Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda

Article *in* Journal of Asia Business Studies · November 2021

DOI: 10.1108/JABS-11-2020-0444

1 author:

James Perez-Moron
Universidad Tecnológica de Bolívar
16 PUBLICATIONS **3** CITATIONS

Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda

James Pérez-Morón

Abstract

Purpose – *The contribution of this study aims to twofold: First, it provides an overview of the current state of research on cyberattacks on Chinese supply chains (SCs). Second, it offers a look at the Chinese Government's approach to fighting cyberattacks on Chinese SCs and its calls for global governance.*

Design/methodology/approach – *A comprehensive literature review was conducted on Clarivate Analytics' Web of Science, in Social Sciences Citation Index journals, Scopus and Google Scholar, published between 2010–2021. A systematic review of practitioner literature was also conducted.*

Findings – *Chinese SCs have become a matter of national security, especially in the era of cyber warfare. The risks to SC have been outlined. Cybersecurity regulations are increasing as China aims to build a robust environment for cyberspace development. Using the Technology-organization-environment (TOE) framework, the results show that the top five factors influencing the adoption process in firms are as follows: relative advantage and technological readiness (Technology context); top management support and firm size (Organization context) and government policy and regulations (Environment context).*

Research limitations/implications – *This review focuses on cyberattacks on Chinese SCs and great care was taken when selecting search terms. However, the author acknowledges that the choice of databases/terms may have excluded a few articles on cyberattacks from this review.*

Practical implications – *This review provides managerial insights for SC practitioners into how cyberattacks have the potential to disrupt the global SC network.*

Originality/value – *Past researchers proposed a taxonomic approach to evaluate progress with SC integration into Industry 4.0; in contrast, this study is one of the first steps toward an enhanced understanding of cyberattacks on Chinese SCs and their contribution to the global SC network using the TOE framework.*

Keywords *China, Supply chain, Supply chain management, Cybersecurity, Cyberattacks, Supply chain risks, TOE framework*

Paper type *Conceptual paper*

James Pérez-Morón is based at Business Department, Universidad Tecnológica de Bolívar, Cartagena De Indias, Colombia.

Received 10 November 2020
Revised 29 April 2021
25 July 2021
9 August 2021
Accepted 10 August 2021

The author would like to thank the two unknown reviewers for their constructive feedback to improve the contents of this paper. The author also gratefully thanks PhD Felix Wang (Taiwan), for his support. Needless to say, this does not imply that they endorse the analysis in this publication. Tjebbe Donner (Scotland) assisted in copy editing the manuscript.

1. Introduction

Increasing technological sophistication has led to a rise in cybercrime (Soumyo, 2004; Sabillon, 2016; Kennedy *et al.*, 2019; Chandra and Snowe, 2020; Buil-Gil *et al.*, 2021), which affects global business every day (Zheng and Albert, 2019; Hassija *et al.*, 2020). Thus, governments, organizations and businesses of all sizes must prioritize protections against it to mitigate-related risks (Bambauer, 2014; Brookson *et al.*, 2016; Pandey *et al.*, 2019; Simon and Omar, 2019; Li and Xu, 2021), prevent their information and services (Harfouche and Robbin, 2015; Minnaar, 2017; Rahman *et al.*, 2020; Alzubaidi, 2021; Cascavilla *et al.*, 2021) to enrich their competitiveness level (Duong *et al.*, 2020; Yassine and Singh, 2020).

Cybercrime (unlawful acts that target or use computers, computer networks or networked devices) (Dashora, 2011; Choo *et al.*, 2021) is more of a general term. Cyberattacks, a

branch of cybercrime, are more specific and relate to specific attacks made on someone using new technology, a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. In total, 53% of cyberattacks result in over US$500,000 in damages and other serious consequences (Lindsay, 2015; Cisco Annual Cybersecurity Report, 2020). Cybersecurity is the use of technology to protect information (Darko and Boris, 2017; Colajanni *et al.*, 2018; Li and Xu, 2021).

From a managerial perspective, senior global executives have understood the importance of cybersecurity, the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks (Darko and Boris, 2017; Massimino *et al.*, 2018; Jang-Jaccard and Nepal, 2021; Kaspersky, 2021) and 83% of them have improved the security of computers, devices or systems; 78% have improved data protection capabilities; 63% have assessed cyber risks/controls against cybersecurity standards; and 62% have strengthened cybersecurity policies and procedures (Sarathy, 2006; Marsh Microsoft Global Cyber Risk Perception Survey, 2019; Parenty and Domet, 2019; Annarelli *et al.*, 2020) in and at their companies.

Cybercrimes in China are 1/3 of total crimes nationwide, with a growth rate of 30% per year (Jiang, 2020). In total, 80% of people and businesses in China have experienced cybercrime (Mu and Yonggang, 2014) including the disclosure of personal information, online fraud, stolen accounts or passwords and viruses (Kshetri, 2013; Cho and Chung, 2017; Zhang *et al.*, 2018; China Internet Network Information Center, 2017). Internet users have also suffered cybercrimes, e.g. in India 80%, the USA 61%, France 60%, New Zealand 59%, Australia 57%, UK 57%, Italy 53%, The Netherlands 51%,– Germany 47% and Japan 42% (Xuetong, 2006; Bellabona and Spigarelli, 2007; Hang, 2017; NortonLifeLock Cyber Safety Insights Report, 2019). As Washington and Beijing trade tensions rise, 87% from people in the USA considered cyberattacks from China as concern number two, others are economic threats, environmental damage and human rights (Spring 2018 Global Attitudes Survey, 2018).

Many multinational enterprises have made China their operational base (Singh and Gaur, 2020), which points out the importance of China's measures to tackle serious risks regarding the security of its SC (Savitri and Dyah, 2019). This has led to China implementing preventive measures against these tactics, including new technologies with interesting functionalities to help firms secure their SCs (Sarathy, 2006; Cui *et al.*, 2020). The development of cybersecurity norms – namely, the "rules of the road" to guide the behavior of nation-states in cyberspace (Deibert, 2011) – is emerging as a primary international security challenge (Neutze and Nicholas, 2013; Visner, 2013; Zhao, 2016; Kokas, 2018). China believes that the best way to overcome these challenges is to determine/cyberspace standards according to its domestic conditions or, in other words, to prioritize solving internal problems (Nathan, 2012; Kshetri, 2013; Li *et al.*, 2019; Qian, 2019; Manantan, 2021) and to stop gradually the rely on imported basic hardware and software (Mu and Yonggang, 2014). Chinese Government has expedited key policies to strengthen its technological ecosystem including the "Made in China 2025", the "Internet Plus" plan, the "Digital Silk Road" and the "Belt and Road Initiative" among others (Jiang, 2020).

This research aims to explore the cyberattacks on Chinese SCs using the Technology-organization-environment (TOE) framework, focusing on the following research question (*RQ*): *What has been China's approach to combat cyberattacks on its SC and its calls for the global governance?*

The contribution of this study is twofold and includes the following research objectives (ROs) in relation to this *RQ*:

RO1. To provide an overview of the current state of research on cyberattacks on Chinese SC.

RO2. To offer a look at the Chinese Government's approach to fighting cyberattacks on Chinese SCs and its calls for the global governance.

The structure of this paper is as follows: it begins with the literature review, then an overview of the theoretical foundation and methodology used in this research, followed by a discussion of the major findings. Finally, the author presents the main conclusions, limitations and outline avenues for future research.

2. Literature review

Cyberattacks continue to attract great attention worldwide. In July 2021, a Google search returned 19 million results for cyberattacks, 7.4 million for cyberattacks on supply chains and 74 million results related to cybersecurity on SC (Kshetri, 2017). Following Fosso Wamba *et al.* (2018), the author outlines an increased interest in the topic, reflected by Google Trends that identify Singapore, the USA, Canada, United Arab Emirates and the Philippines, as the top five countries with greater interest in this topic between 2010 and 2021.

Several researchers have focused on SC cyberattacks in recent years. Ariffin (2021) focused on cyberattacks using internet access and Urquhart and McAuley (2018) on the protection on industrial things from the internet. Levy (2021) covered how cyberattacks are focusing on individuals or small organizations that are part of the SC of larger organizations. Radanliev *et al.* (2020) identified a dynamic and self-adapting SC system supported by Artificial Intelligence and Machine Learning (AI/ML) and real-time intelligence for predictive cyber risk analytics. Etemadi *et al.* (2021) described using blockchain for robust cyber SC risk management (CSCRM) (Gourisetti *et al.*, 2019; Pournader *et al.*, 2019; Alazab, 2020; Dehghani *et al.*, 2020; Ram and Zhang, 2020; Etemadi *et al.*, 2021). Barata (2021) looked at the ongoing fourth revolution of SCs (4SC) and cyber risks due to the evolution of technology (Rodger and George, 2017; Kumar *et al.*, 2018; Golmohammadi and Hassini, 2020; Ahmad *et al.*, 2021).

Some of these reviews have been comprehensive (Macedo *et al.*, 2019; Pandey *et al.*, 2019; Sengupta *et al.*, 2020; Sepulveda *et al.*, 2020) while others have focused on specific aspects, such as the internet of things (IoT) (Oravec, 2017) enabled cyberattacks in industry, smart grid, transportation, medical services and smart homes (Stellios *et al.*, 2018; Kennedy *et al.*, 2019; Gupta *et al.*, 2020a), Block Chain integration in health supply chain management (SCM) (Nanda and Nanda, 2021) or ethical and regulatory issues as related to cyberattacks (Pesapane *et al.*, 2018). These reviews have covered key issues and provided key insights, but ours is one of the first studies to examine cyberattacks on Chinese SCs and calls for global governance, an issue not well studied in the literature, our works aim to reduce these gaps.

Following DePietro *et al.* (1990), Wallace *et al.* (2020) presented an extended TOE framework specifically aimed at cybersecurity and included new dimensions, such as cyber catalysts and practice standards. For instance, Hasan *et al.* (2021) adopted such a TOE framework to study the factors influencing cybersecurity and its effects on the organization, and Dahabiyeh (2021) used the TOE framework and content analysis to identify key factors that affect organizations and their information security. Daniels and Jokonya (2020) adopted the TOE framework to study the factors that impact digital transformation in the retail SC. Cheung *et al.* (2021) studied the factors that improve cybersecurity in logistics and SCM.

3. Theoretical background: the technology-organization-environment-framework

Following DePietro *et al.* (1990), whose seminal work explains the process by which a firm adopts and implements technological innovations and how this is influenced by the technological, organizational and environmental context, this study uses the

Technology-organization-environment framework (TOE framework) to study and frame our literature review and it will provide a foundation for proposing future *RQ*s. *Technological context* describes all technologies relevant to firms, including in-use technologies and those not currently in use at the firms (Zhu *et al.*, 2002; Baker, 2011). *Organizational context* relates to the firm's features, such as size and managerial structure (Zhu *et al.*, 2002; Baker, 2011). *Environmental context* refers to the structure of the industry (i.e. government, industry competitors (Baker, 2011). See a summary of the TOE framework in Figure 1.

