Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 181 (2021) 261–268

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2020

Supply chain flows and stocks as entry points for cyber-risks

Núbio Gomes Filho[a,*], Nazaré Rego[a,b], João Claro[b,c]

[a]*Escola de Economia e Gestão, Universidade do Minho, Braga, 4710-057, Portugal*
[b]*INESC TEC, Porto, 4200-465, Portugal,*
[c]*Faculdade de Engenharia, Universidade do Porto, Porto, 4200-465, Portugal*

Abstract

As supply chains become more digital to reach new levels of global competitiveness, caveats from this decision arise. Cyber-risks are one of these potential setbacks, affecting supply chains directly and indirectly, and propagating via supply chain flows and stocks – information, material, and financial. This study applied a systematic literature review to determine how the supply chain's flows and stocks serve as points of entry to cyber-risks. Cyber-risks arise from different sources (i.e., direct attacks, built-in problems, low-quality issues), impacting supply chains' flows and stocks (material and information). There is a relation between the type of supply chain and which flow, or stock facilitates access to the supply chain. Finally, we provide a distinction between two concepts related to Supply Chain Risk Management and cyber-risks. This research is useful to 1) enterprise decision-makers, as the description of potential cyber-risks' points of entry delivers hints on where to focus managerial efforts; 2) developers of Supply Chain Management (SCM) Information and Communication Technology (ICT) systems, since discussing potential points of entry build awareness about probable exploitation points, thus improving ICT systems' resiliency, and 3) scholars, as the depiction of the state-of-the-art may serve as a common departing point for future research.

Keywords: Supply chains; Supply Chains' flows; Supply Chains' stocks; Cyber-risks; Supply Chain Cyber Risk Management.

* Corresponding author. Tel.: +351-916-704-147
E-mail address: nubiovidal@hotmail.com; id7657@alunos.uminho.pt

10.1016/j.procs.2021.01.145

1. Introduction

In a world of an ever-growing digitalization process, supply chains follow the digitalization path in order to boost their global competitiveness [10,11] through rapid response and mass customization [24]. Relying on Information and Communication Technologies (ICT) helps supply chains increase their resilience [17,22,24,30]. However, the digitalization process comes with significant setbacks, for example, cyber-risks [10,16]. Cyber-risks constitute a severe supply chain issue because they may change organizations' goals [29] and actions [12].

Supply chain (SC) is a fruitful landscape for cyber-risks to spread [1,8] because every SC element is in danger: companies, flows, stocks, or stakeholders. Although cyber-risks gain power during economic stress [2], they also happen in periods of economic stability. During the relative stability of 2018, cyber-attacks (one group of cyber-risks) increased by 78% [28], and they were among the top-10 concerns of companies for impact and likelihood [34].

Cyber-risks impact supply chains, both directly and indirectly. Directly, cyber-risks impose disruptions in different supply chains' flows, affecting production, revenue, and profits [21,30,31], and generating regulatory penalties due to (information) breaches [27], as imposed by EU General Data Protection Regulation (GDPR). Indirectly, cyber-risks undermine trust among partners [20,23,31] and reduce companies' market value [20,23,27].

Within the potential solution set, cybersecurity training to employees may deal with most cyber-risks [11]. If the supply chain's companies coordinate their cybersecurity investments, they reach optimal levels of security, considering the likelihood of indirect damages [12,27] originated from attacks in their partners.

Cyber-risks tend to use weaker SC elements to propagate among its participants. Thus, this paper determines how the supply chain's flows and stocks serve as points of entry to cyber-risks. Such analysis is cardinal because it provides decision-makers points to focus on, reducing the effects of cyber-attacks. This study is relevant to create coordinated cyber-security policies in SCs. These policies' starting point relates to firms developing their defenses, and a condition to do it is recognizing their exploitable entry points.

The remainder of the paper is organized as follows: Section 2 depicts the steps of the systematic literature review (SLR) conducted to gather the insights systematized; Section 3 answers the research's objective through previous theory, and Section 4 exposes the conclusions and points potential future research topics.

2. Methodology

A SLR on the theme Supply Chain Cyber Risk Management was conducted to determine how the supply chain's flows and stocks serve as points of entry to cyber-risks. By now, Supply Chain Risk Management (SCRM) is aware of cyber-risks as potential problems, and its analytical comprehensiveness aids the recognition SCs' points of entry, which the primary step to describe correct counter-measures to these risks.

