This paper was presented at The XXXIII ISPIM Innovation Conference "Innovating in a Digital World", held in Copenhagen, Denmark on 05 June to 08 June 2022.
Event Proceedings: LUT Scientific and Expertise Publications: ISBN 978-952-335-694-8

How digitalization capabilities support cyber resilience

Alessandro Annarelli

Sapienza University of Rome, Department of Computer, Control and Management Engineering, Via Ariosto 25, Roma, 00185, Italy
Email: alessandro.annarelli@uniroma1.it

Fabio Nonino

Sapienza University of Rome, Department of Computer, Control and Management Engineering, Via Ariosto 25, Roma, 00185, Italy
Email: alessandro.annarelli@uniroma1.it

Giulia Palombi*

Sapienza University of Rome, Department of Computer, Control and Management Engineering, Via Ariosto 25, Roma, 00185, Italy
Email: giulia.palombi@uniroma1.it

* Corresponding author

Abstract:

In the last decades, digitization and innovation have led to structural changes in the way organizations operate, generating new procedures, approaches, and new capabilities. The so-called digitalization capabilities, considered a source of competitiveness, are spreading.
However, cyber security and how these changes are leading to new risks and vulnerabilities should not be underestimated in the digital transformation. Therefore, the ability of organizations to adapt to change, to react to cyber attacks and to exploit them to become more robust recalls the concept of resilience, or rather, of cyber resilience.
This study combines digitalization capabilities with cyber resilience by extending the use of these capabilities within cyber security: resilience and competitiveness can no longer be considered separately. To demonstrate the existence of a possible contribution from digitalization capabilities for cyber resilience, an empirical investigation of a case study active in highly innovative and technological sectors was conducted: aerospace and security.
The results provide interesting actions to be taken, exploiting the digitalization capabilities to obtain resilient cyber systems.

Keywords: Digital Transformation, Cybersecurity, Organizational resilience, Case study analysis.

This paper was presented at The XXXIII ISPIM Innovation Conference "Innovating in a Digital World", held in Copenhagen, Denmark on 05 June to 08 June 2022.
Event Proceedings: LUT Scientific and Expertise Publications: ISBN 978-952-335-694-8

1 Introduction

Digitalization is transforming organizations by advancing knowledge and creating new value for customers. It includes Smart Manufacturing, Industrial Internet of Things, Digital Factory, and Industry 4.0 phenomena and is transforming organizations by introducing new skills and capabilities that generate new value for customers, new market opportunities and new revenue opportunities for companies.
The set of capabilities that allow to combine digital and non-digital resources, to exploit digital to innovate products/services and processes creating new value for the customer and guaranteeing a competitive advantage for companies, have been described as digitalization capabilities (Annarelli *et al*., 2020).
However, with the growing adoption of emerging technologies, digital transformation significantly increases risks of vulnerability which expose organizations to cyber-attacks (Carayannis *et al*., 2019).
Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events (Björck *et al.*, 2015).
Organizations that lack cyber defense and do not engage in any organizational learning about cyber attack and defense, in fact, could be considered to lack cyber resilience (Ferdinand, 2015).
The aim of this study, therefore, is to demonstrate the possibility of receiving a contribution from digitalization capabilities for organizational cyber resilience.
For these purposes, we conducted a case study analysis in a big organization operating in a highly innovative and technological sector.
In this way, the paper proposes new ways of using and exploiting these capabilities in an area they have not explored, such as cybersecurity.
Furthermore, digitalization capabilities can be seen as the junction point between competitiveness and resilience: as a fundamental resource for exploiting technological opportunities and strengthening cybersecurity and cyber resilience (Annarelli and Palombi, 2021).
The present work is divided into the following sections. Section 2 reports the theoretical background, section 3 describes the research methodology, section 4 contains the obtained results exposing the most relevant elements of the research carried out.
The final considerations are reported in the conclusions with the recognition of the limitations of the research and the indications for future research.

Theoretical background

Digitalization and digitalization capabilities

Companies need dynamic tools to support the management of the new digital innovation processes that emerge.
So, one of the challenges that businesses face is having to balance existing capabilities and build new digital capabilities that major processes address the tensions associated with integration. Indeed, it is argued that companies can learn to manage radical and incremental innovation, building ambidextrous structures (Carayannis, et al., 2019;, Nylén & Holmström, 2015): companies are called to constantly keep updated on how new digital technologies relate to their processes and define new opportunities.