The TOE framework is selected for this study as it takes a holistic approach for organizational-level research (Al Hadwera *et al.*, 2021), instead of other frameworks' individual approach as follows: Innovation diffusion model (Rogers, 2003); technology acceptance model (TAM) (Venkatesh, 2008); Human-organization-technology model (Yusof *et al.*, 2008); and Technology task fit model (Goodhue and Thompson, 1995).

The TOE framework is related to cybersecurity adoption decision-making processes (Wallace *et al.*, 2020) and has corroborated its relevance in multiple studies, in addition to having been tested in Asian, European and American contexts (Chau and Tam, 1997; Kuan and Chau, 2001; Ramdani *et al.*, 2009). In particular, the adoption of innovations in several industries, such as manufacturing (Zhu *et al.*, 2004; Mishra *et al.*, 2007), health care (Lee and Shim, 2007), retail, wholesale and financial services (Zhu *et al.*, 2004; Zhu and Kraemer, 2005), has been widely studied in the twenty-first century.

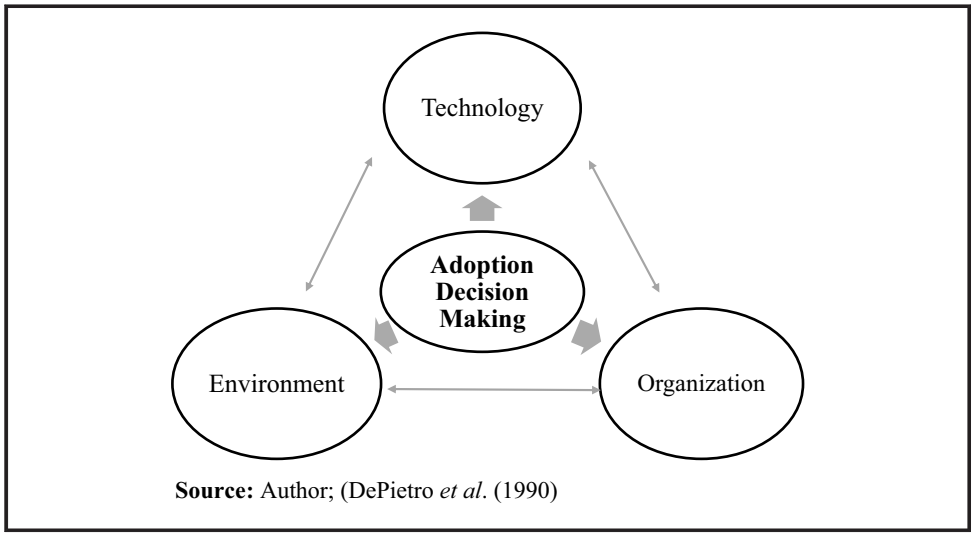
We will also follow Pandey *et al.* (2019) to cover SC risk, defined as "potential deviations from the initial overall objective that, consequently, trigger the decrease of value-added activities at different levels" (Jüttner *et al.*, 2003; Bandaly *et al.*, 2013). Mitchell (1995) proposed how damages occur because of risk, with P being the probability of damage, and I, the significance of that damage to an organization as follows:

*Risk = P (Loss)** I (Loss)

Thus, the sources and types of SC risk can be seen in Figure 2.

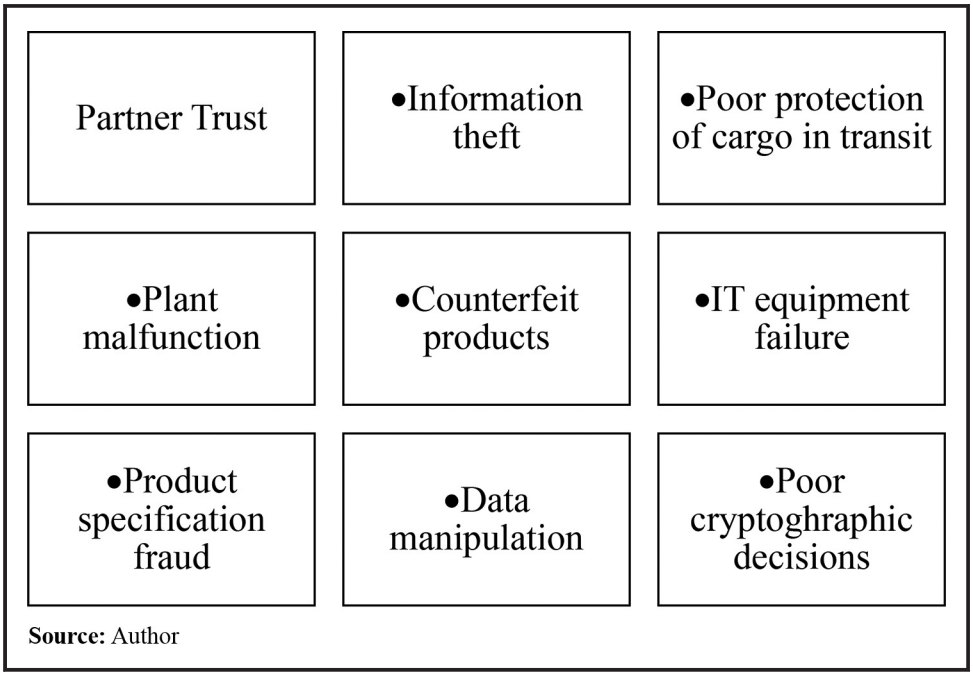
The author finds the following are the methods used by SC cyberattacks (Pandey *et al.*, 2019): Password sniffing/cracking software, Spoofing attacks, Denial of service attacks, Direct attacks, Malicious tampering or Insider threats and Malware infections, Social engineering, Brute-force attack, Exploiting configuration vulnerability, Physical attack or

Figure 1 TOE framework



Source: Author; (DePietro *et al.* (1990)

Figure 2 Sources and types of SC risk



Source: Author

Modification, Open-Source Intelligence, Counterfeiting (ENISA, 2021). Figure 3 contains the multiple risk sources and their corresponding risk categories for global SCs.

3.1 Cyberattacks on supply chain

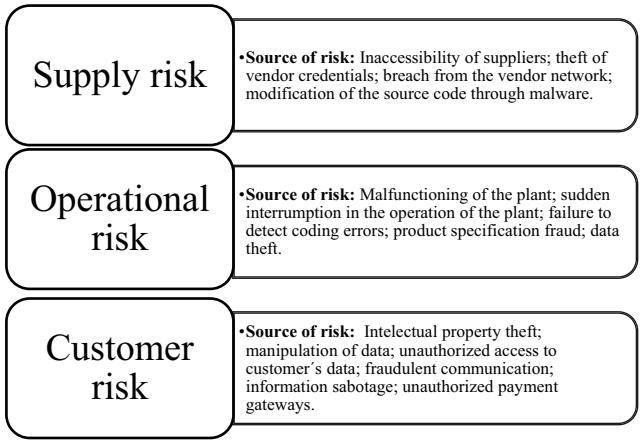
Natural disasters, movements, such as Black Lives Matter and EndSARS, and more recently, the global COVID-19 pandemic, have had a severe impact on manufacturing, logistics and global SC flows that require technology to rapidly overcome the operational disruptions generated, including cyberattacks on SCs (mostly via data breaches, ransomware and operational vulnerabilities), specifically on production sites, shipping and logistics operators and entire industries.

Cyberattacks in SC are soaring amid COVID-19. In total, 40% of manufacturers reported being affected by a cyber incident within the past year, with financial impacts ranging from US$330,000 (IoT cyber incidents) to US$7.5m (data breach). Major cyber risks identified can be broken down as follows: 87% unauthorized access, 85% intellectual property theft and 86% operational disruption.

In 2020 several cyberattacks were observed on multiple key global SC players, including ransomware attacks on two of the world's major shipping lines, MSC Mediterranean Shipping Company S.A. and CMA CGM S.A., and the International Maritime Organization (Everstream Analytics, 2021), SolarWinds Orion, Mimecast, Ledger, Kaseya in 2021, as well as attacks on governments, COVID-19 vaccine researchers and the health-care SC. A list of prominent SC attacks from January 2020 to early July 2021 can be found in Table 1.

Cyberattacks are expected to rise due to vulnerabilities in global SC networks, highlighting the importance of this and all related research as operational perils continue growing for global SCs. Cyberattacks on SC, a fundamental part of international trade, which threaten to steal important information from suppliers, companies and consumers, are currently among the most dangerous emerging obstacles to international trade (Lu *et al.*, 2013; Peng, 2015; Lindsay *et al.*, 2015). The physical SC is the sum of those activities that promote the

Figure 3 Cybersecurity risks in global SCs



Source: Author

Table 1 Prominent attacks on global SC (2020–July 2021)

Supplier	*Supplier category*	*Year*
Mimecast	Security software	2021
SITA	Aviation	2021
Ledger	Blockchain	2021
Verkada	Physical security	2021
Apple Xcode	Development software	2021
Codecov	Enterprise software	2021
Kaseya	IT management	2021
Microsoft HCP	Software	2021
SolarWinds	Cloud management	2020
Accellion	Security software	2020
NetBeans	Development software	2020

Source: Author, based on ENISA (2021)

circulation of commodities (Lu *et al.*, 2013; Rongping and Yonggang, 2014; Savitri and Dyah, 2019). The Information and Telecommunications (ICT) SC includes all the actors that make up the network infrastructure (Boyson, 2014; Lu *et al.*, 2013; Rongping and Yonggang, 2014). If the ICT SC is destroyed, the physical SC will be too (Lu *et al.*, 2013; Von Solms and Van Niekerk, 2013; Karjalainen, 2019).

Hence, the SCM refers to the active management of SC activities which include everything from product development, sourcing, production and logistics, as well as the information systems needed to coordinate these activities to maximize customer value and achieve a sustainable key competitive advantage (Monczka *et al.*, 2015; Singh, 2019). According to Mangan and Lalwani (2016), SCM is:

[. . .] designed to get the right product, in the right quantity, in the right place at the right time, for the right customer at the right cost.

Cyberattacks pose a complex challenge for SCM (Austin, 2016; Gjesvik and Overbo, 2019; Simon and Omar, 2019). Companies with strong brands are likely to be even more concerned about the overall impact of a security breakdown on their brand value and corporate reputation. Cybersecurity is now an essential and central part of the SC, and

factories, operations and customers must develop strategies and skills to cope with these new security demands and improve organizational competitiveness (Sarathy, 2006; Manning, 2019; Pandey *et al.*, 2019; Duong *et al.*, 2020; Ramirez-Pena *et al.*, 2020; Mageto, 2021).

