# Integrating artificial intelligence capabilities in supply chain cyber risk management

Claudia Ciceri, Federico Caniato and Antonella Moretto
*School of Management, Politecnico di Milano, Milan, Italy*

International Journal of Physical Distribution & Logistics Management

Received 17 January 2025
Revised 29 May 2025
3 October 2025
9 January 2026
Accepted 10 January 2026

## Abstract

**Purpose** – In recent years, supply chain (SC) cyber risks have become a significant organizational challenge. While artificial intelligence (AI) can play an important role in cyber risk protection, a comprehensive analysis of its impact is missing. This article aims to answer this gap by analyzing how different AI capabilities support the different phases of the Supply Chain Cyber Risk Management (SCCRM) process.

**Design/methodology/approach** – Three embedded case studies involving three different classes of cybersecurity providers with different roles in the cybersecurity industry were developed. The three cases of vendors, system integrators and consultancy firms have been chosen as these three distinct classes of actors can provide different perspectives about their specific business.

**Findings** – An analysis of how different AI capabilities are exploited by the three cases in the different phases of the SCCRM process is presented. In addition, a practical framework for managers is provided about how these solutions can be leveraged to enhance cybersecurity in the SC.

**Originality/value** – The present article contributes to theory by expanding the existing literature on SCCRM and establishing a link between the domains of AI and cybersecurity. It demonstrates the potential of AI capabilities to support the various phases of the SCCRM process. Specifically, the results revealed that AI plays a crucial role in supporting sensing, seizing and transforming capabilities in dealing with cyber risk. Thus, this study advances dynamic capabilities (DC) theory by offering an interpretive lens through which to understand AI adoption in SCCRM.

**Keywords** Supply chain risk management, Cyber risk, Supply chain cyber risk management, Artificial intelligence, Dynamic capabilities

**Paper type** Research article

## 1. Introduction

Cyberattacks have surged year over year, with reports indicating over 2,200 attacks per day globally in 2025, roughly one every 39 s (World Economic Forum, 2025). One of the most significant issues is that a cyberattack on a single firm can have cascading effects on other organizations directly or indirectly connected to it. Indeed, a firm can be attacked even by breaching one of its first, second, third, or even fourth-tier suppliers (Friday *et al.*, 2024). In addition, cyber risks distinguish themselves within the broader context of SC risks as they possess unique characteristics that make them more challenging for supply chains (SCs) (Herburger *et al.*, 2024). However, proper solutions to deal with cyber risks at the SC level are still missing (Colicchia *et al.*, 2019; Creazza *et al.*, 2022). Therefore, some researchers have started to search for new ways of managing cyber risks, and some of them have found that artificial intelligence (AI) can be a game changer in cybersecurity, providing visibility and transparency across the entire SC (Taddeo *et al.*, 2019; Zeadally *et al.*, 2020).

The importance of managing cyber risks at the SC level has been widely discussed in the literature (Colicchia *et al.*, 2019; Creazza *et al.*, 2022; Gaudenzi and Siciliano, 2017; Ghadge



International Journal of Physical Distribution & Logistics Management
Emerald Publishing Limited
e-ISSN: 1758-664X
p-ISSN: 0960-0035
DOI 10.1108/IJPDLM-01-2025-0028

et al., 2020; Guerra and Estay, 2018; Siciliano and Gaudenzi, 2018). Indeed, some high-profile attacks, such as the SolarWinds case, have underscored the relevance of cybersecurity at the SC level (Berry, 2023), shedding light on the imperative to transcend the technical realm in addressing cyber risks and advocating for an approach that comprehensively embraces the interconnected nature of SCs. Indeed, the strength of the SC is tied to the cybersecurity of its weakest link (Berry, 2023; Colicchia *et al*., 2019). In this landscape, digitization can be a double-edged sword for the management of cyber risks, increasing the strength of cyberattacks but also supporting companies in the management of cyber risks (Hendriksen, 2023; Taddeo *et al*., 2019). Indeed, cybercriminals are increasingly employing AI to execute sophisticated cyberattacks that are difficult to detect. Similarly, AI has the potential to improve cybersecurity solutions, thereby improving defenses against cyber threats and reducing or avoiding the repercussions of cyber risk (Zeadally *et al*., 2020). Indeed, AI can provide analytics and intelligence to protect against the ever-evolving nature of cyberattacks by quickly analyzing millions of events and tracking a wide variety of cyber threats to anticipate and counteract threats before they materialize (Kaur *et al*., 2023). These capacities are especially relevant in SC cyber risk management contexts, which are characterized by evolving landscapes, unstructured decision-making processes, and the constantly changing status of systems cybersecurity (Helo and Hao, 2022; Richey *et al*., 2023).

However, despite some researchers started to theorize about the benefits of the application of AI in cybersecurity (Corbett and Sajal, 2023; Zeadally *et al*., 2020) and some others addressed the usage and development of specific algorithms in cybersecurity (Chan *et al*., 2019; Kaur *et al*., 2023; Wiafe *et al*., 2020), the literature at the intersection between AI and Supply Chain Cyber Risk Management (SCCRM) is still scarce and conceptual. Furthermore, besides the identification of its potential relevance (Hendriksen, 2023; Radanliev *et al*., 2020), no one has empirically explored how AI could strengthen the SCCRM process.

Indeed, some researchers have begun to advocate that AI can be extremely useful in cybersecurity, as it can improve the security of systems and reduce their vulnerability to attacks while also altering the dynamics that facilitate offense over defense in cyberspace and, lastly, improve SC efficiency (Radanliev *et al*., 2020; Taddeo *et al*., 2019; Zeadally *et al*., 2020). However, to the best of our knowledge, no one has empirically analyzed how different AI capabilities can be leveraged in the different phases of the SCCRM process. Therefore, we set in this discourse, trying to understand how AI capabilities can act in this direction, supporting the different phases of the SCCRM process. This goal was operationalized in the following research question:

*RQ*. How do AI capabilities impact the SCCRM process?

The present study contributes significantly to the advancement of both theoretical understanding and managerial implications within the examined domain. In particular, it expands the existing body of literature on SCCRM by integrating the domains of AI and cybersecurity by showing how diverse AI capabilities could enhance the different phases of the SCCRM process. In this way, this article responds to the call for research on the role of AI in reshaping SC processes (Richey *et al*., 2023). In particular, a comprehensive analysis of the results revealed three key insights regarding the contributions of AI capabilities to SCCRM. First, AI plays a crucial role in supporting the sensing of the cyber risk environment, facilitating the development of a comprehensive understanding of the risks to which SCs are exposed. Second, AI supports firms in seizing the sensed cyber risks by determining their nature and impact and implementing appropriate responses. Third, AI facilitates the transformation of SC settings, enhancing the overall level of cyber risk protection to align with the sensed and seized risks. The aforementioned findings are consistent with the principles outlined in dynamic capabilities (DC) theory (Teece *et al*., 1997), which posits that a firm's ability to sense, seize and manage external environmental changes is a critical factor that contributes to gaining a competitive advantage. This theory is commonly used to explain contexts marked by high dynamism and uncertainty, where the ability to detect and adapt quickly to external

environmental changes is paramount (Ellström *et al*., 2022; Hilliard and Goldstein, 2019). Therefore, it is considered a valuable lens for interpreting our results (Maxwell, 2013), explaining how AI capabilities can help address the volatile and complex environment created by cyber risks. In addition, although the DC perspective is conventionally employed to elucidate how firms discern and react to both opportunities and threats in their environment, the existing literature has demonstrated some applications limited only to the context of threats (Dubey *et al*., 2023; Herburger *et al*., 2024; Jazairy *et al*., 2024; Juan and Li, 2023). Indeed, threat recognition has a greater impact on revenue growth than opportunity recognition, however, firms generally focus more on opportunities rather than threats (Herburger *et al*., 2024). Therefore, some scholars have started to adopt DC to study cybersecurity, as the rapidly evolving nature of cyber risks and their higher undetectability cause significant uncertainty that needs to be managed (Herburger *et al*., 2024; Jazairy *et al*., 2024; Naseer *et al*., 2024). Therefore, in line with this expanding body of literature, we consider DC as a valuable theoretical lens to interpret our results. Furthermore, the subject of SCCRM is also relevant to the industry, where there is an urgent need for SC cybersecurity. Indeed, high economic, business, infrastructure and national security costs are associated with cyber risks. These costs are even higher when we talk about cyber risk management at the SC level. Indeed, requiring SC partners to comply with cybersecurity practices can cause them to exit the SC. This departure can create significant costs related to the lack of materials and the time and effort required to replace them (Melnyk *et al*., 2022). Therefore, the identification of sustainable solutions to this issue is of paramount importance. Our findings aim to contribute in this direction, informing industry practice on the role of AI capabilities in SCCRM, and offering practical guidelines for managers on how to implement it.

This research employs an exploratory embedded case study methodology, considering three classes of cybersecurity providers: vendors, system integrators and consulting companies. Multiple companies were interviewed for each case, each company serving as an illustrative example within the broader case framework. This approach facilitated the understanding of the different perspectives of the three classes of companies, emphasizing both the similarities and differences between their business while also allowing the identification of the specific traits of each organization. Semi-structured interviews were conducted with four vendors, five system integrators, and five consulting firms. These data were complemented with secondary sources coming from the companies' websites or directly provided by interviewees.

The remainder of the article is organized as follows. In Section 2, the theoretical background is discussed. This background is intended to provide an introduction and conceptualization of SCCRM and AI topics. It also provides an overview of the literature at the intersection of the two topics and on the reasons behind the adoption of DC theory to interpret the results. Section 3 delineates the research methodology used in conducting the investigation, the data collection and analysis process and the methodological approach adopted to ensure the validity and rigor of the research. Section 4 provides an analysis of the synthesized findings, showing how different AI capabilities are used in the different phases of the SCCRM process. Section 5 discusses the findings in relation to the previous literature, developing six propositions to extend it. Finally, Section 6 presents the contributions of the research to both theory and practice, as well as the limitations of the study.

## 2. Theoretical background

### *2.1 Supply Chain Risk Management*

Supply Chain Risk Management (SCRM) involves a cross-organizational focus that aims to identify and reduce risks along the entire SC (Wiengarten *et al*., 2016). There is no universally accepted definition of SCRM, however, one of the most comprehensive is the one provided by Fan and Stevenson (2018), which states that *"Supply Chain Risk Management consists in the identification, assessment, treatment, and monitoring of SC risks using internal tools, techniques, and strategies as well as external coordination and collaboration with supply*

*chain members to reduce vulnerability and ensure continuity and profitability, culminating in a competitive advantage"* (Fan and Stevenson, 2018, p. 210). SCRM is therefore a structured process developed through various sequential steps to reduce SC risks (Fan and Stevenson, 2018).

The first phase is risk identification, which aims to uncover all relevant sources of risk along the SC and improve transparency (Hoffmann *et al*., 2013). Risk assessment then involves the evaluation of all identified risks in terms of probability of occurrence and impact on SC performance. This enables the prioritization of risks and the discrimination between those that are highly relevant and those that are less relevant (Blome and Schoenherr, 2011). Risk treatment aims to ensure that the overall level of risk to which a company is exposed remains within acceptable limits by implementing appropriate risk mitigation strategies (Wiedenmann and Größler, 2020). Finally, given that risk is not a static phenomenon, there is the risk monitoring phase, whose objective is to continuously review the risks that have been identified to verify the effectiveness of the actions taken to manage them and to make some adjustments as necessary (Fan and Stevenson, 2018; Hoffmann *et al*., 2013).

These steps, implemented through the utilization of internal tools and the engagement of the other SC members, are designed to safeguard a firm against all possible SC risks (Teuteberg, 2008; Vieira *et al*., 2019).

### *2.2 Supply chain cyber risk management*

Cyber risks are operational risks to the organization's information, technological assets and resources, with negative consequences for the confidentiality, availability and integrity of these assets (Herburger *et al*., 2024). These risks encompass a spectrum of potential issues, including data breaches, malware, ransomware and other forms of cyber threats that can compromise the integrity, confidentiality or availability of SC data and systems (Berry, 2023). Cyber risks differentiate themselves within the broader context of SC risks as they possess unique characteristics that make them more challenging for SCs (Herburger and Omar, 2021). Indeed, they are characterized by a rapidly evolving nature, greater undetectability, SC diffusion, malicious intent and the targeting of both informational and physical assets (Jazairy *et al*., 2024).

Therefore, starting from the SCRM and cybersecurity fields, Supply Chain Cyber Risk Management (SCCRM) emerged as a new research stream that deals with the management of cyber risks across SCs (Colicchia *et al*., 2019). Indeed, cybersecurity is not merely a concern of a single company, it is a shared responsibility of the entire SC (Urciuoli *et al*., 2013). Therefore, the need for a more comprehensive approach to address cyber risks from a SC perspective emerged (Colicchia *et al*., 2019; Creazza *et al*., 2022; Ghadge *et al*., 2020). Researchers have therefore developed the concept of SCCRM to address initiatives that focus on the management of cyber risks throughout the end-to-end operations of a SC (Colicchia *et al*., 2019; Gaudenzi and Siciliano, 2017; Ghadge *et al*., 2020; Guerra and Estay, 2018; Jazairy *et al*., 2024; Siciliano and Gaudenzi, 2018). However, researchers have begun to question whether dedicated management strategies are needed or whether traditional SCRM strategies can be extended to them. In particular, Pandey *et al*. (2020) describe how the three steps of risk identification, risk assessment and risk mitigation of the SCRM process can be tailored to cyber risks. Subsequently, Jazairy *et al*. (2024) adopted the NIST Cybersecurity Framework (Cybersecurity, 2018), with the five phases of identify, protect, detect, respond, and recover, to study the effect of SC cyber risk management strategies on SC integration decisions for cybersecurity to improve the cyber resilience of the SC. Through their study, they demonstrate that it is not necessary to reinvent the wheel but that the constructs of the SCRM process can be extended to SC cyber risks.

In order to contribute to this research stream and better align with the SCRM literature, we consider the SCCRM process as an adapted version of the SCRM one. In particular, we built on the models of Pandey *et al*. (2020) and Jazairy *et al*. (2024), incorporating the risk monitoring phase, a phase that has not been considered in their models but that is essential in the context of

cybersecurity. Indeed, cyber risks are evolving rapidly and continuously (Taddeo *et al*., 2019). Consequently, companies must constantly monitor and scan their business environment to identify new threats and opportunities (Herburger *et al*., 2024; Kosmowski *et al*., 2022).

### *2.3 Artificial intelligence*

A unique definition of AI cannot be found in literature, however, it can be described as a set of intelligent systems that can mimic human behavioral patterns and solve real-world problems as a human with intelligence (Helo and Hao, 2022; Min, 2010). Indeed, AI encompasses systems that interact with the environment in the form of text, video and audio, that can learn from the experience provided by historical data, and that can make decisions that normally require human intelligence through approaches such as planning, optimization, simulation, modeling and programming, and deciding the best actions to take to achieve a given goal (Cannas *et al*., 2024; Samoili *et al*., 2020).

The present study focuses on the capabilities of AI in performing tasks that would typically require human intelligence and the support that AI provides in different problem types. In particular, this study draws on the work of Jackson *et al*. (2024), which provides a capability-based framework for AI in SC and operations management, where the emphasis is on functional aspects and the effects of technology in the field. We believe that this perspective is particularly suitable for this research, where the critical issue is not which algorithms are used but what AI enables in terms of cyber risk management.

A taxonomy of the AI capabilities adopted in this study is presented in Table 1, developed based on the existing literature.

