resilience. *Environ. Syst. Decis.* **2015**, *35*, 291–300. [CrossRef]
18. Boyes, H. Cybersecurity and Cyber-Resilient Supply Chains. *Technol. Innov. Manag. Rev.* **2015**, *5*, 28–34. [CrossRef]

19. Björck, F.; Henkel, M.; Stirna, J.; Zdravkovic, J. Cyber Resilience—Fundamentals for a Definition. In *Advances in Intelligent Systems and Computing*; Springer: New York, NY, USA, 2015; Volume 353, pp. 311–316.
20. 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]
21. Estay, D.A.S.; Sahay, R.; Barfod, M.B.; Jensen, C.D. A systematic review of cyber-resilience assessment frameworks. *Comput. Secur.* **2020**, *97*, 101996. [CrossRef]
22. Annarelli, A.; Clemente, S.; Nonino, F.; Palombi, G. *Effectiveness and Adoption of NIST Managerial Practices for Cyber Resilience in Italy*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 818–832.
23. Carayannis, E.G.; Grigoroudis, E.; Rehman, S.S.; Samarakoon, N. Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience. *IEEE Trans. Eng. Manag.* **2021**, *68*, 223–234. [CrossRef]
24. Kott, A.; Linkov, I. To improve cyber resilience, measure it. *IEEE Comp.* **2021**, *54*, 80–85. [CrossRef]
25. 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]
26. Tukker, A. Product services for a resource-efficient and circular economy—A review. *J. Clean. Prod.* **2015**, *97*, 76–91. [CrossRef]
27. Rai, A.; Patnayakuni, R.; Seth, N. This content downloaded from 216.227.221.251 on Tue. *Manag. MIS Q.* **2006**, *30*, 226–246.
28. Selander, L.; Henfridsson, O.; Svahn, F. Capability search and redeem across digital ecosystems. *J. Inf. Technol.* **2013**, *28*, 183–197. [CrossRef]
29. McAfee, A.; Brynjolfsson, E. Investing in the IT That Makes a Competitive Difference. *Harv. Bus. Rev.* **2008**, *86*, 98–107.
30. Mishra, A.N.; Konana, P.; Barua, A. Antecedents and consequences of Internet use in procurement: An empirical investigation of U.S. manufacturing firms. *Inf. Syst. Res.* **2007**, *18*, 103–120. [CrossRef]
31. Drnevich, P.L.; Croson, D.C. Information T Echnology and B Usiness -L Evel S Trategy: T Oward an I Ntegrated T Heoretical P Erspective 1. *MIS Q.* **2013**, *37*, 483–509. [CrossRef]
32. Tripsas, M.; Gavetti, G. Capabilities, Cognition, and Inertia: Evidence from Digital Imaging. *Strateg. Manag. J.* **2000**, *21*, 1147–1161. [CrossRef]
33. Wheeler, B.C. NEBIC: A dynamic capabilities theory for assessing net-enablement. *Inf. Syst. Res.* **2002**, *13*, 125–146. [CrossRef]
34. Pavlou, P.A.; Sawy, O.A.E. The 'third hand': IT-enabled competitive advantage in turbulence through improvisational capabilities. *Inf. Syst. Res.* **2010**, *21*, 443–471. [CrossRef]
35. El Sawy, O.A.; Malhotra, A.; Park, Y.K.; Pavlou, P.A. Seeking the configurations of digital ecodynamics: It takes three to tango. *Inf. Syst. Res.* **2010**, *21*, 835–848. [CrossRef]
36. Kannan, P.K. Digital marketing: A framework, review and research agenda. *Int. J. Res. Mark.* **2017**, *34*, 22–45. [CrossRef]
37. Yang, M.; Fu, M.; Zhang, Z. The adoption of digital technologies in supply chains: Drivers, process and impact. *Technol. Forecast. Soc. Chang.* **2021**, *169*, 120795. [CrossRef]
38. Barua, A.; Konana, P.; Whinston, A.B.; Yin, F. An empirical investigation of net-enabled business value. *MIS Q.* **2004**, *28*, 585–620. [CrossRef]
39. Sambamurthy, V.; Bharadwaj, A.; Grover, V. Shaping Agility through Digital Options: Reconceptualizing the Role of Information. *MIS Q.* **2003**, *27*, 237–263. [CrossRef]
40. Tøndel, I.A.; Line, M.B.; Jaatun, M.G. Information security incident management: Current practice as reported in the literature. *Comput. Secur.* **2014**, *45*, 42–57. [CrossRef]
41. Mendonça, D.; Wallace, W.A. Studying Organizationally-situated Improvisation in Response to Extreme Events. *Int. J. Mass Emerg. Disasters* **2004**, *22*, 5–29.
42. Kachra, A.; White, R.E. Know-how transfer: The role of social, economic/ competitive, and firm boundary factors. *Strateg. Manag. J.* **2008**, *29*, 425–445. [CrossRef]
43. Ganin, A.A.; Quach, P.; Panwar, M.; Collier, Z.A.; Keisler, J.M.; Marchese, D.; Linkov, I. Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Anal.* **2020**, *40*, 183–199. [CrossRef]
44. Teece, D. Explicating Dynamic Capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strateg. Manag. J.* **2007**, *28*, 1319–1350. [CrossRef]