Out of the multiple cyberattacks on Chinese SC during the past years, here we present two SC attacks in China identified, analyzed and validated based on ENISA (2021) as follows:

1. AISINO Credit Information Company supplies tax payment software to international customers through its "Golden Tax" department, including the "Aisino Tax Software Suite." In June 2020, researchers disclosed that the "Aisino Tax Software Suite" was compromised to include malware. It is not known how the software was compromised and what the goal of the attack was. The attack was targeted at businesses in China as this software is part of a national program in that country. The attack was not attributed (ENISA, 2021, p. 37).
2. Microsoft Windows Hardware Compatibility Program. In June 2021, it was disclosed that attackers abused the code signing processes Microsoft uses to validate third-party drivers to sneak and distribute a rootkit malware. Through the valid signature, the malware could be installed in users' systems. The attack appeared to be targeting the gaming sector in China129. The attack was not attributed (ENISA, 2021, p. 53).

4. Methodological approach to the literature review

Based on prior review articles (Paré *et al.*, 2015; Shen *et al.*, 2017; Gilal *et al.*, 2018), the criterion used to identify the articles for this study was their protocol development. First, the author searched for and reviewed past literature reviews on the topic (Table 2). This review allowed practitioners and researchers to understand research topics, trends and gaps to cover in future research. The following is the protocol used to search for the articles included in this work:

- Clarivate Analytics' Web of Science (WoS) and Scopus, the most well-known bibliographic databases (Paul and Criado, 2020), together with Google Scholar were used for searching peer-reviewed articles exclusively published on this topic between 2010 and July 2021 whose titles and abstracts included these keywords as follows: "China," "Supply chain," "Cybersecurity," "Cyberattacks," "Cyber warfare" and "Supply Chain Management" together with other synonyms. This search used Boolean Operators (OR, AND) as these terms have been interchangeably used in SC research.
- Only peer-reviewed articles were included to ensure article quality and inclusion of empirical and theoretical articles.
- Finally, out of all the articles identified, the author considered the ones published in the Social Science Citation Index (SSCI), as this would guarantee high-quality and high-impact research articles related to cyberattacks on SCs (Paul and Singh, 2017; Gupta *et al.*, 2020a).
- Overall, the author identified and included 27 articles. These articles were published in 25 different academic journals. 2020 was the year with most publications (114) followed by 2021 (109). The author used content analysis to analyze the findings (Paul *et al.*, 2017). These 27 articles did not examine or identify cyberattacks on SC in China.

The current state of the practice is key to providing a solid ground for understanding how cyberattacks on SCs are being used in practice. Several sources were consulted to identify the development of cyberattacks on SCs, including McAfee, Cisco Cybersecurity Report, Marsh Microsoft, Norton Cyber Insights, China Internet Network Information Center, Check Point Software Technologies Ltd, European Union Agency for Network and Information

Table 2 WoS articles included in this review

Author	Journal name	Journal impact factor (2020)	Citation count
(Ghadge *et al.*, 2020)	*Supply Chain Management-An International Journal*	9.012	18
(Duong *et al.*, 2020)	*Trends in Food Science & Technology*	12.563	3
(Ramirez-Pena *et al.*, 2020)	*Materials*	3.62	3
(Mageto, 2021)	*Sustainability*	3.25	0
(Manning, 2019)	*Trends in Food Science & Technology*	12.563	10
(Manantan, 2021)	*Australian Journal of International Affairs*	1.411	0
(Parenty and Domet, 2019)	*Harvard Business Review*	6.87	0
(Kshetri, 2017)	*Telecommunications Policy*	3.03	151
(Rodger and George, 2017)	*Journal of Cleaner Production*	9.29	32
(Boyson, 2014)	*Technovation*	6.60	31
(Urquhart and McAuley, 2018)	*Computer Law & Security Review*	2.98	21
(Colajanni *et al.*, 2018)	*International Transactions in Operational Research*	4.19	14
(Hassija *et al.*, 2021)	*IEEE Internet of Things Journal*	9.47	9
(Simon and Omar, 2020)	*European Journal of Operational Research*	5.33	9
(Gupta *et al.*, 2020)	*International Journal of Information Management*	14.09	8
(Kennedy *et al.*, 2019)	*Journal of Crime & Justice*	2.08	8
(Massimino *et al.*, 2018)	*Production and Operations Management*	4.96	8
(Gourisetti *et al.*, 2020)	*IEEE Transactions on Engineering Management*	6.14	7
(Oravec, 2017)	*Technology in Society*	4.19	5
(Alazab *et al.*, 2021)	*Cluster Computing–The Journal of Networks Software Tools and Applications*	1.80	4
(Li and Xu, 2021)	*International Journal of Production Research*	8.56	4
(Annarelli *et al.*, 2020)	*Computers & Industrial Engineering*	5.43	3
(Dehghani *et al.*, 2020)	*Journal of Business & Industrial Marketing*	3.46	2
(Woszczynski *et al.*, 2020)	*Government Information Quarterly*	7.27	2
(Etemadi *et al.*, 2021)	*Sustainability*	3.25	1
(Cheung *et al.*, 2021)	*Transportation Research Part E- Logistics and Transportation Review*	6.87	1
(Rosso *et al.*, 2020)	*New Media & Society*	8.06	1

Source: Author

Security (ENISA) and Pricewagterhouse Coopers (PwC). Popular supply chain platforms, such as information services group, supply chain (SC) Digital, CS Online, Inbound Logistics, Port Swigger and material handling and logistics were visited frequently to obtain the latest developments on the topic. This led to a list of promising initiatives for further discussion. This information from practice helped with our literature analysis and in identifying avenues for future research.

4.1 Inclusion decision based on title and keywords

Final articles were screened based on their title and keywords, and the author excluded articles not related to cyberattacks on SCs. The author then went through the abstracts of the excluded articles to ensure the inclusion of the most promising abstracts. In total, 253 articles for further screening were, thus identified.

4.2 Inclusion decision based on abstract

The author embarked upon an in-depth reading of the abstracts of these articles to filter out irrelevant ones. Although the search terms could be found in the text of the documents that were ultimately excluded, they did not focus on the topic directly. The author then validated the exclusion of the articles with an expert on the topic, to reach a

consensus before moving onto the next step. In total, 89 articles, thus remained for further screening.

4.3 Final selection

This stage involved an in-depth reading of the full text of all 89 articles to filter out irrelevant articles and ensure the inclusion of those focused on the core research topic. Here, the author used the following criteria to shortlist the articles:

- The paper should discuss "Cyberattacks" or "SC" or "SCM" or "China" as its core research topic.
- The *RO* of the paper should be related to "Cyberattacks" or "SC" or "SCM" or "China."

The output of this stage resulted in the identification of 27 articles. Descriptive database statistics: 27 Publications, cited 344 times and 324 without self-citation, 1 language, 25 journals, citing 321 articles and 313 without self-citations, average per item 10.75 and H-index 8. Top 5 WoS categories are as follows: Management and Operations Research Management Science with seven records each (21.21% of the total), Business and Engineering Industrial with five records (15.15%) and Information Science Library Science with four records (12.12%). Out of 14 countries, the USA is the most productive territory in terms of publications with 13 publications (59.37), Australia, England and Italy with three publications each (9.09%), Canada, India, China and Taiwan with two publications each (6.06%).

Only two articles analyzed cybersecurity in SC in China. The first one "Cybersecurity investments in a two-echelon supply chain with third-party risk propagation" (Li and Yu, 2021), proposed a game theory model to investigate cybersecurity investments with third-party risk propagation in a two-echelon SC and recommended some management insights to cybersecurity managers in SC. The second one is "Varieties of public-private co-governance on cybersecurity within the digital trade: implications from Huawei's 5G" (Huang *et al.*, 2021), presented how governments act on the cybersecurity concerns from Huawei's 5G which emphasized the importance of companies to participate in cybersecurity governance constructions within the digital trade system.

Table 3 shows the evolution of the selected publications in 2010–2021. The number of papers has increased through the years, from zero publications between 2010–2013 and 1 in 2014 to 13 in 2020, in 2021, 9 articles have been published.

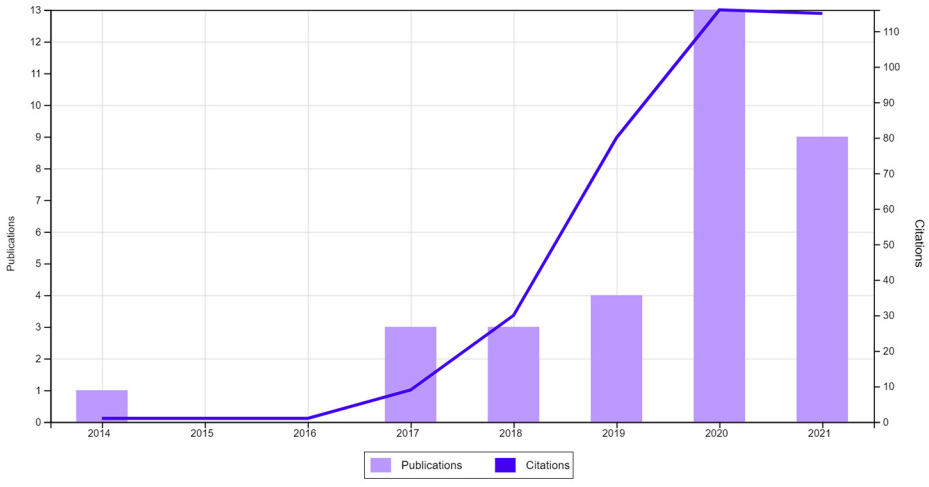
This research reveals the most cited documents in Clarivate Analytics (Figure 4). The most cited article *Blockchain's roles in strengthening cybersecurity and protecting privacy* (Kshetri, 2017), accounting for 151 citations, analyzed blockchain's roles in tracking the sources of insecurity in supply chains related to IoT devices. It also shows that regulators can make it obligatory for firms to deploy blockchain in SC, especially in national security systems. The second most cited article, "Triple bottom line accounting for optimizing natural gas sustainability: A statistical linear programming fuzzy Integrated linguistic operator

Table 3 Published papers by year (2010–2021)

Year	*Documents*	*% of total 27*
2020	10	31.25
2021	7	21.87
2019	3	9.37
2017	3	9.37
2018	3	9.37
2014	1	3.12

Source: Author

Figure 4 Times cited and publications over time (2010–July 2021)



Source: Clarivate Analytics (2021)

weighted average optimized sustainment model approach to reducing supply chain global cybersecurity vulnerability through information and communications technology" (Rodger and George, 2017), used triple bottom line accounting and considered threats to cybersecurity in the context of natural gas and global supply chain sustainability, and the third most cited article, "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems" (Boyson, 2014), focused on help practitioners and information technology (IT) executives to develop organizational assessment tools for CSCRM.

5. Discussion

Understanding cyberattacks on Chinese SCs is of utmost importance as businesses and SC practitioners consider the adoption of decision-making processes for gaining managerial insights into how cyberattacks have the potential to disrupt the global SC networks and help retailers and other businesses to overcome the multiple challenges on SC worsened by the global pandemic. One of the goals of this study is to assess cyberattacks on Chinese SCs and calls for global governance by using the TOE framework, which explains the process by which a firm adopts and implements technological innovations and how this is influenced by the technological, organizational and environmental context. The results show that the top five factors influencing the adoption process are as follows: relative advantage (RA) and technological readiness (Technology context); top management support and firm size (Organization context) and government policy and regulations (Environment context), all of which have differences in the manufacturing, health care, retail, wholesale and financial sectors.