### *2.4 Artificial intelligence in supply chain cyber risk management*

Over the years, although the original motives for carrying out cyberattacks remain unchanged, cybercriminals have become increasingly sophisticated with their techniques. Therefore,

**Table 1.** AI capabilities

| AI capability | Definition | References |
|---|---|---|
| Learning | The ability to automatically learn from data, to predict, analyze and make decisions, improving from experience without explicit programming | Samoili *et al*. (2020), European Commission. Joint Research Centre. (2020), Jackson *et al*. (2024) |
| Perception | The ability to understand and interpret the world by mimicking human senses, such as recognizing objects in images and perceiving or generating audio signals | Samoili *et al*. (2020), European Commission. Joint Research Centre. (2020), Paschen *et al*. (2020) |
| Prediction | The ability to forecast future outcomes and to define strategies for certain activities based on historical data and patterns | Samoili *et al*. (2020), Jackson *et al*. (2024) |
| Interaction | The ability to interact and make decisions in an environment, including interactions with humans | Samoili *et al*. (2020), European Commission. Joint Research Centre. (2020), Jackson *et al*. (2024) |
| Adaptation | The ability to adapt and improve over time based on new data and changing environments | Samoili *et al*. (2020), Jackson *et al*. (2024) |
| Reasoning | The ability to reason, plan and make decisions, by transforming data into knowledge, inferring facts, justifying available data, providing solutions and representing them efficiently | Samoili *et al*. (2020), Jackson *et al*. (2024) |
| Creativity | The ability to generate creative content by leveraging patterns and structures from the data it was trained on and recombining learned elements in innovative ways | European Commission. Joint Research Centre. (2020), Paschen *et al*. (2020), Jackson *et al*. (2024) |

**Source(s):** Adapted from Jackson *et al*. (2024), Samoili *et al*. (2020)

traditional cybersecurity solutions have become inadequate to detect and mitigate emerging cyberattacks (Zeadally *et al*., 2020). Therefore, certain studies posit that relying solely on human behavior is insufficient to effectively manage cyber risks (Li, 2018) as cybercriminals are increasingly using advanced technologies to launch cyberattacks (Zeadally *et al*., 2020). This issue is further intensified by the advances in digital technologies and the consequent interconnectedness, which have resulted in a significant increase in cyberattacks with severe consequences (Kaur *et al*., 2023). Therefore, on the defender's side, there is a growing need for innovative approaches to combat these attacks. Indeed, digital technologies become targets for attacks themselves (Corbett and Sajal, 2023; Wu *et al*., 2018), generating new categories of vulnerabilities and therefore posing serious security threats, necessitating dedicated defense and protection (Taddeo *et al*., 2019).

Researchers have therefore started to analyze how different technologies can have an impact on cyber risk protection. Blockchain has demonstrated its efficacy in facilitating secure and tamper-proof data transactions, thus ensuring traceability and integrity in data exchanges (Kshetri, 2017; Liang *et al*., 2018). A key feature of blockchain is its immutability, meaning that once data is recorded on the ledger, it cannot be altered or deleted. This property ensures integrity and trust in transactional records. However, it poses limitations in terms of real-time detection and rapid response to cyber threats (Akanfe *et al*., 2024). Robotic Process Automation (RPA) plays a crucial role in improving security operations by automating routine tasks, thereby reducing the probability of human error and optimizing response times to cyber incidents (Lacity and Willcocks, 2021). However, some studies have shown that RPAs are susceptible to challenges in dynamic threat environments, particularly when it comes to process changes and exception handling (Armstrong and Berkowitz, 2024; Eulerich *et al*., 2024). Among these technologies, AI emerged as a particularly promising one that can overcome the limitations of the previous technologies proposed due to its ability to analyze large amounts of data, detect anomalies and adapt to evolving threats in real time (Ganesh and Kalpana, 2022). In particular, a strong driver for the use of AI comes from the large amounts of data that are constantly produced today, which require significant resources and time to analyze and detect any patterns, anomalies or intrusions in traffic data (Kaur *et al*., 2023). In addition, zero-day cyberattacks, attacks that exploit an unknown vulnerability for which the company is not prepared, are becoming more prevalent and continuously evolve in complexity over the years (Zeadally *et al*., 2020). The capacity of AI to discover previously unseen patterns in data is therefore one of the key drivers for AI adoption in cybersecurity. In addition, recent advances in cryptographic methods and AI techniques hold significant promise to empower cybersecurity professionals to counter the dynamic threats posed by adversaries (Zeadally *et al*., 2020). Indeed, AI has the ability to intelligently and automatically analyze and classify large amounts of data with high speed and accuracy, saving resources and time and providing a higher return on investment (Ansari *et al*., 2022; Corbett and Sajal, 2023; Zeadally *et al*., 2020). In addition, unlike static security systems, AI-enabled ones can provide real-time detection and reporting of attack attempts, enhancing system security (Ansari *et al*., 2022).

Therefore, given the distinctive characteristics of AI, which make its implementation in cybersecurity different from that of other technologies (Ångström *et al*., 2023), a significant body of research has emerged investigating the integration of AI in cybersecurity (Kaur *et al*., 2023). Indeed, the potential, uses, consequences and expertise required for AI differ significantly from those of other technologies (Ångström *et al*., 2023). Some researchers have therefore started to focus their studies on developing specific AI algorithms to enhance cybersecurity (Cui *et al*., 2018; Dong *et al*., 2016; Yu *et al*., 2016). Overall, some attempts have been made to map the adoption of AI in cybersecurity (Kaur *et al*., 2023; Li, 2018; Wiafe *et al*., 2020). Li (2018) provided a summary of how AI techniques such as machine learning and deep learning have been used to combat cyberattacks. Wiafe *et al*. (2020) conducted a systematic literature review on how different AI algorithms have been applied in cybersecurity domains. Kaur *et al*. (2023) instead presented a systematic literature review on different AI use cases in the cybersecurity domain, classifying the identified use cases according to the NIST

cybersecurity framework and the cybersecurity activities in which AI capabilities have been used. However, a notable gap remains in the literature on how AI can improve SCCRM (Chan *et al*., 2019; Walshe *et al*., 2021; Zeadally *et al*., 2020).

The objective of this article is therefore to perform an empirical study to understand how different AI capabilities can improve the SCCRM process. This topic is of particular relevance given the substantial economic, business, infrastructure and national security costs associated with cyber breaches and the current lack of a proper solution (Melnyk *et al*., 2022). Indeed, even if AI appears to have the potential to address this issue (Taddeo *et al*., 2019; Zeadally *et al*., 2020), no empirical studies have been conducted on its application in SCCRM. Therefore, this represents a highly compelling research opportunity that requires further investigation.

### *2.5 Dynamic capabilities*

Teece *et al*. (1997) introduced the theory of DCs, grounding it in the resource-based view. The DC model is a widely embraced theoretical framework that examines a company's capacity to integrate, develop and adapt internal and external competencies in turbulent environments characterized by rapid and unpredictable changes (Teece *et al*., 1997). In their seminal work, Teece (2007) conceptualized dynamic capabilities as comprising three distinct clusters of capabilities: sensing, seizing and transforming. Sensing capabilities refer to the process of scanning, acquiring knowledge, and interpreting the opportunities and challenges presented by the competitive environment. Seizing capabilities refers to the manner in which companies address the identified issues. Transforming capabilities denote the manner in which companies undergo changes in their organizational structures and functional capacities to align with the evolving environment.

This perspective has traditionally been used to examine how firms navigate both opportunities and threats. However, more recent studies have also applied it specifically to contexts dominated by threats, such as risk and resilience management (Dubey *et al*., 2023; Herburger *et al*., 2024; Jazairy *et al*., 2024; Juan and Li, 2023). For instance, Juan and Li (2023) studied the relationships between dynamic capability and SC resilience, while Dubey *et al*. (2023) studied resilience as an outcome of dynamic digital capabilities grounded in sensing, seizing and transforming.

Given the rapidly evolving nature of cyber risks and their high undetectability, which cause significant uncertainty, scholars have started to consider DC as a promising theoretical lens to study cybersecurity. In particular, Naseer *et al*. (2024) demonstrated the application of DC in cybersecurity through active threat reconnaissance, defense and pervasive learning. Jazairy *et al*. (2024) examined the impact of dynamic capabilities on SC resilience and robustness in the cyber risk domain. Herburger *et al*. (2024) instead investigated methods to improve the cyber resilience of SCs through dynamic sensing, seizing and transforming capabilities. Consequently, in alignment with this expanding body of literature, we employ the DC view to interpret our results in relation to the existing literature (Maxwell, 2013).

## 3. Methodology

This study aims to advance the literature on SCCRM, investigating how AI capabilities can play a role in it. This is a subject that needs further exploration, as shown in the previous sections. In particular, this research engages in theory elaboration, building upon the literature on AI adoption in SCRM to clarify and expand it to cyber risks, and presenting propositions based on theoretical and empirical observations. Indeed, theory elaboration can be a suitable approach when conceptual ideas exist that can serve as the foundation of empirical research, but the premises are not sufficiently detailed to deduce hypotheses for testing (Bals and Tate, 2018).

To achieve this objective, a qualitative research approach was selected. Specifically, multiple embedded case studies were conducted, as they are well-suited to exploratory

research on matters that need deeper understanding (Eisenhardt, 1989). Furthermore, this methodology is well-suited to cope with the increasing frequency and impact of technological and managerial changes, and is one of the main methods employed in operations management (Caniato *et al*., 2018; Voss, 2010).

An abductive approach was adopted to enable seamless integration of theory and empirical observations (Ketokivi and Choi, 2014; Kovács and Spens, 2005). Indeed, abductive reasoning begins with exploratory observations at the individual level and attempts to formulate generalizable explanations through an iterative progression between data and theory (Hughes *et al*., 2023). In particular, the abductive process begins with a set of preconceived notions and theoretical knowledge regarding a particular subject, as is the case in the context of AI adoption in the domain of SCRM. However, the abduction itself originates from an empirical observation of a phenomenon that appears counterintuitive to existing theory. In this instance, the advent of cyber risks in SCs appears to deviate from the conventional patterns exhibited by other SC risks due to their rapidly evolving nature, higher undetectability, SC diffusion, malicious intent and the targeting of both informational and physical assets (Jazairy *et al*., 2024). Therefore, we reviewed the literature to understand how AI can support the management of these specific SC risks. Through a process of theory matching, we interpreted AI capabilities as dynamic capabilities that support the identification, assessment, treatment and monitoring of such risks. The ultimate objective of abduction is to understand this new phenomenon and suggest new theories in the form of hypotheses or propositions (Kovács and Spens, 2005). We therefore formulated six propositions to explain how AI capabilities can support the SCCRM process. However, these propositions are not presented as definitively proven or empirically validated; rather, they are plausible as supported by multiple pieces of evidence, but they still need to be tested (Eriksson and Engström, 2021; Kovács and Spens, 2005).

Indeed, in this study, abductive reasoning is employed as a way of applying critical realism to research. It involves trying to find the best explanation for observed events and developing new theories in the face of a lack of theoretical understanding about an empirical phenomenon. Therefore, the resulting knowledge claims tentatively explain the empirical world surrounding the researchers but always allow for better explanations (Eriksson and Engström, 2021).

Figure 1 presents an overview of the abductive process followed in this research.

### *3.1 Case selection*

Empirical data have been collected from three case studies involving different classes of cybersecurity providers. The choice of interviewing providers is related to the fact that they are more aware of the functioning of the solutions they offer and may provide better insights about the latest technologies adopted, which their customers may not be fully aware of. Providers are usually more technologically mature and at the forefront of innovation; therefore, they can offer better insights on how cutting-edge technologies such as AI can be applied in the field. In addition, providers are usually more prone to share details on cybersecurity threats. In contrast, user companies are more reluctant to share information related to their cybersecurity posture due to the fear of being more exposed to cyberattacks and bad reputation concerns. Lastly, cybersecurity solutions are still underutilized, making it challenging to identify and engage actual users.

In selecting the sample, the aim was to create a diverse yet coherent set for the analysis (Robinson, 2014); therefore, companies with different roles in the cybersecurity industry were selected to have a more heterogeneous perspective. In particular, we developed three embedded case studies (Yin, 2009) in which each case targets one of the three classes of cybersecurity providers available on the market, namely vendors, system integrators and consulting firms. We analyzed them as three separate cases, as they can provide different perspectives on their specific business. The first case (Vendors) comprises firms directly involved in developing and selling cybersecurity solutions, which can offer an in-depth view

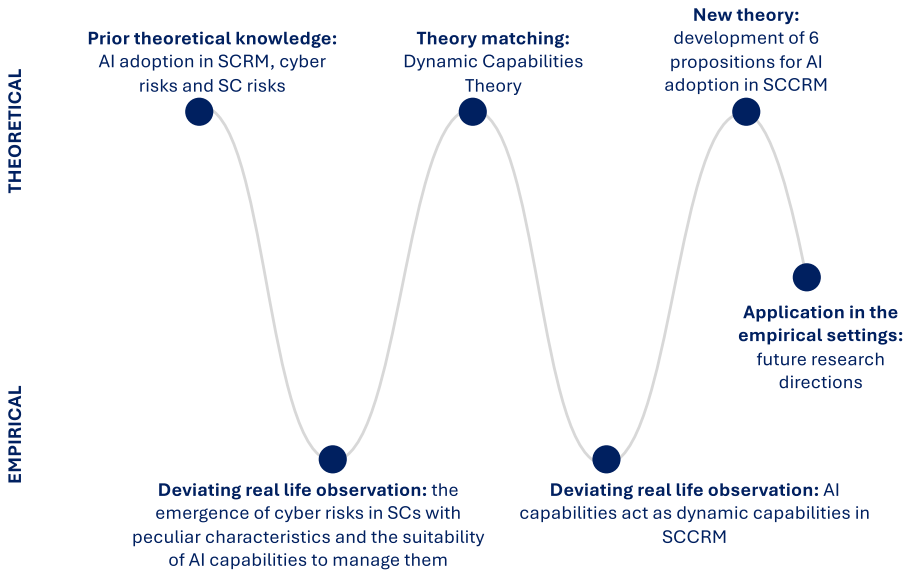


**Figure 1.** Abductive research process followed in this research. Adapted from Kovács and Spens (2005)

of specific products, advanced features and how emerging technologies are integrated into their products. The second case (System Integrators) involves companies responsible for the implementation and integration of cybersecurity solutions within an organization's IT infrastructure. They can provide insights about how different products are combined and integrated into comprehensive solutions, how AI is implemented in these solutions and the associated challenges. Lastly, consulting firms within the cybersecurity sector form the third case (Consultancies), adding to the technical offering also some organizational solutions oriented to processes and people. They can provide strategic insights into cybersecurity market trends, AI adoption best practices and implications. In each case, more than one company has been interviewed, considering each company as an illustrative example within the broader case. Overall, 24 interviews were conducted with cybersecurity experts from different companies belonging to the three categories. The detailed sample is reported in Table 2.

In selecting the sample, companies with a certain number of years of experience in the cybersecurity industry, with advanced technology and mature security protocols, were targeted. Moreover, the study focused on companies with headquarters or branches in Italy to mitigate variations resulting from cultural, linguistic, legal and economic differences between locations, ensuring more consistent findings.

### *3.2 Data collection*

After reviewing the existing literature, we developed a data collection instrument and a semi-structured common interview protocol across all cases (see Table A1 in Appendix 1) to ensure the traceability of the results. The interview protocol was intended as a checklist rather than a strict guideline for the interview, allowing participants to provide flexible responses for a deeper exploration of their experiences and perspectives. The unit of analysis was the SCCRM process. Consequently, during the interviews, the respondents were asked to present how they support their clients' SCCRM process through the cybersecurity solutions they offer, indicating if they exploit AI in these solutions and for what purpose.

**Table 2.** Overview of cases – details about the interviewed companies

| Case | Company name | Turnover | Respondents' role | Secondary sources |
|---|---|---|---|---|
| Vendors | Vendor A | 6 M€ | Head of Cybersecurity, Cybersecurity and Threat Intelligence Senior Analyst, Head of Security Operation Center | Website |
| | Vendor B | 430 M€ | Cybersecurity Solutions Engineering Manager | Website, 2 company reports, 1 whitepaper |
| | Vendor C | 15.5 M€ | Executive Board Member and Chief Marketing Officer | Website, 2 company reports |
| | Vendor D | 2 M€ | Head of Research and Co-founder | Website, 1 company report |
| System Integrators | System Integrator A | 15300 M€ | Innovation and Sustainability Manager | Website |
| | System Integrator B | 46000 M€ | Director, Partner Cybersecurity Services | Website |
| | System Integrator C | 5.5 M€ | Co-Founder and Senior System Engineer | Website |
| | System Integrator D | 92 M€ | Cyber Security Operation Center Manager | Website |
| | System Integrator E | 34 M€ | Cloud and Cybersecurity, Cybersecurity Manager, Cybersecurity Director, Director of Business Integration Innovation and IT | Website |
| Consultancies | Consultancy A | 45000 M€ | Senior Consultant, Senior Manager Cybersecurity, Cybersecurity Consultant, Cybersecurity Consultant | Website, 2 company reports |
| | Consultancy B | 0.7 M€ | Cybersecurity Specialist | Website |
| | Consultancy C | 3 M€ | Business Developer and Pre-Sales | Website |
| | Consultancy D | 60000 M€ | Cybersecurity Senior Manager | Website, 2 company reports |
| | Consultancy E | 46000 M€ | Cybersecurity and Privacy Partner, Cybersecurity and Privacy Senior Associate | Website, 3 company reports |

The data obtained from semi-structured interviews were triangulated with information from other sources, including provider websites, informative sections, white papers and case studies to ensure the validity of the results.