Given the disruptive nature of digitalization, Warner & Wäger, (2019), speculate that the dynamic capabilities are powerful tools for examining the digital transformation of companies. Unlike operational organizational skills, dynamic skills allow you to govern and manage the rate of change in the environment. In fact, they are based on innovation and are essential in responding to technological changes, integrating e-business and offering a better connection with customers and suppliers in order to create and extend the set of resources of a company.
In this regard, dynamic abilities are theorized at different levels. The first order deals with extending, modifying, changing and / or creating ordinary capabilities. In their absence, a company may need to adopt a completely new approach to develop second-order (or higher-order) dynamic capabilities that allow for a spontaneous response in new situations (Karimi & Walter, 2015).
However, the study of digitalization capabilities should not be limited to competitiveness and strategic insights, but rather embrace a much broader perspective to fully understand their potential, as they allow us to perceive and seize opportunities and threats, allowing a reconfiguration of resources and routines in the context of digital transformation. More specifically, three dimensions of analysis can be considered: scanning of digital evolution, continuous learning and improvisation (Nylén & Holmström, 2015).

Cyber resilience

The concept of cybersecurity is bringing a renewed attention to organizational resilience (and hence, cyber resilience or IT resilience), assuming a particular relevance in many industrial contexts where competitiveness and resilience are nowadays built upon the same means. The need to manage cybersecurity risks and, hence, plan for effective and sustainable investments has been largely debated (Khan and Estay, 2015; Armenia et al., 2021) by studies focused on cyber (risk and resilience) frameworks (Collier et al., 2013; Linvok et al. 2013; Jensen et al., 2015; Annarelli et al., 2020) and on the budget allocation for cyber risk mitigation (Katzumata et al.,2010; Chen et al., 2011; Bojanc and Jerman Blasic, 2013; Paté-Cornell et al., 2018). For instance, four general phases of cyber resilience can be considered: plan/prepare, absorb, recover and adapt (Linkov et al., 2013), but there is still need for further research on identification of new phases/processes, their contextualization in different industrial environments and their effective implementation.

Research gap and research question

Cyber resilience in organizations can be reached exploiting opportunities given by the combined use of different dynamic capabilities leading to increasing levels of maturity in this area (Ferdinand, 2015) and by a complex process of dynamic intangible organizational assets and resources (Carayannis et al., 2021). Furthermore, given their potential to foster key characteristics like preparedness and agility (Barua et al., 2004; Nylen and Holmstrom, 2015), digitalization capabilities can be seen as the conjunction point between, and the enablers of, competitiveness and resilience.
Hence, we investigated this issue by answering the following research question:

- "How can digitalization capabilities support cyber resilience?"

In order to answer this question, we realized a case study analysis hich is described in detail in the following sections.

3 Methodology

The case study methodology is particularly suitable for empirical research since it allows the identification of crucial variables during the analysis of a phenomenon. Case studies are designed to guarantee methodological rigor and high quality of investigation, trying to identify the reason why a certain decision was taken, how it was resolved and what the consequences were (Schramm, 1971).
In particular, this research used a multi-source analysis scheme relating to a single case study: a large Italian company active in a highly technological and innovative sector, such as aerospace and defence. The selection of the case under analysis took place following a sampling strategy with predefined criteria (sampling criteria) in order to maximize the possibility of receiving a contribution with a high degree of information and coherence with the research.
The company taken into consideration operates in the aerospace and defence sector, articulated through different business divisions that are thought about the nature of the product they offer. Specifically, the majority of the respondents who were contacted belong to the division dealing with digitization and cybersecurity.
A large part of the company is oriented to the defence sector, another part is aimed at the law enforcement sector and the public administration, as well as private companies.
In order to avoid the single respondent bias and maximize the validity and reliability, it was decided to involve multiple respondents: to avoid obtaining results distorted from reality and to avoid considering the point view of a single respondent as the view of the whole company, different perspectives were considered.
Given this objective, the study involved six key informants who hold high-level managerial roles, in order to have an all-encompassing and heterogeneous vision on the organization regarding the topic under analysis. In this way it was possible to study different realities and points of view within the same working context. Table 1 presents the respondents involved and their organizational role.