Technology Context. *Relative Advantage:* RA relates to the "degree to which an innovation is perceived as being better than the idea it supersedes" (Gökalp *et al.*, 2020). In this work, RA refers to the positive influence on the performance of SCM in Chinese firms being cyberattacked. This is in good agreement with Oliveira *et al.* (2014) and with Gökalp *et al.* (2020). Firms showed benefits, such as an increase of productivity, and faster time responses to suppliers and consumers. RA from the Adoption of decision-making processes is more relevant for organizations in logistics, maritime (Mileski *et al.*, 2018) and manufacturing organizations (Huma *et al.*, 2021; Khaw *et al.*, 2021) than for those

organizations in the service industry. On a comparative note, Yeboah-Ofori *et al.* (2021), highlighted the following sectors as cyber vulnerable: Energy, Communication, Transport, Health-care and Manufacturing, and calls on cybersecurity to include the global delivery of physical goods plus the delivery of software. Organizations also need to tackle individual and driverless fleet delivery and full automation of the SC is also expected, which opens an additional avenue of research as more investigation is required on these new threats.

Technological Readiness: Our results are in complete agreement with Oliveira *et al.* (2014), Boyson (2014) and Ghadge *et al.* (2020). The stronger a company's technological infrastructure is and the more skilled workers it has, the more prepared will that organization be to mitigate cyber risks and cyberattacks. In their analysis, Oliveira *et al.* (2014) show that organizations with a robust technological infrastructure are better equipped and provide faster responses to cyberattacks. Boyson (2014) notes that cybersecurity is both *structural and technical*. Ghadge *et al.* (2020) reveals that skilled employees prevent and react better to cyberattacks, as they are in the front line of cybersecurity.

Organization Context. *Top Management Support.* With upper management fully committed, the planning and responses to cyberattacks on SC are better, faster and stronger. This study indicates that top-management-team security investments to fight against cyberattacks and managing cyber risks are of extreme importance, which is in good agreement with earlier findings. For instance, Goel *et al.* (2020) developed a framework to prioritize, resource, implement, standardize and monitor to help organizations to make decisions for cybersecurity risk assessment. Oliveira *et al.* (2014) also highlights the importance of financial and organizational support from top management to mitigate cyber risks. Boyson (2014) also reveals that CSCRM is relevant for executives, and company partners to strategically control cyber risks. Davis (2015) also reported how businesses can react and adopt measures as protection from cyberattacks on SC. The impact of cyberattacks on SC goes beyond the organization and may transfer to cities and countries, as it happened in China, or even to the complete continent. From a managerial standpoint, another important concept that emerges in this study is Cyber Third-Party Risk Management, which sheds light on the fact that risks for the organizations can come from inside the company and also from a third party, supplier or customer (Keskin *et al.*, 2021).

Firm Size is significant for organizations when dealing with cyberattacks on SC. The bigger the organization size is, the more resources are available to prevent and mitigate the risks it faces. Thus, large organizations react faster that small and medium-sized enterprises, which also has a positive influence in the firm's productivity (Gupta *et al.*, 2020b). Organization size is also related to financial resources, which large organizations count on to invest in new technologies against cyberattacks (Chana and Chong, 2013).

Environment Context. *Government Policy and Regulations.* As expected, our study reveals the importance of the Chinese Government's use of new technologies to regulate the Chinese cyber ecosystem and to protect cyber sovereignty. China has expedited important cybersecurity policies during the past few years and invested multiple resources to protect the nation and their society. This represents an important component in the trade and technological war against the USA (Gökalp *et al.*, 2020) and SC cybersecurity is a top priority on the Chinese Government's agenda. All organizations worldwide need to be aware and clearly understand these laws and policies and their international scope and geopolitical importance; all in all, they are the ones who benefit the most from data and customer protection, prevention of cybercrime and cyber defense regulations (Jiang, 2020).

5.1 Implications of cyber-attacks on supply chain

SCM in today's competitive world is increasingly challenging. The greater the uncertainties related to supply and demand, the higher the exposure to SC risk (Christopher and Towill, 2002; Ball and Waters, 2013; McAfee Center for Strategic and International Studies, 2014;

Boyson, 2014). China has also been a target, with over 80% of Chinese internet users falling victim to cyber-attacks at one time or another. In 2011, China exported US$508bn in ICT goods/services and had 1.1 billion internet users and 1.2 million 3 G mobile network users (The State Council, 2013; Simon and Omar, 2019).

Annual economic losses run into the tens of billions of US$ (Cai, 2013). This is a huge problem due to cyber-terrorist attacks that can disrupt a country's water and electricity supplies, telecommunications (severing its connections to the world) and national defenses (Herzog, 2011; Wortzel, 2011; Litvinenko, 2019). Thus, one way in which cyber attackers could disrupt a SC network is by targeting the power infrastructure (Jabbour and Devendorf, 2017; Heath *et al.*, 2020). These supply disruptions can have severe consequences, including massive financial losses (Li and Chen, 2020).

The multifaceted nature and vulnerability of SCs can also increase "confusion" related risks inside the SC (Zheng and Albert, 2019; Woszczynski *et al.*, 2020). These chaotic impacts result from over-response, superfluous intercessions, re-thinking, doubt and distorted data throughout the SC (Childerhouse *et al.*, 2003) This makes it hard to be receptive to clients, respond to changes in financial situations and provide proper client support. Lead times quoted to clients will generally be longer, as added security is required when sellers do not trust in the SC (Christopher and Lee, 2004) Consequently, it is important that nations implement measures to secure their economies, so organizations do not break down completely (Woszczynski *et al.*, 2020).

5.2 Chinese Government actions to mitigate cyberattacks on supply chain

President Xi stated in 2014 "Without cybersecurity, there is no national security." China's cyber strategy appears to be focused on attaining cyber sovereignty, and this purpose unifies the country's cyber activities (Kolton, 2017). China's cyberspace capabilities are analyzed through a strategic lens, and it is argued that their development will ensure its future rise to superpower status (Crosston, 2011; Hjortdal, 2017). Any cyber deterrence system must, therefore, be capable of overcoming the attribution problem to be relevant to the most important issue of all – state security (Crosston, 2011; Kallender and Hughes, 2016; Shackelford *et al.*, 2018). China is not a member of the Budapest Convention or Convention of Cybercrime, although, it is a member of the Shangai Cooperation Organization (SCO) of 2012, a signee of the World Intellectual Property Organization Copyright Treaty of 1985 and the UN Convention against Transnational Organized Crime of 2000 (Jiang, 2020).

Global governments may benefit if mirroring China's strategies to mitigate cyberattacks on SC is to properly design facilities for the new SC networks or fortify existing SC networks. Risk diversification, by working with multiple suppliers, provides decision-makers with greater flexibility for handling disruptions. Backup emergency equipment can help mitigate the impact of disruptive events. Backup suppliers can be used to cover potentially unmet demand or provide substitute products or production processes (Ni *et al.*, 2018). Backup resources can include generators, employees to perform repairs and square credit card processing systems (Jabbour and Devendorf, 2017; Radanliev *et al.*, 2020).

The Chinese Government continues to raise awareness on the importance of cybersecurity in the country, aiming to protect serious economic infrastructure against cybercrime (Ikenson, 2017), and to safeguard from external cyber terrorism through the SCO (Jiang, 2020).

But it is not only the Chinese Government, military, civilians and public organizations that are developing cyber strategies. Private organizations are getting more involved in the creation of private cybersecurity policies (Brenner and Lindsay, 2015). Nations around the world should collaborate and develop international policies/norms. This could help reduce the impact of cyberattacks on SC business sectors (Cheung *et al.*, 2021).

The evolution of cybercrime in recent years has led to AI being added to the quest for cybersecurity. This is a new technological tool that can help with "sustainable, rapid and viable regional development." The Chinese Government's use of AI could help detect, track and fight cybercrime and it will bring more value to governments and private organizations by "focusing on more valuable security tasks" (Mosteanu, 2020). AI arises as one of the latest global defense capabilities, a field of high importance for China which set the goal to become the "world leading" science and technology power by 2049 (Gill, 2016; Segal, 2020) and is key when it comes to national defense, specifically for The USA, Russia and China which have openly informed their developing military technologies (Sharikov, 2018), China also uses AI for economic, political and strategic objectives (Johnson, 2019; Segal, 2020), however, Chinese companies' expenditure in cybersecurity is still far from the US's (Chinese companies estimate to spend US$7.3bn, 9 times less than US companies) (Nathan, 2015; Qi *et al.*, 2018; Sharikov, 2018; Segal, 2020).

China seeks to increase its control of domestic internet activity and the information traversing it and uses strict mandates to protect Chinese businesses from foreign competition [. . .] In other words, Beijing is guaranteeing its self-declared right to cyber sovereignty, a concept that is still contested within the international community (Chopra *et al.*, 2007; Patterson, 2011; Iasiello, 2017; Yang and Xu, 2018; Yu, 2017). Another attractive solution China has found to this issue is monitoring communications network platforms communication for malicious activity to achieve improved cybersecurity (Hayden *et al.*, 2004; Nathan, 2012).

Cyberattacks on China also include cyber espionage, cyberattacks for political and military gain, cyber assaults and cyberattacks on SC, increasing its concern for the cyber-SC (Jabbour and Poisson, 2016). The Standing Committee of the National People's Congress has also expedited cybersecurity laws and regulations (Cyberattacks on SC in China – Laws and Regulations).

Cyberattacks on SC in China – Laws and Regulations as follow:

- Regulations for the Security and Protection of Computer Information Systems, Administrative Measures for Internet Information Services.
- Administrative Measures for the Prevention and Treatment of Computer Viruses.
- Administrative Measures for the Hierarchical Information Security Protection.
- Law on Guarding State Secrets.
- The Cybersecurity Law.
- Cybersecurity Review Measures.
- Security Review Measures for Network Products and Services.
- National Emergency Response Plan for Cybersecurity Incidents.
- Provisions for the Protection of Children's Personal Information Online.
- Information Security Technology-Baseline for Classified Cybersecurity Protection.
- Information Security Technology-Evaluation Requirements for Classified Cybersecurity Protection.
- Information Security Technology-Technical Requirements for Classified Cybersecurity Protection Security Design.
- The National Program for Key Basic Research and Development (R&D). Includes research on information security.
- The Outline of National Medium- and Long-Term Plan for Science and Technology Development (2006–2020). Includes three out of 16 cyber-related megaprojects.

- The National Program for Key Basic R&D. Includes research on information security.
- The National Program for High-Tech R&D, which prioritizes network and information security.
- The National Security Law.
- Counterterrorism Law.
- Multi-level Protection System.

Source: Author.