### *3.3 Data analysis*

Initially, informants' responses, as well as data collected from secondary sources, were organized and coded in vivo. Subsequently, we gradually progressed toward a more theory-driven explanation, comparing our first-order categories with insights from previous research, and structured them into second-order themes and higher-level aggregate dimensions (Giudici *et al.*, 2018). The detailed description of the coding and selected quotations for each code are presented in Appendixes 2–5.

Following this, an in-depth within-case analysis was conducted to produce case study reports, identifying and categorizing patterns within each case (see additional material for publication). In the beginning, each interviewee was considered a separate entity and analyzed independently. Subsequently, the responses of the various interviewees pertaining to the same case were aggregated and collectively analyzed in the within-case analysis. The objective of

this aggregation process was to develop a comprehensive and nuanced perspective on each case. Indeed, rather than seeking to harmonize or reconcile divergent perspectives within a single case, a deliberate focus was placed on the examination of divergences and unique features emerging from the individual perspectives. This approach was taken to capture the inherent complexity and richness of each case study.

Then, a cross-case analysis was conducted to compare the three cases, highlighting patterns, similarities and differences between variables, performed independently by two researchers with discrepancies resolved through consensus with a third researcher. Findings were then presented to the interviewees for validation, seeking feedback to ensure the accuracy and validity of the results. According to the unit of analysis, we compared cases based on the AI capabilities they exploit in the different phases of their SCCRM process. By examining the similarities and differences between cases, we aimed to elaborate theory, grounding constructs through conceptualization and abstraction (Kembro and Norrman, 2025).

## 4. Findings

Overall, the results of the case studies show that cybersecurity providers are beginning to make different uses of AI in their cybersecurity solutions for SCCRM. In this section, we describe the role of different AI capabilities in each of the phases of the SSCRM process. In Figure 2, it is possible to see an overall picture of how the three cases take advantage of the different AI capabilities (in the rows) in the different phases of the SCCRM process (in the columns and reported with similar colors).

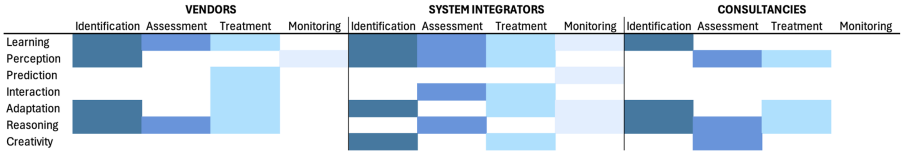


**Figure 2.** Mapping of AI capabilities adopted in the different SCCRM process phases: overview of the results by case

### *4.1 Risk identification*

In the identification phase, our findings show that AI capabilities strongly reinforce the activities of anomaly detection and threat analysis. In particular, the three cases state that they exploit AI's **learning** capability to facilitate the identification of cyber risks through the detection of anomalous behavior. Indeed, AI's learning capability enables the system to dynamically flag irregular patterns that may signal the onset of an attack based on previous experience (System Integrator B). For instance, it enhances the identification of anomalous user behaviors, such as unusual access times, geolocations, or communication channels (Vendor A; Vendor B; Consultancy B), and it helps in highlighting discrepancies between actual company policy and behaviors, helping to identify if some individuals are taking advantage of their access rights for malevolent purposes (System Integrator D). Another application of AI's learning capability is in analyzing system activity to improve the early detection of threats that may otherwise go unnoticed. Indeed, AI solutions integrated in antivirus and Endpoint Detection and Response (EDR) systems [1] can analyze the behavior of executables across extensive datasets to identify deviations from standard operations and issue alerts to human operators, who can then investigate and respond appropriately (System Integrator A, System Integrator C, Vendor D). Lastly, Consultancy E also employs AI's learning capability to identify emails of a malicious nature, such as phishing [2] or spam emails, based on their content.

Another capability of AI that emerged from the three cases is that of **adaptation**, which improves cyber risk identification by enabling anomaly detection in dynamic and unpredictable environments. In contradistinction to learning that depends exclusively on predefined rules, adaptive AI technologies update in real time to new and previously unseen conditions, thereby facilitating the identification of unknown threats. This is exemplified by System Integrator C, who says: "*In zero day attacks, which are the attacks that are not known and can be very dangerous precisely because the company is not prepared, AI can help to identify patterns of behavior also based on the analysis of the system state.*" Other companies echoed this responsive logic, stating that AI adaptation capability enables "responsive visibility" by supporting the real-time analysis of data and helping in the interaction with unknown entities, therefore allowing for proactively identifying emerging threats (Consultancy E, System Integrator B, System Integrator D, System Integrator E, Vendor C).

Furthermore, vendors and consultancies emphasized the supportive role of AI's **reasoning** capability in the identification of cyber risks by enhancing threat analysis routines. In particular, AI's reasoning capability facilitates the processing of data, thereby enabling the automation of threat analysis and, therefore, the identification of the nature of potential risks (Vendor B, Vendor D). In addition, AI's reasoning capability supports the operator in threat intelligence activities [3], performing correlation analysis of different data points throughout the SC ecosystem and thus facilitating the detection of risks along the SC that would otherwise be too complex or time-consuming for human analysts to identify (Consultancy D).

Vendors and system integrators have reported that AI's **perception** capability also supports the identification of cyber risks by enhancing anomaly detection. AI's perception capability consists of the capacity of AI to perceive, sense, interpret and extract meaning from unstructured or semi-structured data. In particular, in our sample, AI's perception capability is exploited to improve log analysis, by enabling the operators to recognize patterns of possible dangerous situations. In addition, it can enhance text analysis by scanning for predefined keywords and raising alerts when suspicious terms are detected, prompting a human review.

Table A2 (Appendix 2) summarizes the key constructs derived from empirical evidence that underlie how AI capabilities support the identification phase of the SCCRM process.

### *4.2 Risk assessment*

From our findings, it emerges that AI capabilities can support risk assessment in SCCRM in two ways. On one side, providing support to the assessment of the identified cyber risks. On the other side, AI can support the evaluation and improvement of the cybersecurity posture of a company and its SC.

In the first case, the findings of this research indicate that, in all the cases examined, AI's **reasoning** capability plays a critical role in the assessment of cyber risk, particularly in supporting the evaluation of the impact of cyber risks. Indeed, AI's reasoning capability can facilitate the management of alerts by detecting false positives and recommending response actions (System Integrator E, Vendor D). In addition, AI's reasoning capability helps to determine the severity of a threat, for instance, in EDR solutions, AI helps assess the situation and determine if it needs to be addressed immediately (System Integrator E, Vendor D).

In addition, according to vendors and system integrators, AI **learning** capability can support risk assessment by enhancing the methods for determining the likelihood of cyber risks. In particular, it assists in analyzing behavioral patterns over time to assess the contextual legitimacy of user behavior based on historical access data. This enables determining whether a cyber risk is more or less probable and which events must be managed as a priority (Vendor B, System Integrator B).

On the other side, according to system integrators, AI's **reasoning** capability supports in determining and prioritizing the areas of vulnerability of a company to foster the improvement of its cybersecurity posture. Indeed, AI models can integrate public and private data sources to assess the vulnerabilities to which a company is most exposed (System Integrator E). In

addition, AI can support in the field of vulnerability management [4] by identifying which systems should be targeted for penetration testing [5] (System Integrator E, Consultancy B). Indeed, as System Integrator E said: *"starting from the data that you can collect, both public data and private data, [AI] can give me as an answer to what this company is most vulnerable to, what it should reallocate budget to, what technologies it should choose; something that helps you to do assessment."*

In addition, consultancies state that it is possible to exploit AI's **perception** capability to enhance third-party risk assessment with data that would otherwise be impossible for humans to analyze. In particular, AI's perception capability enables to assess the current level of protection of the SC and suggest adjustments as necessary. Indeed, AI's ability to perceive and process complex textual and contextual information can enhance the efficiency, scalability, and depth of cyber risk assessment activities. In addition, AI's perception capability can support the supplier assessment process by performing semantic analysis of massive documents to identify pertinent elements related to the level of cybersecurity, business continuity and data protection of suppliers (Consultancy B, Consultancy C). Furthermore, AI's perception capability can enhance threat intelligence solutions, particularly in the context of gathering and interpreting publicly available data related to suppliers and in the real-time scanning and interpretation of compromised credentials on the dark web [6] (Consultancy E).

Lastly, thanks to the advancements of generative AI models, consultancy companies state that they are also exploiting AI's **creativity** capability to improve vulnerability assessments. In particular, generative AI tools can augment the realism and intricacy of attack simulations by generating phishing emails that are linguistically and culturally tailored, or by simulating voices in vishing [7], thereby rendering the simulations more challenging (Consultancy D). In this way, AI's creativity capability enables a more precise assessment of the cybersecurity posture of companies and consequent improvements.

Table A3 (Appendix 3) summarizes the key constructs derived from the empirical evidence that underlie how the identified AI capabilities have a role in cyber risk assessment.

### *4.3 Risk treatment*

In the treatment phase, our findings indicate that AI capabilities support and transform the practices to respond to cyber risks in two ways.

From one side, AI enhances the treatment of cyber risks by enabling faster information processing, reducing the cognitive load of human analysts, and improving the overall responsiveness of cybersecurity systems. From the other side, AI is changing the routines of the people working in the cybersecurity domain, enhancing their effectiveness and efficiency, and enabling the transition from reactive to proactive cyber risk treatment.

In the first case, according to system integrators and consultancies, AI's **learning** capability plays a crucial role in supporting cyber risk treatment by enabling more timely, targeted and partially automated responses to the threats that have been identified. Indeed, learning models, upon detecting anomalies, can automatically suggest corrective actions to operators, enabling a faster and more precise response (Vendor A, System Integrator B).

In addition, vendors and system integrators highlighted how AI's **interaction** capability to communicate and collaborate with human users through natural and intuitive interfaces supports cyber risk treatment in the definition of mitigation strategies. In particular, management consoles complemented with AI tools can assist the users in responding to threats by guiding them through commands issued in natural language (Vendor A, System Integrator A, B, D).

AI's **creativity** capability also supports the definition of mitigation strategies for cyber risks. Indeed, system integrators exploit AI's creativity capability to support analysts in dealing with complex or unfamiliar scenarios. For example, System Integrator C uses large language models (LLMs), such as ChatGPT, to assist operators in addressing cyber risks in time-sensitive or unfamiliar situations, where operators may lack specific experience. AI's

**adaptation** capability is adopted in cyber risk treatment by all three cases to autonomously respond to evolving threat scenarios or to provide suggestions to respond to new threats. Indeed, AI's adaptation capability can provide automated remediation actions by acquiring knowledge from patterns over time and adapting promptly to mutated data and environmental conditions (Consultancy E, Vendor C) In addition, AI's adaptation capability can support human analysts by providing tailored information about the incident context, the affected systems and the involved users, allowing for a more precise and timely intervention (System Integrator D, Consultancy E).

Vendors and consultancies also leverage AI's **reasoning** capabilities to support risk treatment activities in SCCRM. Indeed, AI's reasoning capability can facilitate the automatic formulation of responses to potential threats by defining playbooks, sequences of actions meticulously designed to evaluate the situation at hand and determine the most effective course of action (Vendors B and D). In this way, rather than executing static, one-to-one remediation actions, operators can interpret complex scenarios more easily and select context-appropriate responses faster, starting from a list of predefined strategies.

Lastly, system integrators and consultancies exploit also AI's **perception** capability in supporting cyber risk treatment activities. Indeed, by analyzing data in different formats and identifying correlations among them, AI's perception capability assists the analysts in the definition of more informed responses to security events.

On the other side, AI can transform risk treatment practices by acting on the way cybersecurity operators work and adjusting the structural configurations of companies and SCs to prevent cyber risks.

According to vendors and consultancies, AI's **learning** capability enables the automation of repetitive, low-value tasks, such as ticket management and routine incident responses, improving the operational efficiency of security operations centers (System Integrator C and B). In addition, as Vendor A says, AI can help in: "*assessing potentially risky situations, such as abnormal behaviors, unusual connections, and similar indicators, and suggesting possible corrections to configurations, adjustments to permission grants, or changes in access regulations, and so on*". In this way, AI's learning capability supports the definition of preventive mitigation actions, shifting from reactive to proactive risk management (Consultancy E, Vendor A).

Vendors and system integrators instead show how AI's **interaction** capability can lower the technical barrier to engage with cybersecurity. In particular, by issuing suggestions in natural language to operators, AI's interaction capability allows operators to avoid navigating through many configuration tabs or writing complex queries, thus accelerating the response time to threats. Additionally, AI's interaction capability can provide preventive suggestions related to permission adjustments and documentation refinement, helping to anticipate potential threats.

Consultancies exploit AI's **reasoning** capability to enhance the speed and accuracy of incident resolution by enabling the system to automatically analyze and respond to threats (Consultancy A). In addition, by correlating alerts and verifying privilege assignments, AI's reasoning capability can help to identify and manage potential threats proactively (Consultancies A and B).

System integrators, instead, exploit AI's **creativity** capability to enable cyber risk professionals to manage the unexpected with greater confidence and agility. In particular, AI's creativity capability supports the operators in the incident response phase by generating new knowledge, thereby increasing the efficiency and effectiveness of responses to threats (System Integrator C).

In addition, according to consultancies and system integrators, AI's **perception** capability can improve risk treatment by enabling operators to respond to incidents more quickly. As System Integrator C says, AI's perception capability can be used "*For the process of gathering and analyzing information from public sources, in such a way that it allows us to collect the data, gather the information in a more timely manner and then analyze the individual texts in a faster manner to then give, through the output that is provided to us, a more timely service*".

Lastly, vendors are increasingly recognizing AI's **prediction** capability as a valuable asset in transforming cyber risk treatment. Indeed, AI's prediction capability supports risk treatment by enabling the anticipation of potential threats and recommending preventive actions to avoid incidents. Specifically, AI can detect statistically significant and recurring patterns of abnormal behavior, generating predictive and preventive recommendations based on aggregated intelligence (Vendor A). Additionally, AI can support threat modeling, a process that experts traditionally carry out manually, to anticipate potential attack vectors during software development (Vendor D).

Table A4 (Appendix 4) summarizes the key constructs derived from empirical evidence that underlie how AI capabilities have a role in supporting the definition of proactive and reactive cyber risk treatment strategies.

### *4.4 Risk monitoring*

In the monitoring phase, our findings indicate that AI capabilities support practices for detecting cyber risks by enabling the constant monitoring of systems, people and online sources.

In particular, system integrators exploit AI's **learning** capability in the context of cyber risk monitoring to address both system and behavioral aspects. Indeed, AI's learning capability enables the development of tools that facilitate the continuous observation and detection of behavioral deviations from historical patterns. In particular, by establishing behavioral baselines and identifying subtle deviations that static rule-based systems may overlook, AI's learning capability provides a foundation for real-time monitoring of systems and networks (System Integrator A and B).

AI's **adaptation** capability is also exploited by system integrators to enhance the monitoring of cyber risk. Indeed, it enables systems to dynamically adapt to evolving behaviors and threat patterns in real time. In particular, AI's ability to adapt to new inputs and behaviors not only improves the accuracy of threat detection but also accelerates it, allowing for a faster and more effective identification of emerging risks (System Integrator D and A). Indeed, as System Integrator A said: *"The ability to learn from the material and establish connections is inherent in the system, making analysis much faster and more efficient, resulting in significantly faster and more effective overall monitoring"*.

According to system integrators, AI's **reasoning** capability also contributes to the realm of cyber risk monitoring by enabling systems to interpret and correlate complex streams of data and draw logical inferences that mirror the analysis of expert cybersecurity operators. For instance, System Integrator D leverages this capability in threat intelligence platforms, where it not only allows gathering and organizing security data from multiple sources but also reasoning across events external to the company to detect broader patterns. This facilitates the monitoring of a more extensive array of data and the establishment of correlations among them, thereby contributing to the development of cybersecurity at the SC level.

Lastly, vendors exploit AI's **perception** capability in risk monitoring in the context of text analysis for dark web monitoring. Indeed, as Vendor B said: *"Another type of AI we use is related to semantics. When we automate certain types of analysis on the dark web, such as monitoring forums and similar platforms"*. In this way, AI's perception capability extends monitoring beyond the analysis of structured logs and data into the more ambiguous realm of human language, enabling organizations to gain earlier and deeper insights into evolving threats.