Table 1 – Key informants involved in the case study

Respondent	***Organizational Role***
Key Informant 1	Head of Line of Business
Key Informant 2	Head of Digital Solutions
Key Informant 3	Head of Engineering Offering
Key Informant 4	Head of Cyber Resilient Products
Key Informant 5	Line of Business Manager
Key Informant 6	Head of Cyber Security

The overall data collection process took about three months. The questionnaire was broken down into two semi-structured interviews of approximately one hour each, which relatively provide a contribution to the literature, conceptualizing and defining digitalization capabilities, and a description of the cyber context in which the case study organization operates. Specifically, the first part of the interview protocol focused on verifying the presence of digitalization capabilities within the organization, based on the breakdown of these capabilities into their main dimensions. The following part focused on the key elements of corporate IT security management with the aim of knowing the cyber context in which the case study operates.

Framework of analysis

The first part of the interview aims to understand whether the interviewed company exhibits digitalization capabilities, and to which extent. These capabilities have been decomposed into a subset of key dimensions necessary both to verify their presence within the organization and to understand if they can operate in support of cybersecurity.
In the case under analysis, therefore, the digitalization capabilities have been broken down into two main sections: *higher-order capabilities* and *first-order capabilities*. The first dimension makes it possible to consider digitalization capabilities as a high-level capability, similar to dynamic capabilities (Wang & Ahmed, 2007) that allows to obtain a lasting competitive advantage and to increase the ability to cope with changes in a digital environment. The second dimension, on the other hand, considers the digital integration capabilities as the micro-foundation of digitalization capabilities (Annarelli, et al., 2021): it consists of the ability to integrate data and processes and ability to integrate channels enabled for digitalization.
The second part of the research framework aimed at understanding and characterizing the cyber resilience context in which the case study company operates. We derived five main dimensions from literature, further divided into twelve variables. These dimensions concern the organizational structure for cyber security (Carayannis et al, 2019), cyber security practices (Annarelli et al., 2020), the change management and risk analysis approach (Katsumata et al., 2010), cyber security competences (Annarelli et al., 2020), and measures to introduce/implement cyber security (Linkov et al., 2013, Collier et al., 2014).
The following tables (Table 2 and Table 3) present the detailed view of the research framework, decomposed into their key distinctive elements, according to literature.

This paper was presented at The XXXIII ISPIM Innovation Conference "Innovating in a Digital World", held in Copenhagen, Denmark on 05 June to 08 June 2022.
Event Proceedings: LUT Scientific and Expertise Publications: ISBN 978-952-335-694-8

Table 2 – Digitalization capabilities decomposed

Digitalization capabilities	
Higher-order capabilities	
1. Reconfiguring firms' digital resources and routines	
1.1. Improvisational capabilities	(Nylén & Holmström, 2015), (Pavlou & Sawy, 2010) (El Sawy, et al. (2010));
1.2. Scanning evolution of digital environment	(Nylén & Holmström, 2015);
1.3. Timely reconfiguration of resources	(Wheeler, 2002);
1.4. Adaptive capabilities	(Kannan & Li, 2017);
2. Seizing firms' digital capabilities	
2.1. Employing heterogeneous resources	(Mishra, Konana, & Barua, 2007);
2.2. Deploying IT for digital competitiveness	(McAfee & Brynjolfsson, 2008);
2.3. Role of managerial cognition in driving change	(Tripsas & Gavetti, 2000);
2.4. Organizing IT capabilities	((Drnevich & Croson, 2013), (Sambamurthy & Zmud, 2000));
3. Sensing opportunities and threats	
3.1. Ecosystem capabilities	(Selander, Henfridsson, & Svahn, 2013);
3.2. Supply chain process integration capability	(Rai, Patnayakuni, & Seth, 2006);
First order capabilities	
4. Integrating data and processes	
4.1. Integrated IS capabilities	(Bharadwaj, Bharadwaj, & Bendoly, 2007);
5. Digitalization-enabled channel integration	
5.1. Cross-channel human resources capabilities	(Oh, Teo, & Sambamurthy, 2012).

Table 3 – Digitalization capabilities decomposed

Cybersecurity	
1. Organizational structure for cyber security	(Carayannis, et al., 2019);
2. Cyber security practices	
2.1. CSRM - Cyber Security Risk Management	((Annarelli , Nonino , & Palombi , 2020), (Katsumata, Hemenway, & Gavins, 2010));
2.2. Cyber Resilience Management	(Annarelli , Nonino , & Palombi , 2020), (Linkov, et al., 2013), (Bodeau & Graubart, 2011));
3. Change management and risk analysis approach	(Katsumata, Hemenway, & Gavins, 2010);
4. Cyber security competences	
4.1. Organizational culture of cyber security	(Annarelli , Nonino , & Palombi , 2020)
4.2. Learning from the environment	(Annarelli , Nonino , & Palombi , 2020)
5. Decisions support systems to introduce/implement cybersecurity actions	
5.1. Resilience matrix	(Linkov, et al., 2013), (Collier, et al., 2014), (Linkov, et al., 2013));
5.2. Cyber security investments	(Armenia et al., 2021)
5.3. Standard	ISO:27001
5.4. Protection tools	(Annarelli , Nonino , & Palombi , 2020)