First, we selected several databases (SCOPUS, Web of Knowledge, Emerald, Science Direct, Wiley, Taylor & Francis, Sage, and IEEE Xplore) to ensure the gathering and analysis of relevant studies. No year discrimination was set, and potential references were collected up to January 2020. After selecting the databases and the timeframe, defining the terms to be searched was the next step. The search terms used were "Supply Chain Cyber Risk Management" (SCCRM), "Cyber Supply Chain Risk Management" (CSCRM), and the combination of: "Supply Chain Risk Management" AND "Cyber Risk" (SCRM + CR). The papers were gathered if the search terms occurred in the title, abstract, or keyword, resulting in the initial sample size of 221 publications presented in Table 1.

Table 1. Sample size

Searched terms	SCOPUS	Web of Science+	Emerald Insight	Science Direct	Wiley	Taylor & Francis*	SAGE*	IEEE Xplore*
SCCRM	70	58	0	15	6	0	1	1
CSCRM	-	-	1	-	-	0	-	0
SCRM + CR	0	1	0	9	6	1	0	52
TOTAL	70	59	1	24	12	1	1	53

Observations: "+" indicates that each term was searched both in publication name and title. "*" stands for the use of "Anywhere" or "All Metadata" while searching, since searching for title, abstract, or keyword was not available. "-" inside the table indicates that database algorithm combines the terms orders; therefore, the same number found for "Supply Chain Cyber Risk Management" (SCCRM) is found in "Cyber Supply Chain Risk Management" (CSCRM).

After gathering an initial sample of 221 studies (in English, Portuguese, French, and Spanish), some exclusion rounds followed. The first screening step looked for duplicated studies, subtracting 112 papers. After that, conference summaries/calls, courses, about authors, indexes, patents were excluded, reducing nine documents more. The third round of exclusions was due to the incapability of downloading potential studies, impeding the analysis of two documents (conference papers). Two sub-phases divided the fourth round of exclusions that resulted in 34 exclusions. The first sub-phase dealt with incompatibility between the abstract and the objective of this research, from which three possible outcomes were found: "Yes", when the study was incompatible; "Dubious" for studies with abstract (in)compatibility not wholly understood; and, "No", when the study was compatible with the objective of this study. For "Dubious" studies, string searches inside the main text body with multiple strings were performed to decide whether they remained, or not, in the sample. Finally, due to paper length limitations, we added the fifth round, excluding papers not published in peer-reviewed journals, and focusing the analysis on 33 journal articles.

Figure 1 describes these rounds, and Figure 2 portrays the distribution of articles of the final sample by the journal's area (according to SCOPUS classification). Two conclusions derive from Figure 2: 1) before 2012, the topic was published exclusively in "Business, Management and Accounting" journals (3 out of 33). However, few researchers were giving proper attention to it; 2) from 2012 onwards, most publications are at "Computer Science" journals (almost half, 15/33), these journals turn into an inviting environment for this topic during 2018-2020 (two-thirds of the publications in this period, and 8 out of 15 publications in this area).