Table A5 (Appendix 5) summarizes the key constructs derived from empirical evidence that underlie how AI capabilities support cyber risk monitoring.

### *4.5 AI capabilities as dynamic capabilities improving SCCRM*

From the analysis of the results, we noticed that the findings of this study trace back to DCs theory (Teece *et al.*, 1997), which underscores the pivotal role of sensing, seizing, and transforming routines in enabling organizations to adapt to evolving environments (Teece, 2007). Indeed, cyber risks contribute to the creation of a highly dynamic and uncertain landscape, where the ability to identify, evaluate, respond, and continuously monitor cyber risks at the SC level becomes critical.

Our results show that the integration of diverse AI capabilities strengthens the routines underlying the basic constructs of DCs theory (Ellström *et al*., 2022): sensing of cyber risks, seizing them, and transforming routines and practices to better deal with them. Therefore, we started the second loop of our abductive process (Figure 1), and we systematically map how different AI capabilities support the sensing, seizing and transforming of cyber risks. We then linked these constructs to the four phases of the SCCRM, showing how DCs support the identification, assessment, treatment and monitoring of cyber risks. In the final results, AI-enabled functions for sensing cyber risks map onto SCCRM identification and monitoring phases, while those for seizing and transforming exhibit a dual role. They support seizing by enabling risk evaluation and immediate mitigation. They support transforming by driving reconfigurations of internal processes and interorganizational relationships. This theoretical framing provides the lens through which the results of this study can be read, showing how AI capabilities enhance the routines behind sensing, seizing and transforming, creating DCs that underpin SCCRM. This can be seen in Figure 3, which presents the final data structure resulting from our analysis.

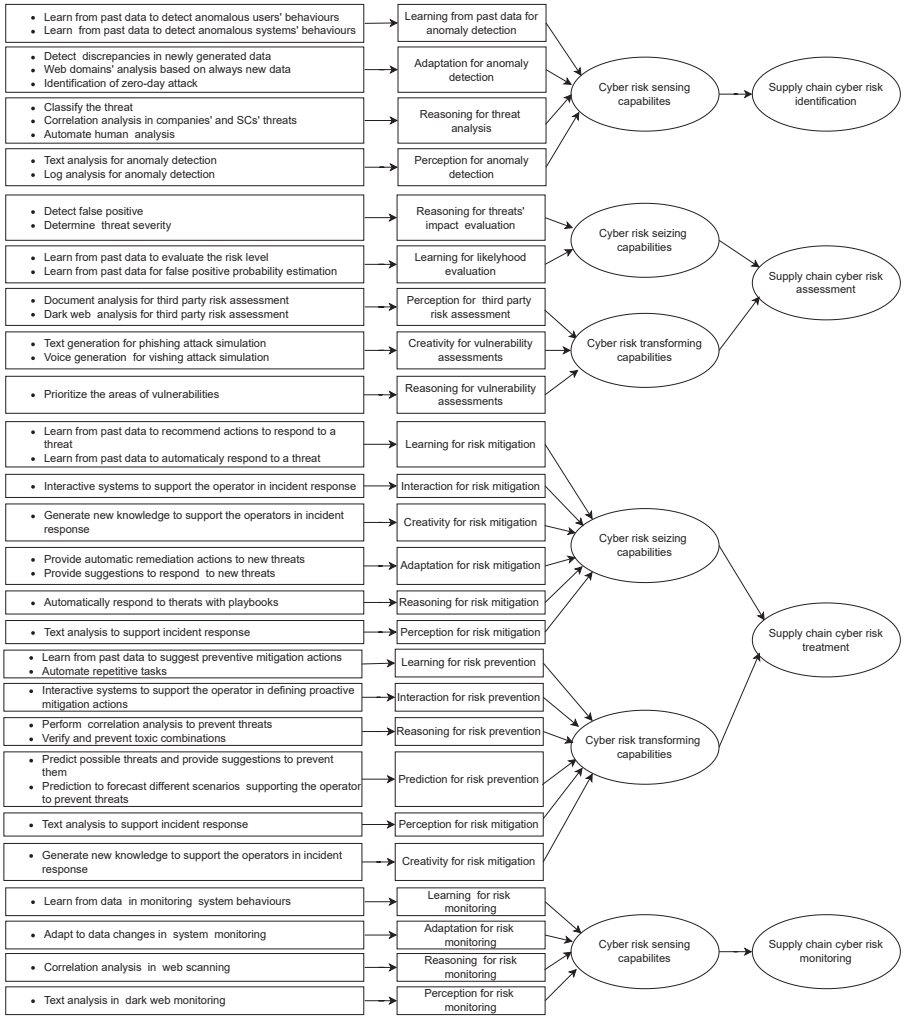


**Figure 3.** Data structure

In particular, our results show that AI learning, reasoning, adaptation and perception capabilities can facilitate the activities of anomaly detection and threat analysis. These activities, enabled by AI, constitute the routines behind cyber risk sensing, supporting the main activities needed in the identification of cyber threats. Learning supports the analysis of historical data concerning the behaviors of users and systems, to discern any alterations in them and to determine whether these alterations constitute a potential threat. Adaptation enables bringing AI's learning capability to the real-time domain. When something new is happening, adaptation supports in sensing if what is going on has a malevolent intent and therefore in detecting potential risks. Reasoning supports in better sensing the nature of the threats and their impact on the surrounding environment. Lastly, perception facilitates the sensing of risks starting from diverse sources by performing text or log analysis.

Then, AI capabilities can support risk assessment in SCCRM in two ways. First, by providing support for the assessment of the identified cyber risks, and second, by enabling the evaluation and improvement of the cybersecurity posture of the SC. Indeed, reasoning and learning capabilities support the seizing of the identified risks by incorporating practices for evaluating risk probability and impact, as well as detecting false positives. On the other side, perception supports the transformation of the risk assessment routines by encompassing risks external to the focal company, for instance, by exploiting document and dark web analysis to evaluate the cyber risk level of suppliers. In addition, creativity supports the enhancement of assessment activities through the implementation of advanced phishing and vishing simulations. Lastly, reasoning has been demonstrated to modify the practices that underpin the assessment of risks to better cope with the peculiar characteristics of cyber risks.

Similar to risk assessment, the results indicate that AI capabilities can support risk treatment in SCCRM in two distinct ways. By enabling the definition of reactive responses to cyber risks when they are detected, therefore supporting the practices behind the seizing of the identified risks. Learning, adaptation, reasoning and perception support the seizing of cyber risks by recommending response actions or automatically responding to a threat. Interaction and creativity instead help to seize cyber risks by providing support to the operator in the incident response phase. On the other side, learning, interaction, prediction, perception, reasoning and creativity capabilities support the redefinition of the routines of the people working in the cybersecurity domain, transforming the cyber risk treatment phase. In addition, they enable the development of proactive mitigation strategies by providing suggestions to the operators or automatically activating proactive mitigation actions. In this way, AI capabilities support the transforming of risk treatment routines by enhancing the efficiency and effectiveness of treatment activities and enabling the transition from reactive to proactive cyber risk treatment.

Lastly, AI learning, adaptation, reasoning and perception capabilities support risk monitoring in sensing risks across both the internal perimeter of the company and the whole SC, by improving the monitoring of systems', networks', webs' and users' behavior's. These AI-enabled activities contribute to the routines behind cyber risk sensing by supporting the identification of cyber risks. Specifically, learning supports the monitoring of systems to detect if anomalous behaviors happen. Adaptation enables to detect if anomalous patterns are emerging from the data that need to be analyzed. Reasoning supports in making correlations in web scanning, enabling the detection of risks that could impact the company's perimeter. Lastly, perception enables the sensing of risks through constant monitoring of the dark web.

## 5. Discussion

### *5.1 The adoption of AI in SCCRM*

A primary trend that has emerged from our analysis is the relatively rapid pace of adoption of AI in the context of SCCRM, which is substantially higher than that observed in traditional SCRM contexts. Indeed, despite the predicted benefits of AI in SCRM (Richey *et al*., 2023),

companies are struggling to adopt AI-based solutions (Ganesh and Kalpana, 2022; Gupta *et al*., 2021). In contrast, our findings demonstrate that in the domain of cyber risk management, the integration of AI technologies is more advanced and accelerated.

This finding was unexpected, as the existing literature on AI adoption in cyber risk management is less developed than the literature on AI adoption in SCRM. Consequently, we anticipated a slower pace of advancements in AI adoption as well. Nevertheless, the findings of this study highlight a divergent observation that prompted further investigation. In particular, the higher level of AI adoption in SCCRM with respect to SCRM appears to be driven by two interrelated factors. First, the cybersecurity sector is characterized by rapid technological innovation (Kaur *et al*., 2023). This has resulted in a competitive landscape in which early adoption of AI is often critical to maintaining relevance and market position. In such environments, AI is not just a support tool, but a strategic asset (Kosutic and Pigni, 2022). It enables faster threat detection, automated response and scalable analysis, all of which are vital in protecting increasingly complex SC ecosystems. Second, the distinctive nature of cyber risks further substantiates the investment in sophisticated AI solutions. In contrast to numerous conventional SC risks, cyber risks are characterized as high-probability and high-impact events with the potential to rapidly propagate across interconnected systems (Herburger *et al*., 2024; Jazairy *et al*., 2024). This combination of frequency and severity has been demonstrated to increase the perceived return on investment of intelligent, adaptive and proactive security technologies (Fan and Stevenson, 2018; Oltramari and Kott, 2018). Consequently, AI emerges as a crucial response to the demands of a threat environment where manual processes and reactive strategies are no longer adequate. Thus, the following proposition is suggested:

*P1*. The unique characteristics of cyber risks act as strong drivers of AI adoption in SCCRM, fostering a faster and more widespread integration of AI solutions than in traditional SCRM domains.

In this way, this study makes a significant contribution to the emerging discourse on the management of cyber risks. Indeed, our findings confirm that there is no necessity to reinvent the wheel and that the SCRM process should be adapted to this particular class of SC risks (Jazairy *et al*., 2024; Pandey *et al*., 2020). However, cyber risks also present some unique characteristics that require dedicated measures within the four phases of the conventional SCRM process. At this higher level of analysis, the reasons for the increased adoption of AI become apparent.

### *5.2 The joint contribution of AI capabilities for the different phases of the SCCRM process*

The literature has widely theorized about the benefits of AI in cybersecurity (Corbett and Sajal, 2023; Kaur *et al*., 2023; Zeadally *et al*., 2020) and how specific algorithms can be used to improve it (Chan *et al*., 2019; Kaur *et al*., 2023; Wiafe *et al*., 2020). However, a notable gap remains in the literature on how AI can improve SCCRM (Chan *et al*., 2019; Walshe *et al*., 2021; Zeadally *et al*., 2020). This study analyzes how different AI capabilities are leveraged in the different phases of the SCCRM process, providing a taxonomy of how AI can address the problems encountered in cybersecurity.

In general, our findings reveal that effective cyber risk management in SCs does not rely on a single AI capability, but rather on the synergistic combination of multiple capabilities. This perspective aligns with the findings of Jackson *et al*. (2024), who argue that AI capabilities rarely exist in isolation and often require integrated functioning to achieve their full potential. In particular, the analysis of our findings shows that specific combinations of AI capabilities play different roles in the different phases of the SCCRM process. And what emerged is that these combinations support three broad categories of activities: the sensing of cyber risks, the seizing of cyber risks, and the transforming of cybersecurity practices and settings in companies and SCs to counteract cyber risks, recalling DC theory (Teece *et al*., 1997). In this

way, our findings contribute to extant literature by applying DC theory to a novel context: AI adoption in SCCRM. This article demonstrates how distinct AI capabilities function as microfoundations of the dynamic capabilities of sensing, seizing and transforming. It is important to note that the application of these diverse capabilities does not progress in accordance with the stages of the SCCRM process. Rather, it is shaped by the development of sensing, seizing and transforming capabilities. Indeed, a limited number of AI capabilities (i.e. learning, reasoning, adaptation, and perception) support cyber risk sensing in the identification and monitoring phases. Other capabilities progressively add to support the seizing of cyber risks (interaction and creativity), and the full spectrum of capabilities is exploited in transforming. This extends the existing body of literature on the subject by presenting AI capabilities as cumulative rather than alternative in the context of AI adoption in SCCRM.

Sensing refers to the capability to actively scan and monitor the business environment to detect emerging threats and opportunities (Teece, 2007). From the analysis of the results, it emerged that AI capabilities support the sensing of cyber risks by improving anomaly detection, threat analysis and systems, web and people monitoring. Therefore, sensing capabilities improve the phases of risk identification and monitoring in SCCRM. Our findings indicate that sensing is strengthened by the AI capabilities of reasoning, learning, perception and adaptation. In particular, AI's learning capability emerged as the most prominent in cyber risk detection. Indeed, through the training of AI-based systems to recognize behavioral baselines of users and technologies, anomalies that may signal potential threats can be detected. This result supports the existing literature on the fundamental role of machine learning in cybersecurity (Kaur *et al*., 2023; Martínez Torres *et al*., 2019). However, as AI technologies advance, the learning process is no longer static or historically bound. In contrast, it becomes contextual and responsive, requiring systems to interpret deviations in real time and respond to previously unseen situations (Ansari *et al*., 2022). In this context, AI's perception and adaptation capabilities play a critical complementary role. Adaptation enables not only the detection of patterns from historical data, but also to continuously adjust to the changing environment, enabling the operator to detect anomalies unknown before. Perception instead helps in the monitoring of systems', webs', and people's behavior. Indeed, by enabling the collection and analysis of structured and unstructured data, it offers increased visibility into threat signals. This perspective contributes to the literature in the field of cybersecurity, which characterizes the domain as an ongoing arms race between attackers and defenders (Herburger *et al*., 2024; Radanliev *et al*., 2020; Taddeo *et al*., 2019). Our results show that, in this dynamic, the ability of the defenders to leverage AI's adaptation capability becomes a key strategic advantage. Furthermore, AI's reasoning capability can support analyzing, correlating and classifying anomalies by simulating the interpretive logic of a cybersecurity analyst. In addition, preliminary use cases indicate the implementation of AI's reasoning capability to correlate events across distributed environments, thereby extending risk monitoring beyond the individual firm to encompass broader ecosystem-level threats. These results answer the recent call for the extension of cybersecurity at the SC level (Berry, 2023; Colicchia *et al*., 2019; Creazza *et al*., 2022). Overall, the integration of learning, adaptation, perception and reasoning capabilities enables AI to enhance the phases of risk identification and monitoring in SCCRM, thus supporting the sensing capability. The following proposition is therefore formulated:

*P2.* AI capabilities of learning, adaptation, perception, and reasoning reinforce the sensing of cyber risks, facilitating risk identification and monitoring in SCCRM.

Seizing activities support firms in addressing sensed threats and risks (Teece, 2007). In the context of SCRM, the literature links seizing to the evaluation and prioritization of threats and the initiation of corrective actions. Specifically, it reflects the ability to assess and prioritize identified risks, select appropriate countermeasures and respond promptly (Ambulkar *et al*., 2015; Herburger *et al*., 2024). Within the scope of this study, AI capabilities support the seizing of cyber risks by improving some of the activities related to risk assessment and risk treatment

in SCCRM. According to our results, seizing practices can be developed by adding creativity and interaction capabilities to the set of AI capabilities already developed for sensing cyber risks. Indeed, our findings underline the pivotal role of reasoning and learning capabilities in assessing cyber risks. Specifically, reasoning facilitates the analysis of large volumes of heterogeneous data by AI systems, helping to evaluate the impact of detected risks. This includes the identification and elimination of false positives, as well as the prioritization of critical threats through logical inference and pattern recognition. On the other hand, learning facilitates the evaluation of risk probability, as AI systems accumulate knowledge from historical data to assess the likelihood that specific threats will materialize under specified conditions. This dual perspective aligns with the traditional view of risk assessment in the SCRM literature, which conceptualizes it as a combination of probability and impact estimation (Fan and Stevenson, 2018; Manuj and Mentzer, 2008). Once cyber risks have been assessed, risk responses are drafted. Our findings show that learning, reasoning and adaptation often work synergistically to analyze historical data, assess response options and suggest appropriate actions to human operators or initiate automated remediation actions for standardized and recurring threats. In addition, perception enables text analysis to support the operator in the incident response phase. These results contribute to the literature on the role of AI in providing operational decision support (Naik *et al*., 2022). In particular, our findings extend the previous literature by illustrating how AI moves beyond augmentation (Ivanov, 2020; Paul *et al*., 2020) to automation of risk responses, showing how the capabilities developed for sensing cyber risks also play a fundamental role in supporting seizing. To this established set, two additional capabilities can be added: interaction and creativity. AI's interaction capability emerged as a game changer in risk treatment, especially in operational environments such as security operations centers. Chatbots and natural language interfaces can indeed provide real-time support to operators by suggesting procedures, retrieving contextual information and guiding them through the response process, therefore improving the overall efficiency and effectiveness of their operations. This contributes to the developments of the recent literature, which has emphasized the growing importance of interactive systems in decision-making, leading to increased efficiency and reducing the cognitive load of operators during time-sensitive interventions (Durach and Gutierrez, 2024). Furthermore, as cyber threats evolve rapidly, often outpacing the capacity of traditional defense systems (Taddeo *et al*., 2019), creativity becomes essential. AI's creative capability enables systems to generate new forms of knowledge, helping operators navigate unfamiliar or ambiguous attack scenarios. By simulating possible responses or generating novel countermeasures, AI empowers defenders to act in dynamic and uncertain contexts, where predetermined rules or past experiences may fall short. In this way, this research answers recent calls in the cybersecurity literature for the use of generative AI to strengthen organizational preparedness (Gupta *et al*., 2023; Sai *et al*., 2024). Therefore, the integration of interaction and creativity into the capabilities already developed to support the sensing of cyber risks helps to seize the sensed risks, enhancing the phases of risk assessment and treatment in SCCRM. Based on this reflection, the following proposition is developed:

*P3.* AI's interaction and creativity capabilities add to the already established set of capabilities developed to support sensing routines to reinforce the seizing of cyber risks, supporting risk assessment and treatment in SCCRM.