4 Results

The case study organization is characterized by digital independence, being able to present innovative solutions and investments to the market to help define new technological standards. The digital transformation has been adopted and developed with a *security first* approach to resilience, aiming at an increased efficiency through digitalization of processes, at the generation of value-added services and providing skills and support for decisions in cybersecurity and cyber resilience domains.
Therefore, it is possible to contribute to the objective of the research by carrying out a critical analysis of the results obtained to define how, to what extent and with what preponderance digitalization capabilities can contribute in the area of IT resilience.
First of all, it is possible to see how in the phase of identification, planning and preparation for cyber threats there are several digitalization capabilities that critically contribute in supporting these activities.

Considering the monitoring activities of security events by the Security Operation Center the case under analysis, in order to anticipate possible attacks, having the ability to scan the evolution of the digital environment might allow to consider issues related to, for instance, brand reputation to understand the risk exposure of products and services with respect to the company positioning on the market and vice-versa, as innovations on the market can constitute new vulnerabilities.

Furthermore, during the Plan/prepare phase it becomes essential to have improvisational skills and to employ teams of heterogeneous resources capable of knowing how to respond and build new operational skills to face unpredictable and destructive environmental situations.

The heterogeneity of resources, combined with their training, allows to exploit skills related to digital solutions in different measures. The same innovative technologies that, through the organizational and development capabilities of IT, were considered for digital competitiveness can and actually are used for the prevention of cyber-attacks.

In the organization, in fact, new technological opportunities have been exploited to achieve new forms of competitive advantage and create value for the customer. Thanks to Competence Centres, these technologies are used above all in industry and security, in image recognition or in predicted maintenance activities in the Plan/Prepare phase through the digital twin and cyber range. In addition, it is possible to follow a *security-by-design* approach by inserting digital components capable of guaranteeing cyber resilience.

Finally, planning and monitoring are continuous activities: thanks also to the integration and interaction capabilities with partners in the supply chain (Ecosystem Capabilities, Supply chain process integration capability and Cross-channel Human Resources capability) it is possible to exchange and process information and prevent a lack of communication, collaboration and sharing from creating security holes within the supply chain.

Having an approach oriented toward open innovation, toward the enhancement of partnerships, as well as internal collaboration between the various resources present, as in the case in question, not only allows to know the digital evolution and therefore to obtain a competitive advantage, but also to integrate information and cybersecurity skills and building resilient cyber systems.

Proceeding with the absorption phase of a harmful event as it occurs, in order to ensure the continuity of operations, an interesting observation emerged when the Head of Line of Business (key informant 1) claimed to be aware that the cyber resilience behind the company's offering must be a distinctive element. In seeking and achieving it, the company prefers the creation of transversal teams to foster knowledge sharing, dissemination of an innovation culture and the enhancement of corporate values. In the case of a malicious event, the heterogeneity of the resources and skills may allow to manage the incident, isolate it and limit it through a timely reconfiguration of the resources capable of implementing workaround procedures.

Therefore, having the ability to promptly reconfigure redundant and heterogeneous resources and allow them to take advantage of digital technologies and innovations, allows to maintain the functionality of the most critical assets and the availability of the services provided.

In case this is not enough, the improvisational skills of human resources can intervene in support to operate, protect and limit damage, guaranteeing the (cyber) resilience of services, products, infrastructure and resources themselves.