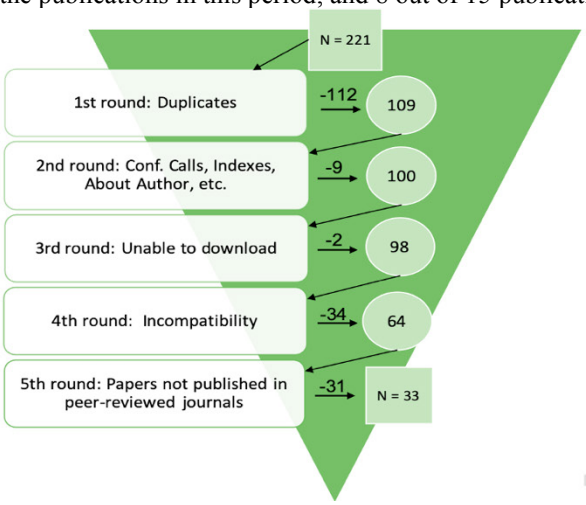

Fig. 1. Rounds of exclusion

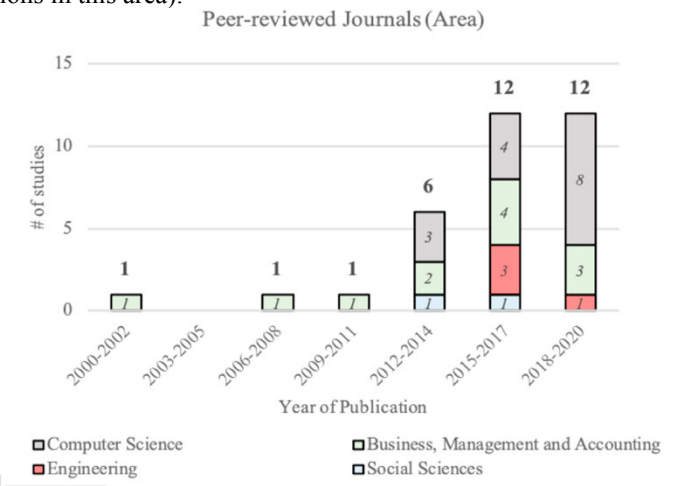

Fig. 2. Peer-reviewed journal articles by Area

Figure 3 depicts a word cloud created using the keywords of the 33 articles. The more recurrent terms are "supply" (30), "chain" (28), "management" (23), "risk" (17), "security" (11), "cyber" (9), "information" (5), and "systems" (5). These words' recurrence makes sense, once this study searched for publications about supply chains and how they manage cyber-risk. For a while, researchers focused mainly on information security and systems, supporting the concern over information flows and stocks. Still, cyber-risks may spread within supply chains using other flows and stocks.

Fig. 3. Keywords word cloud

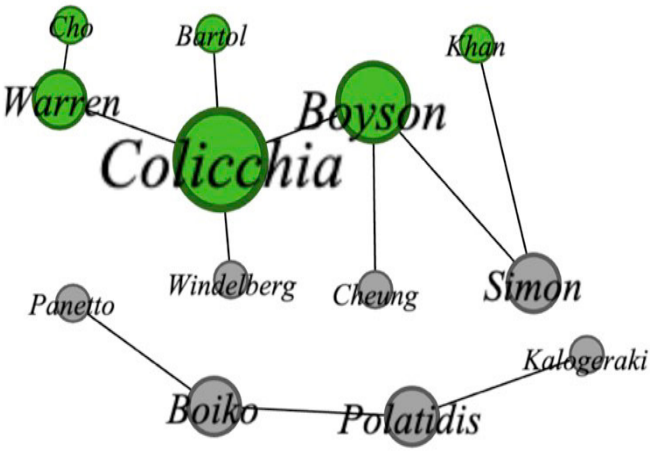

Fig. 4. Citation network

Figure 4 presents the existing citation network among references that compose our final sample. Peer-reviewed articles published in "Business, Management and Accounting" journals are in green, while the studies published in "Computer Science" journals are in grey. There is a connection between 12 references, divided into two clusters. The more significant cluster presents Colicchia et al. (2018) [12] and Boyson (2014) [8] as the central nodes. In [12], there is a thorough analysis of case studies allied to a massive reference body, including [8]. [8] is one of the authors responsible for first using the term "Cyber Supply Chain Risk Management" that concerns Risk Management in Cyber Supply Chains (which provide ICT products/services, like cloud services, hardware, software systems [1,8]). This term gained traction in research after Technovation's volume 34, issue 7, that also published Bartol (2014) [3]. The smaller cluster also has two central nodes: Polatidis et al. (2018) [25] and Boiko et al. (2019) [6]. The first publication, [25], discusses a specific methodology (attack-paths) and how to improve it; the second, [6], focuses on barriers to implement Supply Chain Management (SCM) ICT systems.

3. Findings

In this section, we first identify the potential sources of cyber-threats and cyber-vulnerabilities that combined create cyber-risks (3.1). Source identification increases decision-makers' awareness of how these risks access their organizations, improving the possibility of defending themselves. Moreover, we deepen the discussion about cyber-risks' points of entry using supply chain flows and stocks – information (3.2), material (3.3), and financial (3.4), describing examples, effects and suggestions to mitigate these risks spread. Frequently, once cyber-risks find their way in supply chains, they lead to losses in performance and capacity for supply chains [7]. Although some examples focus on cyber supply chains, the attention should lie on the risk source and not on the type of supply chains, once similar problems start to appear in traditional supply chains, given the increase of smart products manufacture and digitalization process. Lastly, we suggest a conceptual differentiation between two search terms used in our SLR (3.5).