Transforming is related to aligning and realigning resources and competencies to ensure a strategic fit with sensed and seized risks. In particular, it involves redesigning internal and external security standards to reduce future vulnerability (Ambulkar *et al*., 2015; Herburger *et al*., 2024; Teece, 2007). Transforming is where the full spectrum of AI capabilities becomes operationalized in SCCRM, adding prediction capability to the previously developed set. Specifically, AI's creativity and reasoning capabilities support risk assessment routines, enabling the continuous evaluation of the company's cybersecurity posture to detect and prioritize vulnerabilities to prevent cyber risks. In particular, AI's creativity capability offers

unique value in the cybersecurity domain, enabling the evaluation of an organization's cybersecurity posture, its present capacity to resist, respond to, and recover from cyber threats (Radanliev *et al*., 2020). Indeed, the participants emphasized the use of generative AI tools, such as LLMs and voice synthesis systems, to simulate phishing and phishing attacks. In this context, AI not only enhances defensive training but also enables alignment between attack and defense strategies. This answers the literature call to identify a solution to the increasing sophistication of cyberattacks (Taddeo *et al*., 2019). Furthermore, perception capability has the potential to expand the scope of risk assessment beyond the boundaries of a single organization, thus encompassing the broader spectrum of extended SCs. Although the literature frequently notes a lack of cybersecurity collaboration between SC partners Boyson (2014), Colicchia *et al*. (2019), Creazza *et al*. (2022), our findings suggest that AI's perception capability can act in this direction, allowing proactive dark web monitoring and the assessment of the cybersecurity posture of suppliers and customers. AI, therefore, can help overcome the prevailing challenges associated with collaboration among stakeholders within the cybersecurity domain (Creazza *et al*., 2022). Specifically, it facilitates the implementation of alternative strategies, such as the passive monitoring of the parent company's partners, thereby ensuring comprehensive protection. Moving to risk treatment, AI capabilities support the reconfiguration of practices and operational activities in cyber risk treatment to be better aligned with the dynamic cyber risk environment. Learning, reasoning and perception capabilities enable enlarging the scope of risk treatment beyond the remediation of incidents to encompass the anticipation of threats and the implementation of proactive mitigation strategies. This is extremely relevant in SCCRM, due to the unique characteristics of cyber risks of higher undetectability and more severe consequences (Herburger *et al*., 2024). In this way, this research further extends SCRM literature to SCCRM (Fan and Stevenson, 2018; Ritchie and Brindley, 2007). Interaction and creativity support transforming by changing the routines in cyber risk treatment. Through the support of chatbots and generative AI systems, people working in cybersecurity can increase the efficiency and effectiveness of their operations, delegating to AI the most repetitive tasks and dedicating themselves to more value-added activities. This contributes to the literature debate between automation and augmentation by stating that AI can reshape organizational routines, supporting reallocation from operational to higher-value tasks (Susarla *et al*., 2023; Wessel *et al*., 2025). In addition, AI's prediction capability assumes a pivotal role in transforming cyber risk treatment. Indeed, AI prediction capability adds to the set of already established ones to prevent risk occurrence and ensure long-term risk protection. Predictive models help identify which systems are most vulnerable, which suppliers pose the highest risk, or what type of incidents are more likely to occur. This enables companies to take preventive action before disruptions arise, contrasting the high dynamicity of the cybersecurity environment (Taddeo *et al*., 2019). Overall, the combination of all the AI capabilities facilitates the transformation of companies and SCs by assisting them in enhancing their cybersecurity posture and implementing preventive measures to better prepare for future cyber risks, acting on the phases of risk assessment and treatment within the SCCRM framework. Therefore, the following proposition has been developed:

*P4.* AI's Perception capability adds to the already established set of capabilities developed to support sensing and seizing routines to reinforce the transforming capabilities of companies to make them able to better deal with SC cyber risks, supporting risk assessment and treatment in SCCRM.

Overall, the findings of this study indicate a clear predominance of reasoning, learning and adaptation capabilities across AI applications in SCCRM. These capabilities leverage the substantial amount of data available to automatically learn, make decisions, improve from experience and infer facts (Jackson *et al*., 2024; Samoili *et al*., 2020). The extensive utilization of these capabilities reflects the wide adoption of machine learning and deep learning algorithms in the cybersecurity and SCRM literature (Baryannis *et al*., 2019; Ganesh and

Kalpana, 2022; Nila *et al*., 2020). However, the findings of this study also suggest a notable shift driven by the emergence of LLMs and generative AI. Indeed, they have given rise to capabilities such as perception, interaction, creativity and prediction that are becoming increasingly prominent, particularly in tasks that require flexible problem-solving and human-AI collaboration (Jackson *et al*., 2024). These capabilities are also relevant to address the shortage of skilled cybersecurity professionals, as they offer scalable and intelligent support to human analysts during complex or ambiguous scenarios. This trend is in accordance with the emerging body of literature, which underscores how advances in interactive and generative algorithms are expanding the functional scope of AI (Durach and Gutierrez, 2024; Gupta *et al*., 2021; Jackson *et al*., 2024). Our results expand the previous literature by showing how generative AI is increasing the pace of AI adoption in SCCRM. Therefore, the following proposition has been developed:

*P5*. While reasoning, learning and adaptation remain the most prevalent AI capabilities in SCCRM, advances in generative AI are accelerating the adoption of perception, interaction, creativity and prediction capabilities.

In Figure 4, a high-level overview of the results is provided, demonstrating how the diverse AI capabilities contribute to sensing, seizing and transforming, and to the different phases of the SCCRM process. This can be seen as a potential pathway that companies may follow when implementing AI in SCCRM, suggesting a stepwise logic behind the development of AI capabilities for SCCRM. Indeed, a preliminary step in the implementation of AI could be to exploit the more robustly established AI capabilities of learning, reasoning, adaptation, and perception. Indeed, these capabilities provide the basis for sensing cyber risks, seizing them, and developing some initial transforming capabilities. Moreover, the implementation of these four capabilities could facilitate all the phases of the SCCRM process. In addition, providers widely offer these capabilities, and therefore, they are easily accessible as they are present in a multiplicity of solutions available on the market.

However, at this stage, improvements in seizing and transforming remain limited. Therefore, a subsequent step could be to further strengthen the seizing capability by adopting perception and creativity capabilities. These capabilities are still in a nascent stage of development, following the emergence of LLMs and generative AI tools. Nevertheless, these two capabilities have the potential to broaden the scope of risk assessment and treatment in SCCRM. In particular, they facilitate the evaluation and management of unfamiliar scenarios by providing real-time support to operators and helping them navigate unfamiliar attack scenarios, dealing with the evolving threat landscape. Together, these capabilities already create a strong foundation for organizational transformation, enabling firms to adapt more effectively to highly dynamic cyber risk environments.

However, to fully realize the potential of transforming, firms may take a subsequent step in which they acquire AI's prediction capability that supports the definition of preventive actions and suggests corrective action to increase the level of security before disruptions occur. With the addition of this AI capability, it is possible to further strengthen the risk assessment and treatment phase, changing the routines of people working in cybersecurity and allowing the transition from reactive to predictive risk management, enabling the transforming of the cybersecurity posture of a company and its SC. These findings align with recent literature, which underlines the need to transform risk management into a dynamic and proactive process through continuous adaptation and real-time threat intelligence (Zaydi *et al*., 2025).

This pathway underscores the cumulative nature of AI capability development. It has been demonstrated that a set of four AI capabilities is indeed effective in supporting the phases of risk identification and assessment in sensing cyber risks. These capabilities also support the risk assessment and treatment phases by enabling the seizing of cyber risks and some transforming activities. Nevertheless, a comprehensive assessment of cyber risks necessitates the incorporation of interaction and creativity into the existing set of capabilities to have real-time support and to be able to deal with new threat scenarios. Moreover, in order to achieve a

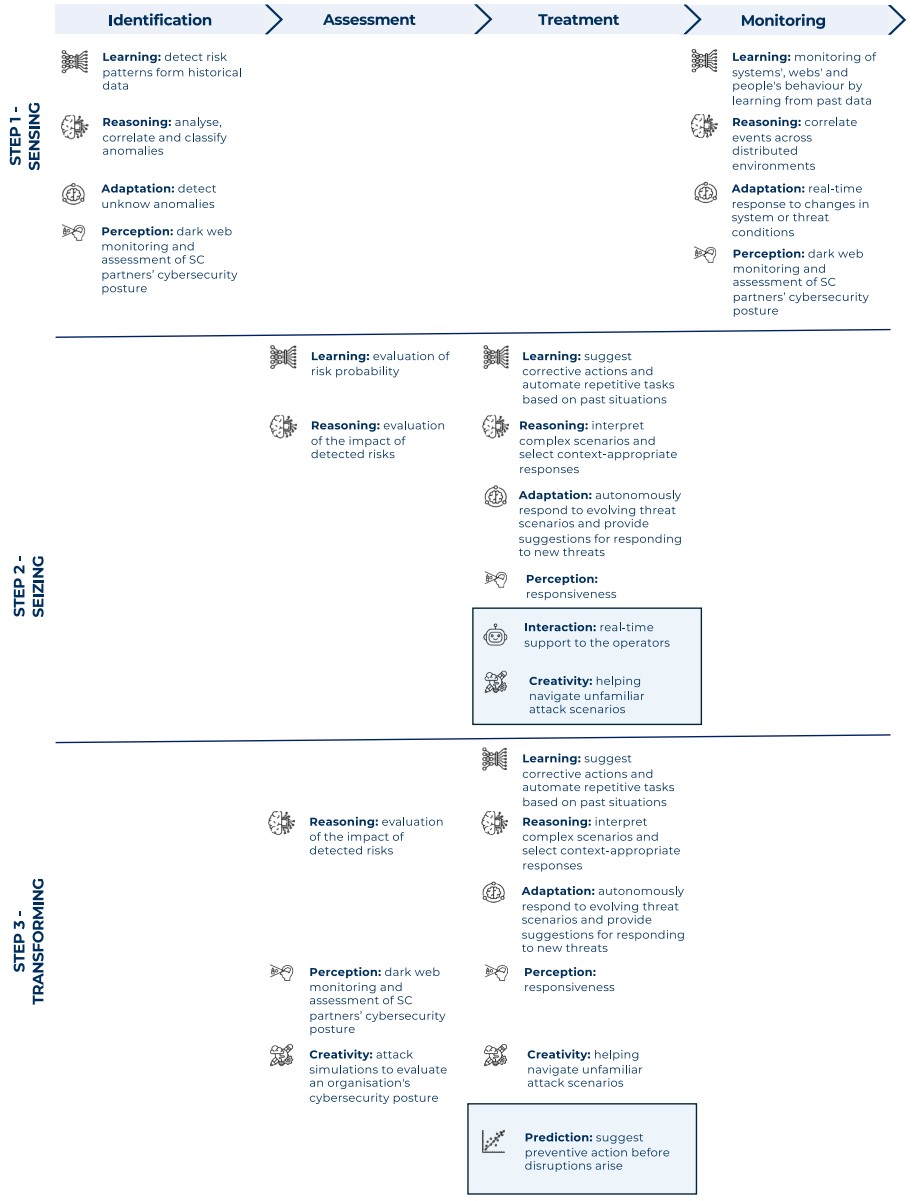


**Figure 4.** Roadmap for AI implementation in SCCRM

comprehensive transformation of the SC cybersecurity posture, it is imperative to incorporate also prediction capability to move from a reactive to a proactive SCCRM. Consequently, the enhancement of SCCRM can be pursued gradually, contingent upon the firm's available resources, as there is no imperative to develop the entire array of dynamic capabilities instantaneously to improve SCCRM. However, to grasp the full potential of AI in SCCRM, developing the full set of capabilities is necessary.

*5.3 Different capabilities for different actors*

The cross-case analysis reveals distinct patterns in how AI capabilities are leveraged in the SCCRM process in the three cases. Vendors emerged as the most technologically advanced in their operationalization of AI for risk prevention. They are the only ones that systematically employ AI's prediction capability to anticipate threats before they materialize, particularly through risk scoring systems and the suggestion of proactive adjustments. Furthermore, vendors are the most committed to automation, as they are the only ones that rely on AI to automatically respond to threats, implementing full playbook-based remediation strategies without human intervention. This advancement can be related to their business model, expertise and the nature of their services. Vendors are indeed the most focused on offering the most advanced technological paradigms and therefore, since attackers are moving faster (Taddeo *et al*., 2019), they are the ones that can develop these advanced IT security tools to counter them (Colicchia *et al*., 2019). By contrast, system integrators distinguish themselves through their focus on adaptive defense mechanisms. They are uniquely engaged in deploying AI adaptation capabilities to address zero-day attacks, where traditional detection methods fail. Moreover, they are the only group that emphasizes the use of interaction and creativity capabilities in the risk treatment phase. Indeed, they employ generative AI tools to simulate new attack scenarios and support security operations center analysts with conversational interfaces for real-time response. This answers the recent call in the cybersecurity literature for leveraging generative AI to strengthen organizational preparedness (Gupta *et al*., 2023; Sai *et al*., 2024). System integrators also stand out for their application of AI in the risk monitoring phase, suggesting a broader view of continuous cyber risk management, responding to the needs highlighted in the current literature (Herburger *et al*., 2024). The fact that they are so active in themes that are now being asked for in the literature and by companies is mainly related to the nature of their business, which is more focused on the implementation than on the software development. Consultancies, on the other hand, adopt a more SC-oriented perspective. They are the only group to apply AI to third-party risk assessment, enabling organizations to evaluate the cybersecurity posture of external partners and suppliers. Indeed, they embrace the idea that cybersecurity should be an end-to-end SC process, encompassing not only technology but also processes and people (Colicchia *et al*., 2019; Creazza *et al*., 2022). AI supports this paradigm shift, improving visibility and transparency (Ganesh and Kalpana, 2022; Hangl *et al*., 2023) and therefore increasing accessibility and adoption of SC-focused solutions. In line with this, consulting firms are also pioneering the use of AI creativity for vulnerability assessment, developing simulations and diagnostic tools that enhance the strategic planning and prioritization of security audits. This is intrinsically related to the core business of the case, which involves the exploitation of technical solutions implemented by vendors or system integrators and is focused on more organization-oriented and awareness solutions (Colicchia *et al*., 2019). Consequently, the organization's innovation process is predominantly focused on these phases. This differentiation suggests that each type of actor plays a complementary role in shaping the SCCRM landscape through AI, reflecting their respective positions in the value chain and their strategic priorities. This contributes to the literature that emphasizes how in SCCRM different actors have different complementary behaviors according to their role in the SC (Choi *et al*., 2001; Wieland, 2021). Based on these findings, the following proposition is therefore formulated:

*P6.* Different actors in the cybersecurity ecosystem configure AI capabilities in SCCRM according to their strategic role and the solutions they aim to offer.