In 2020, China also expedited Measures for Cybersecurity Review, which requires critical operators to pass a cybersecurity (which takes between 45–105 days), for security and SC reliability purposes, and to ascertain if their products, services and sectors (see examples below) pose an unacceptable risk to China's security: *Products and Services:* "core network equipment, high-performance computers and servers, large-capacity storage devices, large-scale databases and application software, cybersecurity equipment, cloud computing services," *and others affecting Critical Information Infrastructure-CII security (Article 20). Sectors:* "important network and information system operators in sectors and areas including telecommunications, radio and television, energy, finance, road and water transport, railroads, civil aviation, post, water management, emergency management, hygiene and healthcare, social security, national defence science, technology and industry, etc."

As a reply, the USA imposed stronger restrictions on US products selling to China. Business and practitioners dealing with China must assess all these measures to prevent supply disruptions to Chinese customers. Decisions from both governments continue increasing the level of uncertainty among suppliers when interacting with Chinese customers. The Chinese Government has also dealt with multiple anticompetitive interventions from the USA, such as the Cyberspace Solarium Commission, which seeks to reduce dependency on Chinese suppliers, specifically the tech SC, and calls for international allies to counter China's tech influence worldwide, especially in the wireless 5 G market.

The new agencies, the Cyberspace Administration of China, as well as the Central Commission for Cybersecurity and Information, established by President Xi Jinping, show how relevant and sensitive this field is for China. However, this should not be a governmental issue only, it also needs to involve industry groups, trade associations, manufacturers, service providers and consumers, that approach will increase the level of trust of SC (Feng, 2019; Kshetri and Voas, 2019).

All these China SC cyber measures and the Cybersecurity Review Office incorporate China's legitimate worry about foreign interference, which are appropriate in the cyberwarfare era and can still improve by expediting supporting official regulations to achieve clarification on cyber review protocols. Nonetheless, non-official documents have regulated this (e.g. Notice Concerning Critical Information Infrastructure Security Protection Work-Related Issues –《关于关键信息基础设施安全保护工作有关事项的通知》*).* These SC cyber measures pose two risk factors: "the security, openness, transparency, and diversity of sources of products and services" and "the risk of supply disruptions due to political, diplomatic, and trade factors".

Uncertainty for suppliers is, also, of extreme interest from a managerial perspective due to the implications in the SC. Practitioners need to be completely aware that all goods and services to enter the Chinese market are under scrutiny mandatorily and businesses ought to clearly understand that additional risks of intellectual property and trade secrets may be revealed during the reviews while the Chinese Government must continue ensuring that such measures are conducted fast and under transparent guidelines to prevent the supply

of goods and services from being interrupted, and specially, to persist with its basic national policy of welcoming all foreign products.

The challenge also raises for Chinese suppliers themselves, particularly for those who use foreign components to operate, as they also have to go through the cybersecurity review and may also consider using and favoring local providers to expedite the review process. In fact, China has developed an ecosystem with world-class firms, such as Huawei, ZTE, Alibaba, Tencent, Baidu and TikTok (Jiang, 2020).

6. Conclusions

Technology and the internet are both very advanced, and the implementation of new national security policies becomes increasingly important and necessary (Manantan, 2021). Governments, large companies, and consumers store information on these technological platforms. This has given rise to a new method of sabotage known as a cyberattack, which seeks to harm the economy of a country by leaking confidential information and as studied in this article, altering the infrastructure of SCs, thus creating obstacles to international trade.

In this study, all the above was looked at from the perspective of China, cyber-ambitious and cyber-vulnerable (Jiang, 2020). This country is widely seen as the next great world power, and, as such, it is a constant victim of cyberattacks that seek to destabilize its economy and achieve supremacy in international trade. Therefore, China is a pioneering country in that it seeks to raise awareness of the importance and transcendence of cybersecurity (Nathan, 2012; Peng, 2015; Lim and Taeihagh, 2018) and SC cybersecurity is a top priority on the Chinese Government's agenda. Chinese cyber ecosystem is robust and unique in its kind able to compete against the USA (Jiang, 2020).

From a managerial standpoint, findings can help practitioners understand the risks and challenges presented by cyberattacks on global SC networks, specifically in China. This article pinpoints areas where cyberattacks disrupt SCs and aims to provide guidance to managers in formulating initiatives to minimize risks, thus mitigating the effects of cyberattacks on SCs.

SCs play a key role in international trade and cyberattacks on both physical and ICT SCs threaten sensitive information belonging to SC participants, including suppliers, companies and consumers (Svenungsen, 2019; Vakulchuk *et al.*, 2020). Multiple strategies have been implemented to reduce security demands (e.g. security of computers, devices or systems; data protection capabilities; cyber risk controls using cybersecurity standards or cybersecurity policies and procedures). AI appears as a potent tool to fight in a faster, better way against cyberattacks.

The globalization of the cyber SC makes this a global matter requiring multilateral collaboration (Bousfield, 2017; Ayson, 2020; Fracalossi de Moraes, 2020), in our current geopolitical environment. In this regard, China works closely with a wide variety of countries including Australia, the UK, France, with Brazil, Russia, India, China and South Africa countries drafted the resolution "Strengthening International Cooperation to Combat Cybercrime" (Mu and Yonggang, 2014) among others. This is a new era that differs from previous ones like the Cold War or the Nuclear age in that now there are no rules, policies, or norms, making cybersecurity threats even more dangerous. No organization, government or individual is immune to cyberattacks, and this is especially true for SCs where the threat is evolving daily. At this point, all SC players have understood its magnitude and severity, so coordinated work between all actors is key for fighting against cyberattacks and being attuned to the latest threats (Check Point Software Technologies, 2019) to safeguard organizations and national security, especially during the ongoing technology-trade war between The USA and China.

6.1 Additional recommendations to prevent cyberattacks on supply chain are listed as follows

- Organizations need to assess the cybersecurity maturity of their suppliers as recent cyberattacks on SC come through third parties.
- Suppliers must ensure that all their products and services comply with globally accepted cybersecurity practices.
- Organizations must permanently monitor all cybersecurity vulnerabilities, both internal and external, by using a Vulnerability Scoring System to analyze cyber risks becomes a valuable management tool to mitigate cyber risks.
- At the industry level, we found some key initiatives that are worth replicating and are useful for all actors of SC: SC Levels for Software Artifacts, launched by Google in 2001 focused on software SC attacks, and *The MITRE D3FEND project,* a framework used by organizations to prevent specific attacks and raise security levels in firms (ENISA, 2021).
- Organizations must protect the users' privacy as part of their social responsibility and when possible, increase their investment in R&D to mitigate cyber risks on SC.

7. Limitations and avenues for future research

This study applied SSCI criteria due to the quality of the journals included thereunder. Future studies could expand data collection to other types of databases to include the latest findings in the field, as well as include Chinese Judicial opinions and administrative regulations. Future research could also compare how other countries are managing cyberattacks on their SCs to add external validity to the study. Our study only focused on adoption decisions (main construct). To obtain a holistic comprehension of cyberattacks on SC, adoption of core process technology and adoption of technology by the group should both be examined. China is an industrialized/unique country. Consequently, one future research direction is to compare cyberattacks on SC in industrialized countries with non-industrialized ones; another possible direction is to design a longitudinal study studying single focal companies. The TOE framework offers valuable insights for practitioners and academics and future work could combine the TOE framework with other theories, such as individual factors in adoption (Premkumar, 2003); the TAM (Davis, 1989); diffusion of innovations (Rogers, 1995) or real options (Black and Scholes, 1973). Other promising topics to study are Cyberdiplomacy and Cyber sovereignty, these would highlight challenges and lessons for the government from both developing and developed countries.

References

Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T. and Baskerville, R.L. (2021), "How can organizations develop situation awareness for incident response: a case study of management practice", *Computers & Security*, Vol. 101, p. 102122.

Al Hadwera, A., Tavana, M., Gillis, D. and Rezania, D. (2021), "A systematic review of organizational factors impacting cloud-based technology adoption using Technology-organization-environment framework", Internet of Things, 100407.

Alazab, M., Alhyari, S., Awajan, A. and Abdallah, A.B. (2021a), "Blockchain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance", *Cluster Computing*, Vol. 24 No. 1, pp. 83-101.

Alazab, M., Lakshmanna, K., Reddy, T., Pham, Q.V. and Maddikunta, P.K.R. (2021b), "Multi-objective cluster head selection using fitness averaged rider optimization algorithm for IoT networks in smart cities", *Sustainable Energy Technologies and Assessments*, Vol. 43, p. 100973.

Alzubaidi, A. (2021), "Cybercrime awareness among Saudi nationals: dataset", *Data in Brief*, Vol. 36, June 2021, Article number 106965.

Annarelli, A., Nonino, F. and Palombi, G. (2020), "Understanding the management of cyber resilient systems", *Computers & Industrial Engineering*, Vol. 149, p. 106829.

Ariffin, K.A.Z. and Ahmad, F.H. (2021), "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0", *Computers & Security*, Vol. 105, p. 102237.

Austin, G. (2016), *China, and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, New York, NY, p. 398, 2015, The China Journal, 75, 161–163.

Ayson, R. (2020), "New Zealand and the great irresponsibles: coping with Russia, China, and the US", *Australian Journal of International Affairs*, pp. 1-24.

Baker, J. (2011), "The technology–organization–environment framework", *Integrated Series in Information Systems*, pp. 231-245.

Ball, D. and Waters, G. (2013), "Cyber defence and warfare", *Security Challenges*, Vol. 9 No. 2, pp. 91-98.

Bambauer, D. (2014), "Ghost in the network", *University of Pennsylvania Law Review*, Vol. 162 No. 5, pp. 1011-1091.

Bandaly, D., Shanker, L., Kahyaoglug, Y. and Satir, A. (2013), "Supply chain risk management – II: a review of operational, financial and integrated approaches", *Risk Management*, Vol. 15 No. 1, pp. 1-31.

Bellabona, P. and Spigarelli, F. (2007), "Moving from open door to go global: China goes on the world stage", *International Journal of Chinese Culture and Management*, Vol. 1 No. 1, p. 93.

Black, F. and Scholes, M. (1973), "The pricing of options and corporate liabilities", *Journal of Political Economy*, Vol. 81 No. 3, pp. 637-654.

Blackwood-Brown, C., Levy, Y. and D'Arcy, J. (2021), "Cybersecurity awareness and skills of senior citizens: a motivation perspective", *Journal of Computer Information Systems*, Vol. 61 No. 3, pp. 195-206.

Bousfield, D. (2017), "Revisiting cyber-diplomacy: Canada–China relations online", *Globalizations*, Vol. 14 No. 6, pp. 1045-1059.

Boyson, S. (2014), "Cyber supply chain risk management: revolutionizing the strategic control of critical IT systems", *Technovation*, Vol. 34 No. 7, pp. 342-353.