During the phase of Recover, the functionalities and services impacted by a malicious event, it becomes essential to have recovery plans, resource reallocation procedures and system changes. In the case under analysis, the Cyber Emergency Readiness Team

manages and defines actions to prevent the recurrence of the same incident. Therefore, IT becomes the most important element of the team.
Having the ability to organize IT and consider it as a catalyst for innovative ideas not only contributes to competitive advantage and business opportunities, but also contributes to a structure capable of facing change and exploiting events as opportunities to become more flexible and therefore resilient.
Finally, updating the information learned includes various activities ranging from: performance evaluation, knowledge integration, the internal reorganization of assets and resources, implementation of new procedures, review of products and services portfolio. Those activities necessarily require the integration of supply chain and cross-channel processes of human resources, the ability to scan the evolution of the digital environment, the ability to reconfigure resources and adaptive capabilities.
Furthermore, knowing how to scan one's digital environment to predict and understand the key changes to be implemented is significantly important in adaptation as the digital ecosystem can involve new opportunities but also new threats and vulnerabilities; therefore, being aware of the IT security consequences of the changes to be adopted is essential.
The strategic and tactical information learned from the event and from the scan must be exchanged through the integration of resources, IT processes and digital platforms, with supply chain partners.
Ultimately, the entire process of adaptation, improvement and updating would not be possible without the ability of top management to guide and accompany resources for change. Despite the already considerable level of digitalization, the case study organization continues to implement awareness and training campaigns to stimulate the entire company to be receptive and flexible to any type of change.
The following table (Table 4) summarizes digitalization capabilities together with the cyber resilience phase and their implementation in the case under analysis.

Table 4 – Digitalization capabilities impact over cyber resilience phases

Employing heterogeneous resources	**Plan/ Prepare**	**Combining resources and capabilities to leverage digital solutions in cyber security in different measures**
Scanning evolution of digital environment		Consider both how the products / services pose themselves to the risks to which the organization is exposed with respect to the company's positioning on the market, and how innovations on the market can constitute new vulnerabilities
Deploying IT for digital competitiveness		IT as a catalyst for innovative ideas for cybersecurity: digital twin and cyber range for training and vulnerability assessment; AI for predicted maintenance; security by design
Organizing IT capabilities		Organize digital innovations for cyber-attack prevention
Improvisational Capabilities		Respond and build new operational capabilities to deal with unpredictable and destructive environmental situations during vulnerability testing and identification activities
Ecosystem Capabilities		Correlation of heterogeneous sensitive information to create context and understand key changes to predict possible threats in that market
Supply chain process integration capability		Open innovation and enhancement of partnerships to integrate information and skills for IT security and the creation of resilient cyber systems
Cross-channel Human Resources capability		Enhancement of communication, collaboration and sharing to avoid creating security holes within the supply chain
Employing heterogeneous resources	Absorb	Creation of cross-functional teams for the sharing of knowledge, dissemination of innovation and enhancement of corporate values, in order to manage, isolate and limit the incident
Improvisational Capabilities		Allowing the experience of resources to operate, protect, limit and ensure the resilience of services
Timely reconfiguration of resources		Allocation of even redundant resources to guarantee workaround during a cyber-attack
Organizing IT capabilities		Cyber competence centre structure to exploit digital innovations to maintain the functionality of the most critical assets and the availability of the services provided
Organizing IT capabilities	Recover	The CERT manages and defines the actions to be implemented to remedy and prevent the recurrence of the same incident
Deploying IT for digital competitiveness		Corporate assets are coordinated, renewed and enhanced through the digital technologies present to become robust systems and prevent the same event from happening again
Scanning evolution of digital environment	Adapt	Predict and understand the key changes in the digital environment, to be aware of the consequences on IT security of the changes to be adopted following an event
Timely reconfiguration of resources		Operating as a system integrator, incorporate information from the ecosystem to which it belongs to reconfigure existing resources and related IT security actions
Adaptive capabilities		Use innovations such as AI and ML to measure, evaluate and learn from the information obtained and update the company knowledge base
Supply chain process integration capability		Request evidence from supply chain actors of logistics and production systems, planning tools and to be compliant with a series of regulations
Cross-channel Human Resources capability		Provide sharing mechanisms protected by their cyber security tools (integration of resources, information systems, digital platforms)
Role of managerial cognition in driving change		Implement awareness and training campaigns to stimulate the entire company to be receptive and flexible to any type of change.