## 6. Conclusions

The present research focuses on the management of cyber risks in SCs, advancing the field of SCCRM, an area at the intersection between SCRM and cybersecurity literature. This research addresses a significant gap in the existing literature on the subject. Indeed, the evolution of AI applications has prompted SC researchers to explore the potential of AI in SC processes (Richey

*et al*., 2023). However, there is a paucity of research on the application of AI capabilities in SCCRM, with only a few studies that address AI applications in specific cybersecurity solutions. Therefore, the present article explores the application of different AI capabilities in the different phases of the SCCRM process through three embedded case studies.

### *6.1 Theoretical contributions*

This study contributes to theory by bridging the emerging field of SCCRM and AI adoption, which has not yet been investigated in the literature. Indeed, while some research has explored the role of AI in SCRM (Baryannis *et al*., 2019; Ganesh and Kalpana, 2022) and cybersecurity (Taddeo *et al*., 2019; Zeadally *et al*., 2020), studies on its application in SCCRM are still lacking.

In order to do so, we introduced some foundational constructs of the SCRM field and extended them to SCCRM, trying to uncover how they can be adapted to address the unique challenges of cyber risks. In doing so, we align with Jazairy *et al*. (2024), who state to avoid reinventing the wheel when investigating the SC cybersecurity phenomenon and, instead, ground future inquiry in established, albeit adapted, SCRM knowledge. Therefore, we consider the SCCRM process as an adapted version of the SCRM one. In particular, we built on the models of Pandey *et al*. (2020), but also incorporated the risk monitoring phase, a phase that has not been considered in their model, but that is essential in the context of cybersecurity (Herburger *et al*., 2024; Kosmowski *et al*., 2022).

In this setting, we considered the AI capabilities introduced by Jackson *et al*. (2024) to see how they can act in the SCCRM landscape. Indeed, in line with some recent research in operations and SC management (Jackson *et al*., 2024; Kaur *et al*., 2023), we would like to focus on what AI tools can do rather than how they are technically built, as we believe that from a SC perspective, the specific algorithm used is often secondary to the functionality it enables. In fact, this shift in perspective is crucial to capture the managerial relevance and operational impact of AI in SC contexts (Jackson *et al*., 2024).

Empirically studying how AI capabilities can be exploited in the pursuit of SCCRM provides a new perspective on AI applications in SCRM and lays the foundation for further research in this area. With this research, we address the lack of knowledge about how and which cybersecurity solutions can be impacted and supported by the potentialities of AI from a SCCRM perspective, a topic that needs further exploration in the literature. Indeed, the existing contributions mainly deal with specific and technical implementations of AI algorithms that address a particular cybersecurity task (Yang *et al*., 2023; Zeadally *et al*., 2020). And, even if some mapping studies have been performed (Chan *et al*., 2019; Walshe *et al*., 2021; Zeadally *et al*., 2020), none of them target the role of AI in SCCRM. The present study contributes to the extant literature on the subject by demonstrating how AI capabilities are adopted in the different phases of the SCCRM process. In particular, the findings of the study reveal a relatively high rate of adoption of AI capabilities in the SCCRM process, which is higher than the rate of adoption in more general SCRM processes.

In particular, the findings of the study show that different AI capabilities combine to support different phases of the SCCRM in a way that can be traced back to the DC theory (Teece *et al*., 1997). Indeed, specific combinations of AI capabilities have been demonstrated to facilitate the sensing of cyber risks, the seizing of those risks, and the adaptation of companies to the dynamic environment caused by cyber risks. We therefore contribute to the theoretical discourse on AI adoption in SCCRM by framing it in DC theory. In the literature, there has been extensive discussion about the definition of DC needed to ensure cyber risk protection (Herburger *et al*., 2024; Jazairy *et al*., 2024). We set in this discourse by extending it from the resilience field to the more comprehensive SCCRM area and linking it deeply with AI adoption.

Furthermore, our findings show that the adoption of AI capabilities in SCCRM is a process that occurs in a cumulative and step-based manner. Specifically, we have developed a

framework that illustrates how the diverse AI capabilities contribute to sensing, seizing and transforming, and to the different phases of the SCCRM process. and consequently to the various phases of the SCCRM process. As demonstrated by this framework, a skeleton consisting of learning, reasoning, adaptation, and perception capabilities has the potential to support companies in all phases of the SCCRM, thereby enhancing their ability to sense cyber risks, seize them and partially transform the cybersecurity settings of companies and SCs. However, to fully enable seizing and transforming activities, other capabilities need to be progressively added to further improve the phases of risk assessment and risk treatment.

Moreover, the present findings contribute to the extant literature by demonstrating that different actors utilize different AI capabilities to support the SCCRM process. In particular, they fulfill a complementary role in the improvement of SCCRM through AI, reflecting their respective positions in the value chain and their strategic priorities.

Lastly, we make a significant contribution to the extant literature by formulating six propositions that elucidate the progression of AI adoption in SCCRM, the ways in which AI capabilities can support the various phases of the process and how different actors in the cybersecurity landscape make use of them. These propositions are the result of an interpretation of the findings, developed from multiple pieces of evidence. However, given the exploratory nature of the study, which sought to theorize about the adoption of AI in SCCRM, these propositions need to be tested in a broader empirical setting to ensure their generalizability.

### *6.2 Managerial contributions*

From a managerial perspective, this article serves first as a foundation for addressing the significant knowledge gap in companies about the relevance of SCCRM. Although companies are beginning to be aware of the importance of cybersecurity at the company level, their knowledge at the SC level is still scarce (Colicchia *et al*., 2019; Ghadge *et al*., 2020). These findings offer valuable insights for practitioners, increasing their awareness of the importance of defining a proper process to manage cyber risks at the SC level.

Second, the objective of this research is to provide a structured framework to support managers' decisions by offering a comprehensive overview of how AI can be applied within the SCCRM context. As illustrated in Figure 4, a framework is proposed to show how the diverse AI capabilities contribute to sensing, seizing and transforming, and to the different phases of the SCCRM process. This framework delineates a progressive implementation pathway that organizations can follow when embarking on AI implementation projects in SCCRM. This framework provides managers with a practical guide to which AI capabilities are best suited for specific tasks such as sensing, seizing or transforming. It also outlines which phase of the SCCRM process each capability is intended to tackle. In addition, it offers brief descriptions of the specific functionalities of each capability in SCCRM.

This research also aims to make companies aware of how AI capabilities can reduce response time and alleviate resource constraints, thus improving their performance. Indeed, this research highlights how AI capabilities can improve the efficiency and effectiveness of all phases of the SCCRM process. In this landscape, the growing relevance of generative AI tools presents an opportunity to grasp. Indeed, the creation and interactive AI capabilities can support less experienced personnel during high-pressure situations, such as incident response. Managers should view these tools not only as support systems but as enablers of knowledge transfer, training, and rapid onboarding. Furthermore, while the majority of contemporary AI applications in SCCRM are designed to support and enhance human decision-making processes, this study demonstrates that automation is becoming increasingly feasible within the SCCRM domain.

Furthermore, AI can improve cybersecurity within the SC due to its capabilities in managing third-party cyber risks. As highlighted in this study, tools that utilize AI for textual and behavioral analysis can assess the cybersecurity posture of partners without the need for

direct interaction. It has been demonstrated that this can resolve numerous issues related to lack of trust, system integration and privacy concerns (Colicchia *et al*., 2019; Herburger *et al*., 2024). Managers must recognize these possibilities, and this research demonstrates the manner in which self-driven approaches to supplier monitoring and intelligence sharing functions act in this direction, progressing toward more transparent and data-driven collaborations.

### *6.3 Limitations and further developments*

This article has some limitations that open avenues for future research. First, it should be noted that the cases under consideration exclusively involved providers, thereby omitting user perspectives due to their resistance and limited awareness of the topic. Involving adopters in future research could offer valuable insights into the role of AI in SCCRM, thus providing a counterbalance to the predominantly optimistic perspectives of providers and offering insight into the challenges associated with the implementation of SCCRM. Involving adopters could also facilitate the evaluation of the applicability of findings across different industries. It is suggested that future research in this field will investigate how AI can be exploited in different SC structures, particularly in SCs characterized by a high level of criticality or complexity, thereby providing a more nuanced reflection on the subject.

Second, the research adopts the perspective of the focal company implementing cybersecurity solutions targeting its SC, sometimes also directly or indirectly involving suppliers. Nevertheless, the implementation of such solutions at the SC level remains limited due to a combination of factors, including issues related to trust, challenges in system integration and concerns about privacy (Colicchia *et al*., 2019; Herburger *et al*., 2024). It is recommended that future studies seek to investigate this topic in depth by involving multiple SC players to gain insight into the relational aspects of SCCRM. A comprehensive study involving all actors in commercial relationships, especially small suppliers, which are typically the most vulnerable to cyber risks and have fewer financial resources, could expand the knowledge on the topic. Such studies would examine how these factors could prevent the implementation of AI in SCCRM and which strategies can be implemented to overcome these issues.

Third, effective SCCRM requires not only technological solutions, but also a series of organizational initiatives aimed at developing a robust organizational structure and a well-trained workforce (Colicchia *et al*., 2019; Zeadally *et al*., 2020). In this research, we focus more on the technological part, studying how a specific technology can help in SCCRM. However, according to the socio-technical perspective (Lyytinen and Newman, 2008), technology should evolve with people to ensure that maximum value is delivered to the organization. Some studies have already demonstrated the socio-technical nature of AI adoption in SC management (Colombo *et al*., 2023), however, the current research does not address this perspective. Therefore, it is recommended that future research focus on the interaction between social and technical dynamics in SCCRM. This could also be interesting in light of the emergence in the literature of a strong discussion about the augmentation and automation paradigm and the development of hybrid intelligences (Burger *et al*., 2023; Jarrahi *et al*., 2022; Van Der Aalst, 2021). Indeed, from our findings, it emerges that AI can have a double role in SCCRM: substitution due to task automation or complementarity related to supporting professional evolution. However, in the current research, the subject is only referenced in the context of the various AI capabilities and their respective roles in the execution of specific SCCRM tasks; it does not represent the core focus of our analysis and discussion, as in Colombo *et al*. (2023). Therefore, future research could combine the socio-technical system perspective with the automation-augmentation paradox to better explore how AI adoption can simultaneously impact the technical and social dimensions of SCCRM.

Fourth, AI is a developing topic, and companies are starting to learn how to incorporate it in SCCRM. Our results show that companies do not take advantage of all the different capabilities in the same way. Indeed, there is a clear predominance of reasoning, learning, and

adaptation capabilities, while interaction, perception, prediction and creativity capabilities are still in their nascent phase. This is partly related to the fact that the first ones are more mature in terms of market presence and implementability, while the second ones are relatively new, developed following the emergence of LLMs and generative AI tools. Despite this preliminary discussion, we are aware that a more thorough investigation is required into the reasons why certain capabilities are more frequently exploited than others and whether there are other factors to consider in their adoption. We therefore suggest this as a potential avenue for future research to encourage further exploration into how these emerging capabilities can enhance SCCRM practices in the coming years. In particular, a longitudinal approach would also allow for consideration of the evolving technological landscape and the provision of a comprehensive view of the field's dynamics and challenges.

Finally, as AI is a developing topic, there is also a strong need to theorize within AI contexts. In our abductive research, we traced back to Teece *et al*. (1997) DCs theory as an interpretive lens for explaining AI adoption in SCCRM. However, our results also show that AI adoption in SCCRM is a context-dependent process that varies from company to company. Therefore, future research may complement this study by adopting a contingency theory perspective. Furthermore, we posit that AI adoption in SCCRM is a step-based process rather than a one-time activity. It allows the development of different AI capabilities at different moments according to a company's available resources. Future research could therefore use Resource Orchestration Theory or Resource Advantage Theory to better understand the influence of resource constraints and how firms can strategically align and mobilize resources to gain a competitive advantage in developing AI capabilities. These proposed theoretical perspectives necessitate further investigation to substantiate their validity. Nevertheless, they could serve as a source of inspiration for the potential directions of future research that could expand upon the current results and address the growing need to theorize about AI.

**Acknowledgments**

The support of the Italian Ministry of University and Research, within the PNRR Piano Nazionale di Ripresa e Resilienza (PNRR) - (National Recovery and Resilience Plan), is gratefully acknowledged.

## Appendix 1

**Table A1.** Case study interview protocol

| Interview protocol |
|---|
| *Cybersecurity solutions offered* |
| What cybersecurity solutions does your company offer? |
| How many customers does your company serve? |
| What are the most common needs that your customers want to satisfy by adopting your solutions? |
| How are these solutions able to improve organizations' cybersecurity? |
| *Supply Chain Cyber Risk Management Process* |
| How do your solutions support your customers in doing cyber risk identification? |
| How do your solutions support your customers in doing cyber risk assessment? |
| How do your solutions support your customers in doing cyber risk treatment? |
| How do your solutions support your customers in doing cyber risk monitoring? |
| *Artificial Intelligence in Supply Chain Cyber Risk Management Process* |
| Do you adopt Artificial Intelligence in your solutions? |
| Which AI capability do you exploit in each of the different solutions? |
| In which of the SSCCRM process phases do you use Artificial Intelligence? |
| What is the value added by Artificial Intelligence to each specific phase? |

## Appendix 2

**Table A2.** AI capabilities in cyber risk identification: selected evidence

| Second-order themes | Selected quotes on first-order categories |
|---|---|
| Learning from past data for anomaly detection | *Learn from past data to detect anomalous users' behaviors*<br>"The AI, if it's a specialized engine, tells you, look, I detected, for example, abnormal behavior, so the access occurred at a different time than usual, by a different terminal than usual, you used a different communication channel than usual. So detection and reporting, that's another important aspect." – Vendor A<br>*Learn from past data to detect anomalous systems' behaviors*<br>"They go and identify precisely anomalies in the behavior of the system and then try to issue alarms, which then go to the operator, who can eventually intervene." – System Integrator C |
| Adaptation for anomaly detection | *Detect discrepancies in newly generated data*<br>"The identification of a malware by deep learning on a huge amount of samples, and then the identification of malware, regardless of how the malware behaves, but simply by a comparison of its own binary code." – System Integrator D<br>*Web domains' analysis based on always new data*<br>"We have anti-cybersquatting tools that deal with detecting those attacks that use squatting of domain URLs to conduct the attack. We use it to detect new threats that arise on the web. On the internet, domains, websites, etc. are registered continuously, we go and analyze them as they arise, and we have precisely AI tools that do this work for us." – Vendor C<br>*Identification of zero-day attack*<br>"We go to identify attack vectors through algorithms that not only in a static way go to identify that something is happening that should not be happening, but that also allows, through a series of parameters, to identify zero-day malware based on the interactions that this entity, like an external IP, has with us." – System Integrator B |
| Reasoning for threat analysis | *Classify the threat*<br>"The threat comes, it identifies it, figures out what it is, does the trace, rules out that it's a false positive, and follows a predefined playbook." – Vendor D<br>*Correlation analysis in companies' and SCs' threats*<br>"Profiling of the company to make those correlations that maybe we miss, or at any rate that would take too much time for a human being, in assessing all the various relationships that may be there. To have a smart Threat Intelligence tool that goes out and gathers information on the ecosystem as well, so the SC theme." – Consultancy D<br>*Automate human analysis*<br>"During the detection phase, we use algorithms meaning that once a large volume of data has been collected and normalized into a common schema, the next step is to bring AI into play to replicate the kind of analysis a cybersecurity specialist would perform, if they were able to process such a large amount of data in such a short time." – Vendor B |
| Perception for anomaly detection | *Text analysis for anomaly detection*<br>"We use AI to read what is written in chats. Through the use of keywords, the system can identify relevant content. When the AI encounters specific keywords that we've pre-defined, it raises a flag and signals that a human should review the content more closely." – Vendor B<br>*Log analysis for anomaly detection*<br>"We realized that this kind of expertise could be used in text analysis and we tried to apply it, we are also applying it on log analysis, with the very intent to recognize patterns and possible dangerous situations." – System Integrator C |