Brookson, C., Cadzow, S., Eckmaier, R., Eschweiler, J., Gerber, B., Guarino, A., Rannenberg, K., Shamah, J. and Górniak, S. (2016), "Definition of cybersecurity - gaps and overlaps in standardization", available at: www-enisa-europa-eu.ezproxy.usal.es/publications/definition-of-cybersecurity

Buil-Gil, D., Miró-Linares, F., Moneva, A., Kemp, S. and Díaz-Castano, N. (2021), "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK", *European Societies*, Vol. 23 No. sup1, pp. S47-S59.

Cai, M. (2013), "Making joint efforts to maintain cyber security (keynote at the 4th world cyberspace cooperation summit)", available at: http://politics.people.com.cn/n/2013/1106/c1001-23443428.html

Cascavilla, G., Tamburri, D. and Van Den Heuvel, W. (2021), "Cybercrime threat intelligence: a systematic multi-vocal literature review", *Computers and Security*, Vol. 105, June 2021, Article number 102258.

Chana, F. and Chong, A. (2013), "Determinants of mobile supply chain management system diffusion: a structural equation analysis of manufacturing firms", *International Journal of Production Research*, Vol. 51 No. 4, pp. 1196-1213.

Chandra, A. and Snowe, M. (2020), "A taxonomy of cybercrime: theory and design", *International Journal of Accounting Information Systems*, Vol. 38, p. 100467.

Chau, P. and Tam, K. (1997), "Factors affecting the adoption of open systems: an exploratory study", *MIS Quarterly*, Vol. 21 No. 1, pp. 1-24.

Check Point Software Technologies (2019), "Cyberattack trends: 2019- mid year report", available at: www.checkpoint.com/downloads/resources/cyber-attack-trends-mid-year-report-2019.pdf

Cheung, K., Bell, M. and Bhattacharjya, J. (2021), "Cybersecurity in logistics and supply chain management: an overview and future research directions", *Transportation Research Part E: Logistics and Transportation Review*, Vol. 146, p. 102217, ISSN 1366-5545.

Childerhouse, P., Hermiz, R., Mason-Jones, R., Popp, A. and Towill, D. (2003), "Information flow in automotive supply chains – present industrial practice", *Industrial Management and Data Systems*, Vol. 103 No. 3, pp. 137-149.

China Internet Network Information Center (2017), available at: www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/202004/P020200428399188064169.pdf (2020).

Cho, Y. and Chung, J. (2017), "Bring the state back in: conflict and cooperation among states in cybersecurity", *Pacific Focus*, Vol. 32 No. 2, pp. 290-314.

Choo, K., Gai, K., Chiaraviglio, L. and Yang, Q. (2021), "A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management", *Computers and Security*, Vol. 102, p. 102136.

Chopra, S., Reinhardt, G. and Mohan, U. (2007), "The importance of decoupling recurrent and disruption risks in a supply chain", *Naval Research Logistics*, Vol. 54 No. 5, pp. 544-555.

Christopher, M. and Lee, H. (2004), "Mitigating supply chain risk through improved confidence", *International Journal of Physical Distribution and Logistics Management*, Vol. 34 No. 5, pp. 388-396.

Christopher, M. and Towill, D. (2002), "An integrated model for the design of agile supply chains", *International Journal of Physical Distribution and Logistics Management*, Vol. 31 No. 4, pp. 262-264.

Cisco Annual Cybersecurity Report (2020), "Cisco cybersecurity report series 2020", available at: www.newhorizons.com/Portals/278/Downloads/Final_Cisco_2020_ACR_WEB.pdf

Colajanni, G., Daniele, P., Giuffrè, S. and Nagurney, A. (2018), "Cybersecurity investments with nonlinear budget constraints and conservation laws: variational equilibrium, marginal expected utilities, and Lagrange multipliers", *International Transactions in Operational Research*, Vol. 25 No. 5, pp. 1443-1464.

Crosston, M. (2011), "World gone cyber MAD: how 'mutually assured debilitation' is the best hope for cyber deterrence", *Strategic Studies Quarterly*, Vol. 5 No. 1, pp. 100-116.

Cui, Y., Kara, S. and Chan, K.C. (2020), "Manufacturing big data ecosystem: a systematic literature review", *Robotics and Computer-Integrated Manufacturing*, Vol. 62, p. 101861.

Dahabiyeh, L. (2021), "Factors affecting organizational adoption and acceptance of computer-based security awareness training tools", *Information and Computer Security*, ISSN: 2056-4961.

Daniels, N. and Jokonya, O. (2020), "Factors affecting digital transformation in the retail supply chain", *International Conference on Management, Business, Economics and Accounting (ICMBEA)*, ISBN: 978-99949-0-615-4.

Darko, G. and Boris, G. (2017), "Cybersecurity and cyber defence: national level strategic approach", *Automatika Journal for Control, Measurement, Electronics, Computing and Communications*, Vol. 58 No. 3, pp. 273-286.

Dashora, K. (2011), "Cyber crime in the society: problems and preventions", *Journal of Alternative Perspectives in the Social Sciences*, Vol. 3 No. 1, pp. 240-259.

Davis, F. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No. 3, pp. 319-333.

Davis, A. (2015), "Building cyber-resilience into supply chains", *Technology Innovation Management Review*, Vol. 5 No. 4.

Dehghani, M., Mashatan, A. and Kennedy, R.W. (2020), "Innovation within networks–patent strategies for blockchain technology", *Journal of Business & Industrial Marketing*.

Deibert, R. (2011), "Tracking the emerging arms race in cyberspace", *Bulletin of the Atomic Scientists*, Vol. 67 No. 1, pp. 1-8.

DePietro, R., Wiarda, E. and Fleischer, M. (1990), "The context for change: organization, technology and environment", in Tornatzky, L.G. and Fleischer, M. (Eds), *The Process of Technological Innovation*, Lexington Books, Lexington, MA, pp. 151-175.

Duong, L.N., Al-Fadhli, M., Jagtap, S., Bader, F., Martindale, W., Swainson, M. and Paoli, A. (2020), "A review of robotics and autonomous systems in the food industry: from the supply chains perspective", *Trends in Food Science & Technology*.

ENISA (2021), "ENISA threat landscape for supply chain attacks", European Union Agency for Cybersecurity, ISBN: 978-92-9204-509-8.

Etemadi, N., Van Gelder, P. and Strozzi, F. (2021), "An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity", *Sustainability*, Vol. 13 No. 9, p. 4672.

Everstream Analytics (2021), "Everstream analytics: annual risk report 2021", available at: www.everstream.ai/wp-content/uploads/2021/03/20210323-Everstream-Analytics-Annual-Risk-Report.pdf

Feng, Y. (2019), "The future of China's personal data protection law: challenges and prospects", *Asia Pacific Law Review*, pp. 1-21.

Fosso Wamba, S., Kala Kamdjoug, J.R., Epie Bawack, R. and Keogh, J.G. (2018), "Bitcoin, blockchain, and FinTech: a systematic review and case studies in the supply chain", *Production Planning and Control*, Forthcoming.

Fracalossi de Moraes, R. (2020), "Whither security cooperation in the BRICS? Between the protection of norms and domestic politics dynamics", *Global Policy*.

Ghadge, A., Weiß, M., Caldwell, N.D. and Wilding, R. (2020), "Managing cyber risk in supply chains: a review and research agenda", *Supply Chain Management*, Vol. 25 No. 2, pp. 223-240.

Gilal, F., Jian, Z., Paul, J. and Gilal, N. (2018), "The role of self-determination theory in marketing science: an integrative review and agenda for marketing research", *European Management Journal*.

Gill, B. (2016), "The United States and Asia in 2015: across the region, US-China competition intensifies", *Asian Survey*, Vol. 56 No. 1, pp. 8-18.

Gjesvik, L. and Overbo, E. (2019), "Deter who? The importance of strategic culture for cybersecurity", *Internasjonal Politikk*, Vol. 77 No. 3, pp. 278-287.

Goel, R., Kumar, A. and Haddow, J. (2020), "PRISM: a strategic decision framework for cybersecurity risk assessment", *Information & Computer Security*.

Golmohammadi, A. and Hassini, E. (2020), "Review of supplier diversification and pricing strategies under random supply and demand", *International Journal of Production Research*, pp. 1-33.

Gökalp, E., Gökalp, M. and Çoban, S. (2020), "Blockchain-based supply chain management: understanding the determinants of adoption in the context of organizations", *Information Systems Management*, pp. 1-22.

Goodhue, D. and Thompson, R. (1995), "Task-technology fit and individual performance. Engineering, computer science", *MIS Quarterly*, pp. 213-236.

Gourisetti, S.N.G., Mylrea, M. and Patangia, H. (2019), "Evaluation and demonstration of blockchain applicability framework", *IEEE Transactions on Engineering Management*, Vol. 67 No. 4, pp. 1142-1156.

Gupta, P., Chauhan, S., Paul, J. and Jaiswal, M. (2020a), "Social entrepreneurship research: a review and future research agenda", *Journal of Business Research. Elsevier*, Vol. 113, pp. 209-229.

Gupta, S., Meissonier, R., Drave, V. and Roubaud, D. (2020b), "Examining the impact of cloud ERP on sustainable performance: a dynamic capability view", *International Journal of Information Management*, Vol. 51, article number 102028.

Hang, N. (2017), "The rise of China: challenges, implications, and options for the United States", *Indian Journal of Asian Affairs*, Vol. 30 Nos 1/2, pp. 47-64.

Harfouche, A. and Robbin, A. (2015), "E-government", *Wiley Encyclopedia of Management*, John Wiley and Sons, Ltd, available at: www.researchgate.net/profile/AliceRobbin/publication/319615017_EGovernment/links/5c1aa7d192851c22a3381630/E-Government.pdf

Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R. (2021), "Evaluating the cyber security readiness of organizations and its influence on performance", *Journal of Information Security and Applications*, Vol. 58, p. 102726.

Hassija, V., Chamola, V., Gupta, V., Jain, S. and Guizani, N. (2020a), "A survey on supply chain security: application areas, security threats, and solution architectures", *IEEE Internet of Things Journal*, pp. 1-1.

Hassija, V., Chamola, V., Krishna, D.N.G., Kumar, N. and Guizani, M. (2020b), "A blockchain and edge-computing-based secure framework for government tender allocation", *IEEE Internet of Things Journal*, Vol. 8 No. 4, pp. 2409-2418.

Hayden, P., Woolrich, D. and Sobolewski, K. (2004), "Providing cyber situational awareness on defense platform networks", *The Cyber Defense Review*, Vol. 2 No. 2, pp. 125-140.

Heath, E., Mitchell, J. and Sharkey, T. (2020), "Models for restoration decision making for a supply chain network after a cyber-attack", *Journal of Defense Modeling and Simulation*, Vol. 17 No. 1, pp. 5-19.

Herzog, S. (2011), "Revisiting the Estonian cyber attacks: digital threats and multinational responses", *Journal of Strategic Security*, Vol. 4 No. 2, pp. 49-60.

Hjortdal, M. (2017), "China's use of cyber warfare: espionage meets strategic deterrence", *Journal of Strategic Security*, Vol. 4 No. 2, pp. 1-24.