5 Conclusion

The main aim of the research was to verify the existence of a possible contribution of digitalization capabilities for cyber resilience, i.e. digitalization as a driver of innovative solutions for effective management of information security, in order to obtain cyber resilient systems.
Despite the numerous facilitations obtained, digital transformation has its weakness in leading companies to face increasingly serious threats in the cyber world. As discussed in the previous sections, if on the one hand all this can be a risk, on the other hand it creates business opportunities: maintaining competitiveness while guaranteeing security and protection and at the same time using cyber security to obtain new forms of competitive advantage is becoming imperative.
However, the rapid evolution of cyber threats demonstrates that current knowledge and skills are gradually becoming obsolete, making the response plans, adopted to date, useless. Hence the need to verify the possibility of receiving support from capabilities such as digitalization capabilities, so far considered only from a strategic business point of view.
Results emerged from the interviews showed how, according to the organization, digitalization and security must go hand in hand and how to achieve an adequate degree of IT resilience, digitalization must necessarily be incorporated into organizational procedures. This result is consistent with the expectations expressed in the research aim, according to which, by now, new technologies and digital capabilities must be used not only to obtain new forms of competitive advantage but also to achieve adequate levels of resilience to face identification. continuous threats and vulnerabilities.
However, it is important to keep in mind that this research has focused on a single case study, so future research is needed with a larger sample to confirm findings and allow for a generalization. A further recommendation could be to carry out a similar, but more in-depth, study on cyber resilience to identify additional digitalization capabilities that can act in support of cyber security.

References

Annarelli, A., Battistella, C. and Nonino, F. (2020) ‘A framework to evaluate the effects of organizational resilience on service quality’, Sustainability (Switzerland), 12(3), pp. 1–15. doi: 10.3390/su12030958.
Annarelli, A., Nonino, F. and Palombi, G. (2020) ‘Understanding the management of cyber resilient systems’, Computers and Industrial Engineering. Elsevier Ltd, 149(January), p. 106829. doi: 10.1016/j.cie.2020.106829.
Annarelli, A. and Palombi, G. (2021) ‘Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework’, Sustainability, 13(23), p. 13065. doi: 10.3390/su132313065.
Armenia, S. et al. (2021) ‘A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs’, Decision Support Systems. Elsevier B.V., 147(April), p. 113580. doi: 10.1016/j.dss.2021.113580.
Björck, F., Henkel, M., Stirna, J., Zdravkovic, J. (2015). 'Cyber Resilience – Fundamentals for a Definition'. In: Rocha, A., Correia, A., Costanzo, S., Reis, L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham. https://doi.org/10.1007/978-3-319-16486-1_31
Carayannis, E. G., Grigoroudis, E., Rehman, S. S., & Samarakoon, N. (2019).

'Ambidextrous cybersecurity: The seven pillars (7Ps) of cyber resilience'. IEEE Transactions on Engineering Management, 68(1), pp. 223-234.
Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). 'Four domains of cybersecurity: a risk-based systems approach to cyber decisions'. *Environment Systems and Decisions*, 4(33), pp. 469-470.
Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014). 'Cybersecurity standards: Managing risk and creating resilience'. *Computer*, 47(9), pp. 70-76.
Ferdinand, J. (2015). 'Building organisational cyber resilience: a strategic knowledge-based view of cyber security management'. *Journal of business continuity & emergency planning*, 9(2), pp. 185-195.
Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). 'Resilience metrics for cyber systems'. *Environment Systems and Decisions*, *33*(4), pp. 471-476.
Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., &
Jensen, S. J., Feldmann-Jensen, S., Johnston, D. M., & Brown, N. A. (2015). 'The emergence of a globalized system for disaster risk management and challenges for appropriate governance'. I*nternational Journal of Disaster Risk Science*, 6(1), pp. 87-93.
Kaplan, J., Richter, W., & Ware, D. (2019). 'Cybersecurity: Linchpin of the Digital Enterprise'. *McKinsey & Company*.
Katsumata, P., Hemenway, J., & Gavins, W. (2010). 'Cybersecurity risk management'. *In 2010 Military Communications Conference* (MILCOM), 890-895.
Kohtamäki, M., Parida, V., Oghazi, P., Gebauer, H., & Baines, T. (2019). 'Digital servitization business models in ecosystems: A theory of the firm'. *Journal of Business Research*, 104, pp. 380-392.
Khan, O., & Estay, D. A. S. (2015). 'Supply Chain Cyber-Resilience: Creating an Agenda for Future Research'. T*echnology Innovation Management Review*, 5(4), pp. 6-12.
Nylén, D. and Holmström, J. (2015) 'Digital innovation strategy: A framework for diagnosing and improving digital product and service innovation', Business Horizons, 58(1), pp. 57–67. doi: 10.1016/j.bushor.2014.09.001.
Karimi, J., & Walter, Z. (2015). 'The role of dynamic capabilities in responding to digital disruption: A factor-based study of the newspaper industry'. *Journal of Management Information Systems*, 32(1), pp. 39-81.
Warner, K. S., & Wäger, M. (2019). 'Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal'. *Long range planning*, 52(3), pp. 326-349.