## Appendix 3

**Table A3.** AI capabilities in cyber risk assessment: selected evidence

| Second-order themes | Selected quotes on first-order categories |
|---|---|
| Reasoning for threats' impact evaluation | *Detect false positive*<br>"The threat comes, it identifies it, figures out what it is, does the trace, rules out if it's a false positive, and follows a predefined playbook." – Vendor D<br>*Determine threat severity*<br>"I perform an EDR analysis, assess the situation, and in the end determine that yes, this is indeed an attack that needs to be addressed immediately. For instance, if the incident involves the CEO'scomputer, it becomes a top-priority case." – Vendor B |
| Reasoning for vulnerability assessment | *Prioritize the areas of vulnerabilities*<br>"In the field of vulnerability management and penetration testing, AI can be leveraged to help prioritize which systems should be targeted for vulnerability assessments and penetration tests." – Consultancy B |
| Learning for likelihood evaluation | *Learn from past data to evaluate the risk level*<br>"We use a lot of machine learning because there is a theme of behavior analysis. If I make a legitimate access tomorrow morning from Florence, the system might say medium risk, she is always around Italy, it this access is legitimate to investigate. If tomorrow morning I make the legitimate access from Timbuktu, the alert is very serious. She is out of the business of Vendor B, It is not her." – Vendor B<br>*Learn from past data for false positive probability estimation*<br>"We go to identify a confidence score from 0 to 100, which allows you to say if it's 100, dear operator, it's a secure threat, so that event you have to handle it as a priority. Conversely, if it is, for example, 30%, we have less confidence that it is an actual cyber incident, as we know it." – System Integrator B |
| Perception for third party risk assessment | *Document analysis for third-party risk assessment*<br>"At the pre-assessment stage, indeed, it will definitely be supportive. To understand what are the clauses, what are the security measures implemented by the vendor and from there the match and mismatch can definitely allow you to speed up the supplier assessment process." – Consultancy C<br>*Dark web analysis for third-party risk assessment*<br>"A company asked us to carry out a threat intelligence activity, providing us with the names of some of their suppliers. We then verified whether any of them had been compromised, for instance, by checking if their credentials were present on the dark web." – Consultancy E |
| Creativity for vulnerability assessments | *Text generation for phishing attack simulation*<br>"In attack simulations, we use ChatGPT to write a phishing email in a language that is not our own. We have a client in France, we need to do a phishing email, now we've seen that ChatGPT does some good stuff." – Consultancy D<br>*Voice generation for vishing attack simulation*<br>"We did some experiments on the topic of voice formulation, so being able to also use someone else's voice to create vishing, and this could be doing an initial call where you record a person's voice and then from there try to use it to create a different message." – Consultancy D |

## Appendix 4

**Table A4.** AI capabilities in cyber risk treatment: selected evidence

| Second-order themes | Selected quotes on first-order categories |
|---|---|
| Learning for risk mitigation | *Learn from past data to recommend actions to respond to a threat*<br>"For example, we also have an algorithm that recommends to the operator the procedures to follow for that specific type of incident. However, the response and closure of the incident are always carried out by a human." – System Integrator B<br>*Learn from past data to automatically respond to a threat*<br>"Automated generation of responses, with the goal also of automating part of the activities of a security operation center. If you can automate even part of the response probably manages to be more effective." – System Integrator C |
| Learning for risk prevention | *Learn from past data to suggest preventive mitigation actions*<br>"Assessing potentially risky situations—such as abnormal behaviors, unusual connections, and similar indicators—and suggesting possible corrections to configurations, adjustments to permission grants, or changes in access regulations, and so on." – Vendor A |
| Interaction for risk mitigation and prevention | *Interactive systems to support the operator in defining proactive mitigation actions*<br>"Anomaly detection, policy suggestions, permission adjustments, documentation refinement, and improved user interaction, so we gradually developed management consoles that can proactively assist the user." – Vendor A<br>*Interactive systems to support the operator in incident response*<br>"A chatbot that, based on a machine learning algorithm, suggests the most appropriate procedure for a given type of incident." – System Integrator B |
| Creativity for risk mitigation | *Generate new knowledge to support the operators in incident response*<br>"To date, precisely, we are experimenting with the Large Language Model with the very aim of creating new knowledge from acquired knowledge that can be of help to operators within the command and control rooms to act in unknown, *a priori* or emergency situations." – System Integrator C |
| Adaptation for risk mitigation | *Provide automatic remediation actions to new threats*<br>"AI tools can support us by providing suggestions or even performing automatic remediation. There are certain events that happen very frequently, generating alerts due to suspicious or potentially malicious activity. In such cases, many of these issues can be managed automatically, reducing the burden on analysts and ensuring timely responses." – Consultancy E<br>*Provide suggestions to respond to new threats*<br>"Definitely on the endpoint protection part, the intelligence acts faster because it does a faster identification of the malware and then allows you to stop the process, the process is not even started. So the mitigation is preventive because identification and blocking come at the same time." – System Integrator D |
| Reasoning for risk mitigation | *Automatically respond to threats with playbooks*<br>"So we have a really innovative automatic remediation, because it's not a one-to-one automatic remediation, but I see an event, I respond with a playbook, which is a set of actions that lead me to then figure out what to actually do." – Vendor B |
| Reasoning for risk prevention | *Perform correlation analysis to prevent threats*<br>"Or tools that correlate those alerts during incident response, such as SOAR platforms. Employing these technologies to enhance event correlation engines, with the aim of improving detection capabilities and accelerating incident response times." – Consultancy A<br>*Verify and prevent toxic combinations*<br>"Facilitate the whole privilege assignment phase through AI tools that then go and verify that there are no toxic combinations at the time you go and do this kind of assignment." – Consultancy B |

(*continued*)

**Table A4.** Continued

| Second-order themes | Selected quotes on first-order categories |
|---|---|
| Prediction for risk prevention | *Predict possible threats and provide suggestions to prevent them*<br>"If you have an integrated system across companies with cross-visibility into everything happening across all your environments, it would be capable of detecting statistically significant events that occur more or less frequently, and more or less consistently across different organizations. This would enable the system to make not necessarily creative, but predictive and preventive suggestions." – Vendor A<br>*Prediction to forecast different scenarios supporting the operator to prevent threats*<br>"Threat modeling is another critical step. This process involves building a model of possible threats and necessary countermeasures prior to software development. This human modeling can involve scenarios that are difficult to imagine or predict. AI can greatly accelerate and improve this process. It can facilitate the interfacing and correlation of models with real attacks that may pose an actual threat to software." – Vendor D |
| Perception for risk mitigation | *Text analysis to support incident response*<br>"These kinds of solutions that are going to use Chat GPT to help security analysts in their work. On that I see it being very effective precisely because it's about for a person having to go and study so much material and make the connections within that material. For an instrument, it's zero time, almost." – System Integrator A |

## Appendix 5

**Table A5.** AI capabilities in cyber risk monitoring: selected evidence

| Second-order themes | Selected quotes on first-order categories |
|---|---|
| Learning for risk monitoring | *Learn from data in monitoring system behaviors*<br>"The machine learning models that are inside the various antivirus applications, the various EDRs that monitor the behavior of what various executables do, working on large amounts of data and what are the anomalies compared to normal operation." – System Integrator A |
| Adaptation for risk monitoring | *Adapt to data changes in system monitoring*<br>"The same thing happens in endpoint protection, where process analysis on the machine can tell when an operation is actually done by a user or not done by a user, because maybe there is malware behind it that is simulating the user's presence. AI can figure out that that activity is not a human activity." – System Integrator D |
| Reasoning for risk monitoring | *Correlation analysis in web scanning*<br>"If we talk about AI on the monitoring part, we can see it applied in the threat intelligence platforms, which put the information together, the system there correlates and says watch out, an event is generated on the firewall, then afterwards I collect this information, put it together and realize it looks like a similar attack that happened right now on the other side of the world in another company." – System Integrator D |
| Perception for risk monitoring | *Text analysis in dark web monitoring*<br>"Another type of AI we use is related to semantics. When we automate certain types of analysis on the dark web, such as monitoring forums and similar platforms" – Vendor B |

## Notes

1. Endpoint Detection and Response systems are cybersecurity tools that continuously monitor endpoints like desktops, laptops and servers for suspicious activity.
2. The fraudulent practice of sending emails or other messages impersonating a legitimate entity to induce individuals into revealing sensitive personal information, like passwords, credit card numbers or bank account details.

3. Threat intelligence solutions are tools and platforms that help organizations collect, analyze and share information about potential and emerging cyber risks.
4. Vulnerability management is the process of identifying, assessing, and addressing security weaknesses in systems, networks and applications.
5. Penetration testing is a simulated attack designed to exploit those vulnerabilities and assess the effectiveness of security measures.
6. The dark web consists of websites and content that are not indexed by traditional search engines, making them invisible to the average Internet user and provides user anonymity.
7. A threat conducted over the phone that tricks victims into providing sensitive information, such as login details, credit card numbers or bank details.

## References


Akanfe, O., Lawong, D. and Rao, H.R. (2024), "Blockchain technology and privacy regulation: reviewing frictions and synthesizing opportunities", *International Journal of Information Management*, Vol. 76, 102753, doi: 10.1016/j.ijinfomgt.2024.102753.

Ambulkar, S., Blackhurst, J. and Grawe, S. (2015), "Firm's resilience to supply chain disruptions: scale development and empirical examination", *Journal of Operations Management*, Vol. 33 No. 1, pp. 111-122, doi: 10.1016/j.jom.2014.11.002.

Ångström, R.C., Björn, M., Dahlander, L., Mähring, M. and Wallin, M.W. (2023), "Getting ai implementation right: insights from a global survey", *California Management Review*, Vol. 66 No. 1, pp. 5-22, doi: 10.1177/00081256231190430.

Ansari, M.F., Dash, B., Sharma, P. and Yathiraju, N. (2022), "The impact and limitations of artificial intelligence in cybersecurity: a literature review", *IJARCCE*, Vol. 11 No. 9, doi: 10.17148/ijarcce.2022.11912.

Armstrong, B. and Berkowitz, B. (2024), "Scaling automation: two proven paths to success", *MIT Sloan Management Review*, Vol. 65 No. 2, pp. 1-8.

Bals, L. and Tate, W.L. (2018), "Sustainable supply chain design in social businesses: advancing the theory of supply chain", *Journal of Business Logistics*, Vol. 39 No. 1, pp. 57-79, doi: 10.1111/jbl.12172.

Baryannis, G., Dani, S. and Antoniou, G. (2019), "Predicting supply chain risks using machine learning: the trade-off between performance and interpretability", *Future Generation Computer Systems*, Vol. 101, pp. 993-1004, doi: 10.1016/j.future.2019.07.059.

Berry, H.S. (2023), "The importance of cybersecurity in supply chain", *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, pp. 1-5.

Blome, C. and Schoenherr, T. (2011), "Supply chain risk management in financial crises—a multiple case-study approach", *International Journal of Production Economics*, Vol. 134 No. 1, pp. 43-57, doi: 10.1016/j.ijpe.2011.01.002.

Boyson, S. (2014), "Cyber supply chain risk management: revolutionizing the strategic control of critical IT systems", *Technovation*, Vol. 34 No. 7, pp. 342-353, doi: 10.1016/j.technovation.2014.02.001.

Burger, M., Nitsche, A.-M. and Arlinghaus, J. (2023), "Hybrid intelligence in procurement: disillusionment with ai's superiority?", *Computers in Industry*, Vol. 150, 103946, doi: 10.1016/j.compind.2023.103946.

Caniato, F., Doran, D., Sousa, R. and Boer, H. (2018), "Designing and developing om research–from concept to publication", *International Journal of Operations and Production Management*, Vol. 38 No. 9, pp. 1836-1856, doi: 10.1108/ijopm-01-2017-0038.

Cannas, V.G., Ciano, M.P., Saltalamacchia, M. and Secchi, R. (2024), "Artificial intelligence in supply chain and operations management: a multiple case study research", *International Journal of Production Research*, Vol. 62 No. 9, pp. 3333-3360, doi: 10.1080/00207543.2023.2232050.

Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., Min, D. and Cao, R. (2019), "Survey of ai in cybersecurity for information technology management", *2019 IEEE Technology and Engineering Management Conference (TEMSCON)*, IEEE, pp. 1-8.

Choi, T.Y., Dooley, K.J. and Rungtusanatham, M. (2001), "Supply networks and complex adaptive systems: control versus emergence", *Journal of Operations Management*, Vol. 19 No. 3, pp. 351-366, doi: 10.1016/s0272-6963(00)00068-1.

Colicchia, C., Creazza, A. and Menachof, D.A. (2019), "Managing cyber and information risks in supply chains: insights from an exploratory analysis", *Supply Chain Management: An International Journal*, Vol. 24 No. 2, pp. 215-240, doi: 10.1108/scm-09-2017-0289.

Colombo, J., Boffelli, A., Kalchschmidt, M. and Legenvre, H. (2023), "Navigating the socio-technical impacts of purchasing digitalisation: a multiple-case study", *Journal of Purchasing and Supply Management*, Vol. 29 No. 3, 100849, doi: 10.1016/j.pursup.2023.100849.

Corbett, M. and Sajal, S. (2023), "AI in cybersecurity", in *2023 Intermountain Engineering, Technology and Computing (IETC)*, IEEE, Provo, UT, pp. 334-338.

Creazza, A., Colicchia, C., Spiezia, S. and Dallari, F. (2022), "Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era", *Supply Chain Management: An International Journal*, Vol. 27 No. 1, pp. 30-53, doi: 10.1108/scm-02-2020-0073.

Cui, Z., Xue, F., Cai, X., Cao, Y., Wang, G.-g. and Chen, J. (2018), "Detection of malicious code variants based on deep learning", *IEEE Transactions on Industrial Informatics*, Vol. 14 No. 7, pp. 3187-3196, doi: 10.1109/tii.2018.2822680.

Cybersecurity, C.I. (2018), "Framework for improving critical infrastructure cybersecurity", available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP,4162018(7)

Dong, Z., Kane, K. and Camp, L.J. (2016), "Detection of rogue certificates from trusted certificate authorities using deep neural networks", *ACM Transactions on Privacy and Security (TOPS)*, Vol. 19 No. 2, pp. 1-31, doi: 10.1145/2975591.

Dubey, R., Bryde, D.J., Dwivedi, Y.K., Graham, G., Foropon, C. and Papadopoulos, T. (2023), "Dynamic digital capabilities and supply chain resilience: the role of government effectiveness", *International Journal of Production Economics*, Vol. 258, 108790, doi: 10.1016/j.ijpe.2023.108790.

Durach, C.F. and Gutierrez, L. (2024), "'Hello, this is your AI co-pilot'–operational implications of artificial intelligence chatbots", *International Journal of Physical Distribution and Logistics Management*, Vol. 54 No. 3, pp. 229-246, doi: 10.1108/ijpdlm-01-2024-0031.

Eisenhardt, K.M. (1989), "Building theories from case study research", *Academy of Management Review*, Vol. 14 No. 4, pp. 532-550, doi: 10.2307/258557.

Ellström, D., Holtström, J., Berg, E. and Josefsson, C. (2022), "Dynamic capabilities for digital transformation", *Journal of Strategy and Management*, Vol. 15 No. 2, pp. 272-286, doi: 10.1108/jsma-04-2021-0089.

Eriksson, D. and Engström, A. (2021), "Using critical realism and abduction to navigate theory and data in operations and supply chain management research", *Supply Chain Management: An International Journal*, Vol. 26 No. 2, pp. 224-239, doi: 10.1108/scm-03-2020-0091.

Eulerich, M., Waddoups, N., Wagener, M. and Wood, D.A. (2024), "The dark side of robotic process automation (rpa): understanding risks and challenges with rpa", *Accounting Horizons*, Vol. 38 No. 2, pp. 143-152, doi: 10.2308/horizons-2022-019.

European Commission. Joint Research Centre (2020), *AI Watch: Defining Artificial Intelligence: Towards an Operational Definition and Taxonomy of Artificial Intelligence*, Publications Office, Luxembourg.

Fan, Y. and Stevenson, M. (2018), "A review of supply chain risk management: definition, theory, and research agenda", *International Journal of Physical Distribution and Logistics Management*, Vol. 48 No. 3, pp. 205-230, doi: 10.1108/ijpdlm-01-2017-0043.

Friday, D., Melnyk, S.A., Altman, M., Harrison, N. and Ryan, S. (2024), "An inductive analysis of collaborative cybersecurity management capabilities, relational antecedents and supply chain cybersecurity parameters", *International Journal of Physical Distribution and Logistics Management*, Vol. 54 No. 5, pp. 476-500, doi: 10.1108/ijpdlm-01-2023-0034.

Ganesh, A.D. and Kalpana, P. (2022), "Future of artificial intelligence and its influence on supply chain risk management–A systematic review", *Computers and Industrial Engineering*, Vol. 169, 108206, doi: 10.1016/j.cie.2022.108206.