Huma, Z., Latif, S., Ahmad, J., Idrees, Z., Ibrar, A., Zou, Z., Alqahtani, F. and Baothman, F. (2021), "A hybrid deep random neural network for cyberattack detection in the industrial internet of things", *IEEE Access*, Vol. 9, pp. 55595-55605.

Huang, Y., Liu, S., Zhang, C., You, X. and Wu, H. (2021), "True-data testbed for 5G/B5G intelligent network", *Intelligent and Converged Networks*, Vol. 2 No. 2, pp. 133-149.

Iasiello, E. (2017), "China's cyber initiatives counter international pressure", *Journal of Strategic Security*, Vol. 10 No. 1, pp. 1-16.

Ikenson, D. (2017), "Cybersecurity or protectionism? Defusing the most volatile issue in the US-China relationship", Cato Institute Policy Analysis, (815).

Jabbour, K. and Devendorf, E. (2017), "Cyber threat characterization", *The Cyber Defense Review*, Vol. 2 No. 3, pp. 79-94.

Jabbour, K. and Poisson, J. (2016), "Cyber risk assessment in distributed information systems", *The Cyber Defense Review*, Vol. 1 No. 1, pp. 91-112.

Jang-Jaccard, J. and Nepal, S. (2021), "A survey of emerging threats in cybersecurity", *Journal of Computer and System Sciences*, Vol. 80 No. 5, pp. 973-993, August 2014.

Jiang, M. (2020), "Cybersecurity policies in China. CyberBRICS: cybersecurity regulations in BRICS countries.Ch.5", pp. 195-212.

Johnson, J. (2019), "Artificial intelligence and future warfare: implications for international security", *Defense and Security Analysis*, Vol. 35 No. 2, pp. 147-169.

Jüttner, U., Peck, H. and Christopher, M. (2003), "Supply chain risk management: outlining an agenda for future research", *International Journal of Logistics Research and Applications*, Vol. 6 No. 4, pp. 197-210.

Kallender, P. and Hughes, C. (2016), "Japan's emerging trajectory as a 'cyber power': from securitization to militarization of cyberspace", *Journal of Strategic Studies*, Vol. 40 Nos 1/2, pp. 118-145.

Karjalainen, M., Siponen, M., Puhakainen, P. and Sarker, S. (2019), "Universal and culture-dependent employee compliance of information systems security procedures", *Journal of Global Information Technology Management*, Vol. 23 No. 1, pp. 5-24.

Kaspersky (2021), "Incident response analyst report", available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/09/13085018/Incident-Response-Analyst-Report-eng-2021.pdf

Kennedy, J., Holt, T. and Cheng, B. (2019), "Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking", *Journal of Crime and Justice*, Vol. 42 No. 5, pp. 632-645.

Keskin, O., Caramancion, K., Tatar, I., Raza, O. and Tatar, U. (2021), "Cyber third-party risk management: a comparison of non-intrusive risk scoring reports", *Electronics*, Vol. 10 No. 10, article number 1168.

Khaw, Y., Jahromi, A., Arani, M., Sanner, S., Kundur, D. and Kassouf, M. (2021), "A deep learning-based cyberattack detection system for transmission protective relays", *IEEE Transactions on Smart Grid*, Vol. 12 No. 3, pp. 2554-2565.

Kokas, A. (2018), "Platform patrol: China, the United States, and the global battle for data security", *The Journal of Asian Studies*, Vol. 77 No. 4, pp. 923-933.

Kolton, M. (2017), "Interpreting China's pursuit of cyber sovereignty and its views on cyber deterrence", *The Cyber Defense Review*, Vol. 2 No. 1, pp. 119-154.

Kshetri, N. (2013), "Cyber-victimization and cybersecurity in China", *Communications of the ACM*, Vol. 56 No. 4, p. 35.

Kshetri, N. and Voas, J. (2019), "Supply chain trust", *IT Professional*, Vol. 21 No. 2, pp. 6-10.

Kuan, K. and Chau, P. (2001), "A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework", *Information Management*, Vol. 38 No. 8, pp. 507-521.

Kumar, V.S., Prasad, J. and Samikannu, R. (2018), "A critical review of cyber security and cyber terrorism–threats to critical infrastructure in the energy sector", *International Journal of Critical Infrastructures*, Vol. 14 No. 2, pp. 101-119.

Lee, C. and Shim, J. (2007), "An exploratory study of radio frequency identification (RFID) adoption in the healthcare industry", *European Journal of Information Systems*, Vol. 16 No. 6, pp. 712-724.

Li, X. and Chen, Y. (2020), "Impacts of supply disruptions and customer differentiation on a partial-back ordering inventory system", *Simulation Modelling Practice and Theory*, Vol. 18 No. 5, pp. 547-557.

Li, Y. and Xu, L. (2021), "Cybersecurity investments in a two-echelon supply chain with third-party risk propagation", *International Journal of Production Research*, Vol. 59 No. 4, pp. 1216-1238.

Lim, H. and Taeihagh, A. (2018), "Autonomous vehicles for smart and sustainable cities: an in-Depth exploration of privacy and cybersecurity implications", *Energies*, Vol. 11 No. 5, p. 1062.

Lindsay, J. (2015), "The impact of China on cybersecurity: fiction and friction", *International Security*, Vol. 39 No. 3, pp. 7-47.

Lindsay, J., Cheung, T. and Reveron, D. (2015), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, USA.

Litvinenko, V. (2019), "Digital economy as a factor in the technological development of the mineral sector", *Natural Resources Research*.

Li, H., Yu, L. and He, W. (2019), "The impact of GDPR on global technology development", *Journal of Global Information Technology Management*, pp. 1-6.

Li, X., Cui, X., Li, Y., Xu, D. and Xu, F. (2021), "Optimisation of reverse supply chain with used-product collection effort under collector's fairness concerns", *International Journal of Production Research*, Vol. 59 No. 2, pp. 652-663.

Lu, T., Guo, X., Xu, B., Zhao, L., Peng, Y. and Yang, H. (2013), "Next big thing in big data: the security of the ICT supply chain", *2013 International Conference on Social Computing*, Alexandria, VA, pp. 1066-1073.

McAfee Center for Strategic and International Studies (2014), "Net losses: estimating the global cost of cyber-crime", Last modified December 17, available at: www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Macedo, E., De Oliveira, E., Silva, F., De Rezende, J. and De Moraes, L. (2019), "On the security aspects of internet of things: a systematic literature review", *Journal of Communications and Networks*, Vol. 21 No. 5, pp. 444-457, 8854272.

Mageto, J. (2021), "Big data analytics in sustainable supply chain management: a focus on manufacturing supply chains", *Sustainability*, Vol. 13 No. 13, p. 7101.

Manantan, M.B.F. (2021), "Advancing cyber diplomacy in the Asia Pacific: Japan and Australia", *Australian Journal of International Affairs*, Vol. 75 No. 4, pp. 432-459.

Mangan, J. and Lalwani, C. (2016), *Global Logistics and Supply Chain Management*, John Wiley & Sons.

Marsh Microsoft Global Cyber Risk Perception Survey (2019), available at: www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

Massimino, B., Gray, J.V. and Lan, Y. (2018), "On the inattention to digital confidentiality in operations and supply chain research", *Production and Operations Management*, Vol. 27 No. 8, pp. 1492-1515.

Mileski, J., Clot, C. and Galvao, C. (2018), "Cyberattacks on ships: a wicked problem approach", *Maritime Business Review*, Vol. 3 No. 4, pp. 414-430.

Minnaar, A. (2017), "Cybercrime, cyberattacks, and problems of implementing organizational cybersecurity. Global issues in contemporary policing".

Mishra, A.N., Konana, P. and Barua, A. (2007), "Antecedents and consequences of internet use in procurement: an empirical investigation of US manufacturing firms", *Information Systems Research*, Vol. 18 No. 1, pp. 103-120.

Mitchell, V.-W. (1995), "Organisational risk perception and reduction: a literature review", *British Journal of Management*, Vol. 6 No. 2, pp. 115-133.

Monczka, R.M., Handfield, R.B., Giunipero, L.C. and Patterson, J.L. (2015), *Purchasing and Supply Chain Management*, Cengage Learning.

Mosteanu, N. (2020), "Artificial intelligence and cybersecurity-face to face with cyberattack a maltese case of risk management approach", *Ecoforum Journal*, Vol. 9 No. 2.

Mu, R. and Yonggang, F. (2014), "Security in the cyber supply chain: a Chinese perspective", *Technovation*, Vol. 34 No. 7.

Nanda, S. and Nanda, S. (2021), "Blockchain adoption in health market: a system thinking and modelling approach", *Journal of Asia Business Studies*, ISSN: 1558-7894.

Nathan, A. (2012), "Cibersecurity and US-China relations", *Foreign Affairs*, Vol. 91 No. 5, pp. 203-204.

Nathan, A. (2015), "China, and cybersecurity: espionage, strategy, and politics in the digital domain", *Foreign Affairs*, Vol. 94 No. 6, pp. 174-176.

Neutze, J. and Nicholas, J. (2013), "Cyber insecurity: competition, conflict, and innovation demand effective cyber security norms", *Georgetown Journal of International Affairs*, pp. 3-15.

Ni, N., Howell, B. and Sharkey, T. (2018), "Modeling the impact of unmet demand in supply chain resiliency planning", *Omega (United Kingdom)*, Vol. 81, pp. 1-16.

NortonLifeLock Cyber Safety Insights Report (2019), available at: https://now.symassets.com/content/dam/norton/campaign/NortonReport/2020/2019_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf?promocode=DEFAULTWEB

Oliveira, T., Thomas, M. and Espadanal, M. (2014), "Assessing the determinants of cloud computing adoption: analysis of the manufacturing and services sectors", *Information & Management*, Vol. 51, pp. 497-510.

Oravec, J.A. (2017), "Kill switches, remote deletion, and intelligent agents: framing everyday household cybersecurity in the internet of things", *Technology in Society*, Vol. 51, pp. 189-198.

Pandey, S., Kumar, R., Gunasekaran, A. and Kaushik, A. (2019), "Cyber security risks in globalized supply chains: conceptual framework", *Journal of Global Operations and Strategic Sourcing*, Vol. 13 No. 1, pp. 103-128, 2020.

Paré, G., Trudel, M.C., Jaana, M. and Kitsiou, S. (2015), "Synthesizing information systems knowledge: a typology of literature reviews", *Information and Management*, Vol. 52 No. 2, pp. 183-199.

Parenty, T. and Domet, J. (2021), "Sizing up your companýs cyber risks. Cybersecurity and Digital Privacy", Harvard Business Review, available at: https://hbr.org/webinar/2021/05/sizing-up-your-companys-cyber-risks

Patterson, G. (2011), "Cyberwar: the United States and China prepare for the next generation of conflict", *Comparative Strategy*, Vol. 30 No. 2, pp. 121-133.

Paul, J. and Criado, A.R. (2020), "The art of writing literature review: what do we know and what do we need to know?", *International Business Review*, Vol. 29 No. 4, p. 101717.