3.1. Types of cyber-risks

Two groups divide cyber-risks: "cyber-threats" and "cyber-vulnerabilities"; for that reason, it is crucial to establish a difference between these two concepts. Cyber-threats represent goal-driven methods employed by attackers aiming to willingly damage [11] SCs, while cyber-vulnerabilities involve opportunistic situations when attackers find out exploitable ways to damage SCs that were not created by them. Table 2 summarizes some sources of SC' attacks, obtained from the SLR, describing cyber-risk type and point(s) of entry (flow or stock) into SCs.

Table 2. Sources of supply chain's attacks, type of cyber-risk and point of entry in supply chains flows or stocks

Sources [Reference]	Type of cyber-risk	Point(s) of entry (flows or stocks)
Built-in problems [2,8,11–13,21,32,35]	Threat	Physical/Information
Hardware/Software counterfeit [2,3,8,10,13,21,32,35]	Threat	-
Direct attacks [2,5,6,8–12,15,18,19,21,23,29–33,35]	Threat	Information/Physical
Insider threat [8,12,29,30,32,33]	Threat	Information/Physical
Low-quality issues [2,11–13,16,21,29,32]	Vulnerability	Physical
Unintentional install. of vulnerabilities on hardware/software [2,7,12,19,23,29,32]	Vulnerability	Information/Physical

Observations: "Built-in problems" cover hardware tampering, malicious code in software. "Direct attacks" represents various methods (i.e., (spear)phishing, (distributed) denial of service, spyware, ransomware attacks) directly aiming their primary target for multiple objectives. "Insider threat" represents employees who are willing to damage companies. "-" indicates that there was no clear point of entry for that source.

Some considerations about Table 2 are noteworthy. In our final sample, most attack sources are goal-driven methods (cyber-threats), representing a concern for firms and SCs, as attackers tend to invest more resources in these scenarios. Concerning the point(s) of entry, almost every attack source has examples in multiple flows and stocks. The written order in this column follows the example frequency in our reference sample. Nevertheless, the examples presented in the next subsections (3.2–3.4) relate to the most frequent point of entry. Finally, counterfeits are not be discussed ahead since there were no examples in our SLR sample providing a clear point of entry, even though they might affect SCs of the original product/service, in terms of demand.

3.2. Information flows and stocks

As digitalization process grows in multiple SCs, information flows and stocks gain importance, since there is an increase in organizations' dependency on data [9,15] for competitive purposes [12]. Without reliable information, managers cannot proactively decide about production or distribution [5,20,26]. Multiple cyber-risks use information flows/stocks to enter SCs, albeit their final product/service. These risks cause severe damage to enterprises, regardless of their size [2,9,23], and concurrently to their SCs' partners.

Direct attacks affect firms' reputation [9], as they try to obtain financial gains, or sensitive information, among other goals. Attacks aiming databases (i.e., data breaches [2,12]) commonly cause reputational problems for companies (and SCs), just as embezzlement [11,29] does. In the past, these attacks focused their main targets openly, but the modus operandi changed as perpetrators are now attacking firms/individuals who provide services [15] to SCs in order to gain their authorized access [12,15], and pursuing after the main target. For example, in 2013, a breach in Target's system containing customers' payment cards data occurred through third-party heating, ventilation, and air conditioning supplier [35] and in 2018, Maersk was breached via its subsidiary, the provider of its ICT system [10], taking ten months to realize the attack. When attacks have purely financial motivation, attackers turn to quick profit methods, like ransomware attacks (WannaCry, in 2017 [10,15]). Industrial espionage, on the other hand, encompasses attacks to acquire sensitive information, which might occur during information transfers or aiming servers that retain organizational secrets (e.g., formulae, source codes, patents, or trademarks [6,10,32]). For example, a Chinese inventory scanner manufacturer inoculated a malware in its product to steal its consumers' intelligence [19]. Industrial espionage occurs using social engineering methods [12], like (spear)phishing campaigns [12,19,33], for instance.

Insider threats happen if employees start acting carelessly on purpose [2] or using authorized access and procedures [2] to alter information or steal sensitive data. This case is one of the most difficult to control and monitor [8] due to the provided access and SCs complexity [8]. Decision-makers use the help of other employees, who may be observing strange behaviors in their colleagues [5], to manage this problem. Finally, cyber-risks may enter SCs through the unintentional installation of vulnerabilities on hardware/software [2,6]. In such cases, investing in employees' cyber-training (as discouraging password sharing [33]) generates good results [10,11,33,35].

Given information importance to SCs, decision-makers must assure privacy, security, reliability of the information as well as assuring process compatibility between partners regarding both internal and external standards [4].

3.3. Material flows and stocks

Material flows and stocks are essential for every SCs' operation. Materials, in this context, represent every raw material, components, work-in-progress, and final products that are used in SC's process of manufacturing physical products or offering services. Attackers, generally, use these points of entry (material flows and stocks) to crawl into cyber supply chains and traditional supply chains that started manufacturing smart products. Cyber-risks affect SCs through these flows and stocks, mainly using tampering and low-quality issues, causing disruption in operations.

Built-in problems (i.e., tampering [10,29]) represent a significant threat to supply chains and society in general. In this scenario, organizations purchase raw materials and intermediate products unaware of these issues. Attackers' main objective here is to exploit such problems at some point. For example, in 2010, Dell sold servers with pre-installed malware in their motherboards, and it took more than fifteen changes in their SCs' procedures to eliminate the threat [8]. Tampering may also affect society if targeting state departments. In 2007, the United States Department of Defense used hard drives with built-in problems that copied sensitive information and sent it to another intelligence department [8]. Supply chains use constrained purchasing from selected suppliers [18], require tamper-proof components, and establish procurement cyber-security policies or procedures [35] to mitigate this source cyber-risk.

Low-quality issues create exploitable vulnerabilities in SCs. This source of cyber-risk presents a relation between its disturbances' impact and the risk acceptance level a SC has. For example, a low-quality chip used in running sneakers, as those manufactured by Xiaomi, may lead to problems in pairing, inaccurate mensuration, or even premature failures [2]. However, more severe problems occur if the military sector uses low-quality embedded chips, for instance. This vulnerability frequency increases as decision-makers opt on suppliers solely based on cost parameters, disregarding effectiveness indicators [14] and do not possess good quality control standards, as quality control may catch these problems. In order to deal with this issue, decision-makers use interviews and background checks [18] before exchanging to a cheaper supplier, as well as increase investments in internal quality control [16].

These cyber-risks also cause reputational problems, if attacker using built-in problems or low-quality issues to access manufacturing systems modify mechanical parameters to disrupt production process or to increase costs with warranty claims due to premature failures [7]. Failures in SCM ICT systems and their components prevent supply chains' from receiving, processing, and fulfilling order requests [7], damaging companies' reputation, as well. Production systems with continuous risk assessment, using machine and deep learning, increase awareness of these cases, enabling a quick override of abnormal changes or informing decision-makers about them.

3.4. Financial flows and stocks

Supply chains' financial transactions occur among companies and their consumers as a counterpart of products/services delivered. In our sample, there were no examples of how cyber-risks used monetary flows or stocks to crawl into SCs. Despite the lack of examples, after each problem described in subsections 3.2 and 3.3, changes in financial stocks occur in response, and, consequently, financial flows take place to move these resources.

3.5. Supplementary findings

A useful differentiation arising from our SLR is added to our previous findings. Originally, the terms "Cyber Supply Chain Risk Management" (CSCRM) and "Supply Chain Cyber Risk Management" (SCCRM) were used interchangeably. Nevertheless, some studies [10,12] used CSCRM as a catch-all term for both the cyber supply chain SCRM and a broader risk environment. CSCRM, though, should concern only with managing risks in cyber (ICT) supply chains [3,8,13,17,25,32]. While SCCRM would be the broader risk environment and thus naming the area of study that encompasses all different supply chains willing to manage cyber-risks, inducing cyber-resiliency [20].

For SCs, the concept of "cyber-resilience" determines the development of capabilities that enable supply chains to respond quickly to cyber-risks' impacts, remaining operational [7,20,30]. Creating such capabilities is important given most organizations [20] do not realize their exposure to this type of risk until they are impacted by them [20,30], especially the ones initializing their digitalization process or the manufacturing of smart products. Cyber-resilience's concept appears three times in our sample [7,20,30] at Technology Innovation Management Review in 2015, although the World Economic Forum had already been defined this concept in 2012 [7]. Table 3 depicts critical references

inside our sample that ground the difference between CSCRM and SCCRM concepts.