Paul, J., Parthasarathy, S. and Gupta, P. (2017), "Exporting challenges of SMEs: a review and future research agenda", *Journal of World Business*, Vol. 52 No. 3, pp. 327-342.

Paul, J. and Singh, G. (2017), "The 45 years of foreign direct investment research: approaches, advances and analytical areas", *The World Economy*.

Peng, S. (2015), "Cybersecurity threats and the WTO national security exceptions", *Journal of International Economic Law*, Vol. 18 No. 2, pp. 449-478.

Pesapane, F., Volonté, C., Codari, M. and Sardanelli, F. (2018), "Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States", *Insights into Imaging*, Vol. 9 No. 5, pp. 745-753.

Pew Research Center (2018), "As trade tensions rise, fewer Americans see China favorably", available at: www.pewresearch.org/global/wp-content/uploads/sites/2/2018/08/Pew-Research-Center_U.S.-Views-of-China_Report_2018-08-28.pdf

Pournader, M., Shi, Y., Seuring, S. and Kh, S. (2019), "Blockchain applications in supply chains, transport and logistics: a systematic review of the literature", *Special Issue: Blockchain in Transport and Logistics*, pp. 2063-2081.

Premkumar, G. (2003), "A Meta-analysis of research on information technology implementation in small business", *Journal of Organizational Computing and Electronic Commerce*, Vol. 13 No. 2, pp. 91-121.

Qi, A., Shao, G. and Zheng, W. (2018), "Assessing China's cybersecurity law. Computer law and security review".

Qian, X. (2019), "Cyberspace security and US-China relations", *Paper presented at the ACM International Conference Proceeding Series*, pp. 709-712.

Radanliev, P., De Roure, D. and Page, K. (2020), "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains", *Cybersecurity*, Vol. 3, p. 13.

Rahman, A., Malaysia, N.A., Sairi, M.T.U.K., Zizi, I.K. and Khalid, F. (2020), "The importance of cybersecurity education in school", *International Journal of Information and Education Technology*, Vol. 10 No. 5, pp. 378-382.

Ram, J. and Zhang, Z. (2020), "Belt and road initiative (BRI) supply chain risks: propositions and model development", *The International Journal of Logistics Management*, Vol. 31 No. 4, pp. 777-799.

Ramdani, B., Kawalek, P. and Lorenzo, O. (2009), "Predicting SMEs adoption of enterprise systems", *Journal of Enterprise Information Management*, Vol. 22 No. 2, pp. 10-24.

Ramirez-Pena, M., Mayuet, P.F., Vazquez-Martinez, J.M. and Batista, M. (2020), "Sustainability in the aerospace, naval, and automotive supply chain 4.0: descriptive review", *Materials*, Vol. 13 No. 24, p. 5625.

Rodger, J.A. and George, J.A. (2017), "Triple bottom line accounting for optimizing natural gas sustainability: a statistical linear programming fuzzy ILOWA optimized sustainment model approach to reducing supply chain global cybersecurity vulnerability through information and communications technology", *Journal of Cleaner Production*, Vol. 142, pp. 1931-1949.

Rogers, E. (1995), *Diffusion of Innovations*, 4th ed., The Free Press, New York, NY.

Rogers, E. (2003), *The Diffusion of Innovation*, Free Press, New York, NY.

Rongping, M. and Yonggang, F. (2014), "Security in the cyber supply chain: a Chinese perspective", *Technovation*, Vol. 34 No. 7, pp. 385-386.

Rosso, M., Nasir, A.B.M. and Farhadloo, M. (2020), "Chilling effects and the stock market response to the Snowden revelations", *New Media & Society*, Vol. 22 No. 11, pp. 1976-1995.

Sabillon, R., Cano, J., Cavaller, V. and Serra, J. (2016), "Cybercrime and cybercriminals: a comprehensive study", *International Journal of Computer Networks and Communications Security*, Vol. 4 No. 6.

Sarathy, R. (2006), "Security and the global supply chain", *Transportation Journal*, Vol. 45 No. 4, pp. 28-51.

Savitri, E. and Dyah, R. (2019), *Sustainable Supply Chain Management: Exploring the Role of Supply Chain Dynamic Capabilities in Determining Firm Performance*, EAI.

Segal, A. (2020), "China's pursuit of cyberpower", *Asia Policy*, Vol. 15 No. 2, pp. 60-66. National Bureau of Asian Research. 27(2).

Sengupta, J., Ruj, S. and Das Bit, S. (2020), "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT", *Journal of Network and Computer Applications*, Vol. 149, p. 102481.

Sepulveda, D., Sahay, R., Barford, M. and Jensen, C. (2020), "A systematic review of cyber-resilience assessment frameworks", *Computers and Security*, p. 101996.

Shackelford, S., Charoen, D., Waite, T. and Zhang, N. (2018), "Rethinking active defense: a comparative analysis of proactive cybersecurity policymaking", *SRN Electronic Journal*, Vol. 41 No. 2, pp. 377-427.

Sharikov, P. (2018), "Artificial intelligence, cyberattack, and nuclear weapons – a dangerous combination", *Bulletin of the Atomic Scientists*, pp. 1-6.

Shen, Z., Puig, F. and Paul, J. (2017), "Foreign market entry mode research: a review and research agenda", *The International Trade Journal*, Vol. 31 No. 5, pp. 429-456.

Simon, J. and Omar, A. (2019), "Cybersecurity investments in the supply chain: coordination and a strategic attacker", *European Journal of Operational Research*.

Singh, S. (2019), "Sustainable business and environment management", *Management of Environmental Quality: An International Journal*, Vol. 30 No. 1, pp. 2-4, ISSN: 1477-7835.

Singh, S. and Gaur, S. (2020), "Managing organization and business in Asia", *Journal of Asia Business Studies*, Vol. 14 No. 2, ISSN: 1558-7894.

Soumyo, M. (2004), "Cybercrime: towards an assessment of its nature and impact", *International Journal of Comparative and Applied Criminal Justice*, Vol. 28 No. 2, pp. 105-123.

Stellios, I., Kotznikolau, P., Psarakis, M., Alcaraz, C. and Lopez, J. (2018), *IEEE Communications Surveys and Tutorials*, Vol. 20 No. 4, pp. 3453-3495, 8410404.

Svenungsen, B. (2019), "Internet as geopolitical arena?", *Internasjonal Politikk*, Vol. 77 No. 3, pp. 225-240.

The State Council (2013), "The notice on the 'strategy of broadband China and implementation plan'", Guofa No. 31, available at: www.gov.cn

Urquhart, L. and McAuley, D. (2018), "Avoiding the internet of insecure industrial things", *Computer Law & Security Review*, Vol. 34 No. 3, pp. 450-466.

Vakulchuk, R., Overland, I. and Scholten, D. (2020), "Renewable energy and geopolitics: a review", *Renewable and Sustainable Energy Reviews*, p. 109547.

Venkatesh, V. (2008), "Technology acceptance model 3 and a research agenda on interventions", *Decision Sciences*, Vol. 39 No. 2, pp. 273-315.

Visner, S. (2013), "Cyber security's next agenda", *Georgetown Journal of International Affairs*, pp. 89-99.

Von Solms, R. and Van Niekerk, J. (2013), "From information security to cyber security", *Computer Security*, Vol. 38 No. 10, pp. 97-102.

Wallace, S., Green, K.Y., Johnson, C., Cooper, J. and Gilstrap, C. (2020), "An extended TOE framework for cybersecurity-adoption decisions", *Communications of the Association for Information Systems*, Vol. 47.

Wortzel, L. (2011), "China's approach to cyber operations: implications for the United States", *China's Cyberwarfare Capability*, pp. 89-99.

Woszczynski, A., Green, A., Dodson, K. and Easton, P. (2020), "Zombies, Sirens, and Lady Gaga–Oh My! Developing a framework for coordinated vulnerability disclosure for US emergency alert systems", *Government Information Quarterly*, Vol. 37 No. 1, p. 101418.

Xuetong, Y. (2006), "The rise of China and its power status", *The Chinese Journal of International Politics*, Vol. 1 No. 1, pp. 5-33.

Yang, F. and Xu, J. (2018), "Privacy concerns in China's smart city campaign: the deficit of China's cybersecurity law", Asia and the Pacific Policy Studies.

Yassine, N. and Singh, S. (2020), "Sustainable supply chains based on supplier selection and HRM practices", *Journal of Enterprise Information Management*.

Yeboah-Ofori, A., Islam, S., Lee, S., Shamszaman, Z., Muhammad, K., Altaf, M. and Al-Rakhami, M. (2021), "Cyber threat predictive analytics for improving cyber supply chain security", *IEEE Access*, Vol. 9, pp. 94318-94337.

Yu, J. (2017), "Cybercrime in China – a review focusing on increasing criminalisation of harmful cyberactivities", *Hong Kong Law Journal*, Vol. 47, pp. 937-950.

Yusof, M., Kuljis, J., Papazafeiropoulou, A. and Stergioulas, L. (2008), "An evaluation framework for health information systems: human, organization and technology-fit factors (HOT-fit)", *International Journal of Medical Informatics*, Vol. 77 No. 6, pp. 386-398.

Zhang, H., Tang, Z. and Jayakar, K. (2018), "A socio-technical analysis of China's cybersecurity policy: towards delivering trusted e-government services", *Telecommunications Policy*, Vol. 42 No. 5, pp. 409-420.

Zhao, Y. (2016), "China, and cybersecurity: espionage, strategy, and politics in the digital domain", *Pacific Affairs*, Vol. 89 No. 4, pp. 872-874.

Zheng, K., Albert, L.A., Luedtke, J.R. and Towle, E. (2019), "A budgeted maximum multiple coverage model for cybersecurity planning and management", *IISE Transactions*, pp. 1-37.

Zhu, K. and Kraemer, K. (2005), "Post-adoption variations in usage and value of E-business by organizations: cross-country evidence from the retail industry", *Information Systems Research*, Vol. 16 No. 1, pp. 61-84.

Zhu, K., Kraemer, K. and Xu, S. (2002), "A cross-country study of electronic business adoption using the technology-organization-environment framework", *ICIS Proceedings*, Vol. 31.

Zhu, K., Kraemer, K., Xu, S. and Dedrick, J. (2004), "Information technology payoff in E-business environments: an international perspective on value creation of E-business in the financial services industry", *Journal of Management Information Systems*, Vol. 21 No. 1, pp. 17-54.

Further reading

Shackelford, S. and Craig, A. (2014), "Beyond the new 'digital divide': analyzing the evolving role of national governments in internet governance and enhancing cybersecurity", *Stanford Journal of International Law*, Vol. 50 No. 1, pp. 119-184.

Yang, F. and Mueller, M. (2014), "Internet governance in China: a content analysis", *Chinese Journal of Communication*, Vol. 7 No. 4, pp. 446-465.

Corresponding author

James Pérez-Morón can be contacted at: jperez@utb.edu.co