Table 3. In-sample grounding references for differentiation between CSCRM and SCCRM

CSCRM	SCCRM
Bartol [3]	Boyes [7]
Boyson [8]	Khan and Estay [20]
Davidson and Shankles [13]	Urciuoli [30]
Ivanov et al. [17]	
Polatidis et al. [25]	
Windelberg [32]	

4. Conclusion and Recommendations

As supply chains go digital, they are turning into more complex and dynamic networks. This paper determines how the supply chain's flows and stocks serve as points of entry to cyber-risks. Recognizing potential points of entry creates conditions for SCs' participants to build up their defenses, which represents the first step for developing coordinated cyber-security policies to monitor and manage the whole SC [10], which ultimately enables SCs to act against these risks propagation [33,35] promptly.

Cyber-risks arise from different sources [35], using mainly (physical and information) flows and stocks to enter supply chains. Information flows, and its stocks continue to be the primary access cyber-risks have to crawl into SCs, since these points of entry have low relation with its final product/service. Cyber supply chains and traditional supply chains producing smart products are also targeted via physical flows and stocks. Cyber-risks' sources and impacts must be minimized in order to maintain the supply chain's performance [10] and resiliency [12].

Secondly, the modus operandi of how cyber-risks crawl into supply chains evolved [10,35]. In the past, the main targets were openly focused, while nowadays, cyber-risks first reach more vulnerable targets (users or small companies) moving later to higher-profile firms, as in Target's data breach. Once cyber-risks enabled attackers in, their actions' impacts may cascade to other flows/stocks and organizations in the supply chain. Though supply chains benefit from coordination in its components' cyber-security investment [27], it is naïve to assume that all supply chain participants, or its subcontractors, implement fully protective actions [15] for known cyber-risks. Thus, adapting SCRM tools for managing cyber-risks increases SC's cyber-resiliency.

Multiple agents may find this research useful, given it: 1) provides information to enterprise decision-makers about potential points of entry for cyber-risks in SC, focusing their managerial efforts; 2) enables developers of SCM ICT systems to be more aware of potential exploitation points in SC, improving SCM ICT systems' resiliency; and, 3) contributes to systematize the state-of-the-art around the studied topic.

This research's main limitation concerns its reference sample since we defined the points of entry using frequent examples in the SLR database. We expect to increase this analysis in a future publication, by expanding our reference sample using other terms, like the ones in [3]. This expansion could enhance the set of SC's attack sources, offer additional examples of points of entry beyond flows/stocks, and refine the definitions of CSCRM and SCCRM.

As avenues for future research, we suggest: 1) observing if, and how, cyber-attacks affect SC's monetary flows and stocks. 2) Contacting decision-makers and ICT specialists to comprehend which SC elements concern them most relatively to cyber-risk, focusing future analysis on creating faster solutions to deal with opportunistic and goal-driven attackers, as they are adaptive adversaries [35]. Lastly, 3) cyber-resilience issues may be dependent on a product's lifecycle [7], thus observing this relation also provides decision-makers better tools to manage cyber-risks.

Acknowledgments

Portuguese national funds from FCT - Fundação para a Ciência e a Tecnologia, within the Ph.D. Scholarship Reference: SFRH/BD/145941/2019, partially supported this research.

References

[1] Akinrolabu, O. et al. (2019) "CSCCRA: A Novel Quantitative Risk Assessment Model for SaaS Cloud Service Providers" *Computers* **8** 66.

[2] Axelrod, C.W., and S. Haldar. (2018) "Security Risks to IT Supply Chains under Economic Stress" *Int. J. Cyber Warf. Terror* **3** 58–73.
[3] Bartol, N. (2014) "Cyber supply chain security practices DNA - Filling in the puzzle using a diverse set of disciplines" *Technovation* **34** 354–361.
[4] Bhimani, A., and M. Ncube. (2006) "Virtual integration costs and the limits of supply chain scalability" *J. Account. Public Policy* **25** 390–408.
[5] Birkel, H.S., and E. Hartmann. (2019) "Impact of IoT challenges and risks for SCM" *Supply Chain Manag. An Int. J.* **24** 39–61.
[6] Boiko, A. et al. (2019) "Information systems for supply chain management: Uncertainties, risks and cyber security" *Procedia Comput. Sci.* **149** 65–70.
[7] Boyes, H. (2015) "Cybersecurity and Cyber-Resilient Supply Chains" *Technol. Innov. Manag. Rev.* **5** 28–34.
[8] Boyson, S. (2014) "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems" *Technovation* **34** 342–353.
[9] Brown, L. (2015) "High on the Risk Radar - Reputation Risk" *Food Aust.* **67** 31–35.
[10] Cheung, K. and M.G.H. Bell. (2019) "Attacker-Defender Model against Quantal Response Adversaries for Cyber Security in Logistics Management: An Introductory Study" *Eur. J. Oper. Res.*
[11] Cho, S. and M. Pak. (2011) "An Integrative View on Cyber Threat to Global Supply Chain Management Systems" *J. Korea Trade* **15** 55–83.
[12] Colicchia, C. et al. (2019) "Managing cyber and information risks in supply chains: insights from an exploratory analysis" *Supply Chain Manag. An Int. J.* **24** 215–240.
[13] Davidson, D. and S. Shankles. (2013) "We cannot blindly reap the benefits of a globalized ICT supply chain!" *CrossTalk* **26** 4–7.
[14] Dunlap, H. (2016) "A path towards cyber resilient and secure systems metrics and measures" *Insight* **19** 54–57.
[15] Häyhtiö, M. and K. Zaerens. (2017) "A Comprehensive Assessment Model for Critical Infrastructure Protection" *Manag. Prod. Eng. Rev.* **8** 42–53.
[16] Ioshifu, K. et al. (2017) "Cybersecurity Consulting Services in the World of IoT" *NEC Tech. J.* **12** 1–9.
[17] Ivanov, D. et al. (2019) "The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics" *Int. J. Prod. Res.* **57** 829–846.
[18] Jones, R.A. and B. Horowitz. (2012) "A System-Aware Cyber Security architecture" *Syst. Eng.* **15** 225–240.
[19] Kalogeraki, E.-M. et al. (2018) "A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments" *Appl. Sci.* **8** 1477.
[20] Khan, O. and D.A.S. Estay. (2015) "Supply Chain Cyber-Resilience: Creating an Agenda for Future Research" *Technol. Innov. Manag. Rev.* 6–12.
[21] Mensah, P. and Y. Merkuryev. (2014) "Developing a Resilient Supply Chain" *Procedia - Soc. Behav. Sci.* **110** 309–319.
[22] Mensah, P. et al. (2015) "Using ICT in Developing a Resilient Supply Chain Strategy" *Procedia Comput. Sci.* **43** 101–108.
[23] Osborn, E. and A. Simpson. (2018) "Risk and the Small-Scale Cyber Security Decision Making Dialogue - A UK Case Study" *Comput. J.* **61** 472–495.
[24] Panetto, H. et al. (2019) "Challenges for the cyber-physical manufacturing enterprises of the future" *Annu. Rev. Control* **47** 200–213.
[25] Polatidis, N. et al. (2018) "Cyber-attack path discovery in a dynamic supply chain maritime risk management system" *Comput. Stand. Interfaces* **56** 74–82.
[26] Qian, F. et al. (2017) "Fundamental Theories and Key Technologies for Smart and Optimal Manufacturing in the Process Industry", *Engineering* **3** 154–160.
[27] Simon, J. and A. Omar. (2020) "Cybersecurity investments in the supply chain: Coordination and a strategic attacker" *Eur. J. Oper. Res.* **282** 161–171.
[28] Symantec. (2019) "Internet Security Threat Report: Volume 24".
[29] Torabi, S.A. et al. (2016) "An enhanced risk assessment framework for business continuity management systems" *Saf. Sci.* **89** 201–218.
[30] Urciuoli, L. (2015) "Cyber-Resilience: A Strategic Approach for Supply Chain Management" *Technol. Innov. Manag. Rev.* **5** 13–18.
[31] Warren, M. and W. Hutchinson. (2000) "Cyber attacks against supply chain management systems: a short note" *Int. J. Phys. Distrib. Logist. Manag.* **30** 710–716.
[32] Windelberg, M. (2016) "Objectives for managing cyber supply chain risk" *Int. J. Crit. Infrastruct. Prot.* **12** 4–11.
[33] Wolden, M. et al. (2015) "The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system" *IFAC-PapersOnLine* **28** 1846–1852.
[34] World Economic Forum. (2020) "The Global Risks Report 2020".
[35] Zheng, K. and L.A. Albert. (2019) "A Robust Approach for Mitigating Risks in Cyber Supply Chains" *Risk Anal.* **39** 2076–209.