Gaudenzi, B. and Siciliano, G. (2017), "Managing it and cyber risks in supply chains", in *Supply Chain Risk Management: Advanced Tools, Models, and Developments*, Springer, pp. 85-96.

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: An International Journal*, Vol. 25 No. 2, pp. 223-240.

Giudici, A., Reinmoeller, P. and Ravasi, D. (2018), "Open-system orchestration as a relational source of sensing capabilities: evidence from a venture association", *Academy of Management Journal*, Vol. 61 No. 4, pp. 1369-1402, doi: 10.5465/amj.2015.0573.

Guerra, P.J. and Estay, S.D.S. (2018), *An Impact-Wave Analogy for Managing Cyber Risks in Supply Chains, 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, IEEE, pp. 61-65.

Gupta, S., Modgil, S., Meissonier, R. and Dwivedi, Y.K. (2021), "Artificial intelligence and information system resilience to cope with supply chain disruption", *IEEE Transactions on Engineering Management*, Vol. 11, pp. 80218-80245, doi: 10.1109/ACCESS.2023.3294279.

Gupta, M., Akiri, C., Aryal, K., Parker, E. and Praharaj, L. (2023), "From ChatGPT to ThreatGPT: impact of generative AI in cybersecurity and privacy", *IEEE Access*, Vol. 11, pp. 80218-80245, doi: 10.1109/access.2023.3300381.

Hangl, J., Krause, S. and Behrens, V.J. (2023), "Drivers, barriers and social considerations for AI adoption in SCM", *Technology in Society*, Vol. 74, 102299, doi: 10.1016/j.techsoc.2023.102299.

Helo, P. and Hao, Y. (2022), "Artificial intelligence in operations management and supply chain management: an exploratory case study", *Production Planning and Control*, Vol. 33 No. 16, pp. 1573-1590, doi: 10.1080/09537287.2021.1882690.

Hendriksen, C. (2023), "Artificial intelligence for supply chain management: disruptive innovation or innovative disruption?", *Journal of Supply Chain Management*, Vol. 59 No. 3, pp. 65-76, doi: 10.1111/jscm.12304.

Herburger, M. and Omar, A. (2021), "Connecting supply chain", *Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions*, Vol. 1, p. 13.

Herburger, M., Wieland, A. and Hochstrasser, C. (2024), "Building supply chain resilience to cyber risks: a dynamic capabilities perspective", *Supply Chain Management: An International Journal*, Vol. 29 No. 7, pp. 28-50, doi: 10.1108/scm-01-2023-0016.

Hilliard, R. and Goldstein, D. (2019), "Identifying and measuring dynamic capability using search routines", *Strategic Organization*, Vol. 17 No. 2, pp. 210-240, doi: 10.1177/1476127018755001.

Hoffmann, P., Schiele, H. and Krabbendam, K. (2013), "Uncertainty, supply risk management and their impact on performance", *Journal of Purchasing and Supply Management*, Vol. 19 No. 3, pp. 199-211, doi: 10.1016/j.pursup.2013.06.002.

Hughes, M.M., Zhou, Z., Zinn, W. and Knemeyer, A.M. (2023), "Plastic response to disruptions: significant redesign of supply chains", *Journal of Business Logistics*, Vol. 44 No. 1, pp. 80-108, doi: 10.1111/jbl.12321.

Ivanov, D. (2020), "Predicting the impacts of epidemic outbreaks on global supply chains: a simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case", *Transportation Research Part E: Logistics and Transportation Review*, Vol. 136, 101922, doi: 10.1016/j.tre.2020.101922.

Jackson, I., Ivanov, D., Dolgui, A. and Namdar, J. (2024), "Generative artificial intelligence in supply chain and operations management: a capability-based framework for analysis and implementation", *International Journal of Production Research*, Vol. 62 No. 17, pp. 6120-6145, doi: 10.1080/00207543.2024.2309309.

Jarrahi, M.H., Lutz, C. and Newlands, G. (2022), "Artificial intelligence, human intelligence and hybrid intelligence based on mutual augmentation", *Big Data and Society*, Vol. 9 No. 2, 20539517221142824, doi: 10.1177/20539517221142824.

Jazairy, A., Brho, M., Manuj, I. and Goldsby, T.J. (2024), "Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness", *International Journal of Physical Distribution and Logistics Management*, Vol. 54 No. 11, pp. 1-29, doi: 10.1108/ijpdlm-12-2023-0445.

Juan, S.-J. and Li, E.Y. (2023), "Financial performance of firms with supply chains during the covid-19 pandemic: the roles of dynamic capability and supply chain resilience", *International Journal of Operations and Production Management*, Vol. 43 No. 5, pp. 712-737, doi: 10.1108/ijopm-04-2022-0249.

Kaur, R., Gabrijelčič, D. and Klobučar, T. (2023), "Artificial intelligence for cybersecurity: literature review and future research directions", *Information Fusion*, Vol. 97, 101804, doi: 10.1016/j.inffus.2023.101804.

Kembro, J.H. and Norrman, A. (2025), "A strategic perspective on automated warehouse systems in retail: insights from a multiple case study", *International Journal of Physical Distribution and Logistics Management*, Vol. 55 No. 11, pp. 57-91, doi: 10.1108/ijpdlm-05-2024-0218.

Ketokivi, M. and Choi, T. (2014), "Renaissance of case research as a scientific method", *Journal of Operations Management*, Vol. 32 No. 5, pp. 232-240, doi: 10.1016/j.jom.2014.03.004.

Kosmowski, K.T., Piesik, E., Piesik, J. and Śliwiński, M. (2022), "Integrated functional safety and cybersecurity evaluation in a framework for business continuity management", *Energies*, Vol. 15 No. 10, p. 3610, doi: 10.3390/en15103610.

Kosutic, D. and Pigni, F. (2022), "Cybersecurity: investing for competitive outcomes", *Journal of Business Strategy*, Vol. 43 No. 1, pp. 28-36, doi: 10.1108/jbs-06-2020-0116.

Kovács, G. and Spens, K.M. (2005), "Abductive reasoning in logistics research", *International Journal of Physical Distribution and Logistics Management*, Vol. 35 No. 2, pp. 132-144, doi: 10.1108/09600030510590318.

Kshetri, N. (2017), "Blockchain's roles in strengthening cybersecurity and protecting privacy", *Telecommunications Policy*, Vol. 41 No. 10, pp. 1027-1038, doi: 10.1016/j.telpol.2017.09.003.

Lacity, M.C. and Willcocks, L.P. (2021), "Becoming strategic with intelligent automation", *MIS Quarterly Executive*, Vol. 20 No. 2, p. 7.

Li, J.-h. (2018), "Cyber security meets artificial intelligence: a survey", *Frontiers of Information Technology and Electronic Engineering*, Vol. 19 No. 12, pp. 1462-1474, doi: 10.1631/fitee.1800573.

Liang, G., Weller, S.R., Luo, F., Zhao, J. and Dong, Z.Y. (2018), "Distributed blockchain-based data protection framework for modern power systems against cyber attacks", *IEEE Transactions on Smart Grid*, Vol. 10 No. 3, pp. 3162-3173, doi: 10.1109/tsg.2018.2819663.

Lyytinen, K. and Newman, M. (2008), "Explaining information systems change: a punctuated socio-technical change model", *European Journal of Information Systems*, Vol. 17 No. 6, pp. 589-613, doi: 10.1057/ejis.2008.50.

Manuj, I. and Mentzer, J.T. (2008), "Global supply chain risk management", *Journal of Business Logistics*, Vol. 29 No. 1, pp. 133-155, doi: 10.1002/j.2158-1592.2008.tb00072.x.

Martínez Torres, J., Iglesias Comesaña, C. and García-Nieto, P.J. (2019), "Machine learning techniques applied to cybersecurity", *International Journal of Machine Learning and Cybernetics*, Vol. 10 No. 10, pp. 2823-2836, doi: 10.1007/s13042-018-00906-1.

Maxwell, J.A. (2013), *Qualitative Research Design: An Interactive Approach: An Interactive Approach*, Sage, Thousand Oaks.

Melnyk, S.A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J.F. and Friday, D. (2022), "New challenges in supply chain management: cybersecurity across the supply chain", *International Journal of Production Research*, Vol. 60 No. 1, pp. 162-183, doi: 10.1080/00207543.2021.1984606.

Min, H. (2010), "Artificial intelligence in supply chain management: theory and applications", *International Journal of Logistics: Research and Applications*, Vol. 13 No. 1, pp. 13-39, doi: 10.1080/13675560902736537.

Naik, B., Mehta, A., Yagnik, H. and Shah, M. (2022), "The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review", *Complex and Intelligent Systems*, Vol. 8 No. 2, pp. 1763-1780, doi: 10.1007/s40747-021-00494-8.

Naseer, H., Desouza, K., Maynard, S.B. and Ahmad, A. (2024), "Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics", *European Journal of Information Systems*, Vol. 33 No. 2, pp. 200-220, doi: 10.1080/0960085x.2023.2257168.

Nila, C., Apostol, I. and Patriciu, V. (2020), "Machine learning approach to quick incident response", *2020 13th International Conference on Communications (COMM)*, Bucharest, IEEE, pp. 291-296.

Oltramari, A. and Kott, A. (2018), "Towards a reconceptualisation of cyber risk: an empirical and ontological study", *Journal of Information Warfare*, Vol. 17 No. 1, pp. 49-73.

Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A. (2020), "Cyber security risks in globalized supply chains: conceptual framework", *Journal of Global Operations and Strategic Sourcing*, Vol. 13 No. 1, pp. 103-128, doi: 10.1108/jgoss-05-2019-0042.

Paschen, U., Pitt, C. and Kietzmann, J. (2020), "Artificial intelligence: building blocks and an innovation typology", *Business Horizons*, Vol. 63 No. 2, pp. 147-155, doi: 10.1016/j.bushor.2019.10.004.

Paul, S.K., Riaz, S. and Das, S. (2020), "Organizational adoption of artificial intelligence in supply chain risk management", *Re-imagining Diffusion and Adoption of Information Technology and Systems: A Continuing Conversation: IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2020*, Tiruchirappalli, December 18-19, 2020, Proceedings, Part I, Springer, pp. 10-15.

Radanliev, P., De Roure, D., Page, K., Nurse, J.R.C., Mantilla Montalvo, R., Santos, O., Maddox, L. and Burnap, P. (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 No. 1, p. 13, doi: 10.1186/s42400-020-00052-8.

Richey, R.G., Jr., Chowdhury, S., Davis-Sramek, B., Giannakis, M. and Dwivedi, Y.K. (2023), "Artificial intelligence in logistics and supply chain management: a primer and roadmap for research", *Journal of Business Logistics*, Vol. 44 No. 4, pp. 532-549, doi: 10.1111/jbl.12364.

Ritchie, B. and Brindley, C. (2007), "Supply chain risk management and performance: a guiding framework for future development", *International Journal of Operations and Production Management*, Vol. 27 No. 3, pp. 303-322.

Robinson, O.C. (2014), "Sampling in interview-based qualitative research: a theoretical and practical guide", *Qualitative Research in Psychology*, Vol. 11 No. 1, pp. 25-41, doi: 10.1080/14780887.2013.801543.

Sai, S., Yashvardhan, U., Chamola, V. and Sikdar, B. (2024), "Generative ai for cyber security: analyzing the potential of chatgpt, dall-e and other models for enhancing the security space", *IEEE Access*, Vol. 12, pp. 53497-53516, doi: 10.1109/ACCESS.2024.3385107.

Samoili, S., Lopez Cobo, M., Gómez, E., De Prato, G., Martínezplumed, F. and Ai, W. (2020), "Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence", Brussels.

Siciliano, G.G. and Gaudenzi, B. (2018), "The role of supply chain resilience on it and cyber disruptions", in *Network, Smart and Open: Three Keywords for Information Systems Innovation*, Springer, pp. 57-69.

Susarla, A., Gopal, R., Thatcher, J.B. and Sarker, S. (2023), "The janus effect of generative ai: charting the path for responsible conduct of scholarly activities in information systems", *Information Systems Research*, Vol. 34 No. 2, pp. 399-408, doi: 10.1287/isre.2023.ed.v34.n2.

Taddeo, M., McCutcheon, T. and Floridi, L. (2019), "Trusting artificial intelligence in cybersecurity is a double-edged sword", *Nature Machine Intelligence*, Vol. 1 No. 12, pp. 557-560, doi: 10.1038/s42256-019-0109-1.

Teece, D.J. (2007), "Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance", *Strategic Management Journal*, Vol. 28 No. 13, pp. 1319-1350, doi: 10.1002/smj.640.

Teece, D.J., Pisano, G. and Shuen, A. (1997), "Dynamic capabilities and strategic management", *Strategic Management Journal*, Vol. 18 No. 7, pp. 509-533, doi: 10.1002/(sici)1097-0266(199708)18:7<509::aid-smj882>3.0.co;2-z.

Teuteberg, F. (2008), "Supply chain risk management: a neural network approach", in *Strategies and Tactics in Supply Chain Event Management*, Springer, pp. 99-118.

Urciuoli, L., Männistö, T., Hintsa, J. and Khan, T. (2013), "Supply chain cyber security–potential threats", *Information and Security: An International Journal*, Vol. 29 No. 1, pp. 51-68, doi: 10.11610/isij.2904.

Van Der Aalst, W.M. (2021), "Hybrid intelligence: to automate or not to automate, that is the question", *International Journal of Information Systems and Project Management*, Vol. 9 No. 2, pp. 5-20, doi: 10.12821/ijispm090201.

Vieira, A.A., Dias, L.M., Santos, M.Y., Pereira, G.A. and Oliveira, J.A. (2019), "Simulation of an automotive supply chain using big data", *Computers and Industrial Engineering*, Vol. 137, 106033, doi: 10.1016/j.cie.2019.106033.

Voss, C. (2010), "Case research in operations management", in *Researching Operations Management*, Routledge, pp. 176-209.

Walshe, R., Koene, A., Baumann, S., Panella, M., Maglaras, L. and Medeiros, F. (2021), "Artificial intelligence as enabler for sustainable development", *2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Cardiff, IEEE, pp. 1-7.

Wessel, M., Adam, M., Benlian, A., Majchrzak, A. and Thies, F. (2025), "Generative ai and its transformative value for digital platforms", *Journal of Management Information Systems*, Vol. 42 No. 2, pp. 346-369, doi: 10.1080/07421222.2025.2487315.

Wiafe, I., Koranteng, F.N., Obeng, E.N., Assyne, N., Wiafe, A. and Gulliver, S.R. (2020), "Artificial intelligence for cybersecurity: a systematic mapping of literature", *IEEE Access*, Vol. 8, pp. 146598-146612, doi: 10.1109/access.2020.3013145.

Wiedenmann, M. and Größler, A. (2020), "Supply risk identification in manufacturing supply networks", *The International Journal of Logistics Management*, Emerald Publishing Limited, Vol. 32, pp. 650-672.

Wieland, A. (2021), "Dancing the supply chain: toward transformative supply chain management", *Journal of Supply Chain Management*, Vol. 57 No. 1, pp. 58-73, doi: 10.1111/jscm.12248.

Wiengarten, F., Humphreys, P., Gimenez, C. and McIvor, R. (2016), "Risk, risk management practices, and the success of supply chain integration", *International Journal of Production Economics*, Vol. 171, pp. 361-370, doi: 10.1016/j.ijpe.2015.03.020.

World Economic Forum (2025), "Global Cybersecurity Outlook 2025", World Economic Forum, available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ (accessed 13 January 2025).

Wu, J.-x., Li, J.-h. and Ji, X.-s. (2018), "Security for cyberspace: challenges and opportunities", *Frontiers of Information Technology and Electronic Engineering*, Vol. 19 No. 12, pp. 1459-1461, doi: 10.1631/fitee.1840000.

Yang, M., Lim, M.K., Qu, Y., Ni, D. and Xiao, Z. (2023), "Supply chain risk management with machine learning technology: a literature review and future research directions", *Computers and Industrial Engineering*, Vol. 175, 108859, doi: 10.1016/j.cie.2022.108859.

Yin, R.K. (2009), *Case Study Research: Design and Methods*, Sage, Thousand Oaks, Vol. 5.

Yu, J., Zhang, B., Kuang, Z., Lin, D. and Fan, J. (2016), "iPrivacy: image privacy protection by identifying sensitive objects via deep multi-task learning", *IEEE Transactions on Information Forensics and Security*, Vol. 12 No. 5, pp. 1005-1016, doi: 10.1109/tifs.2016.2636090.

Zaydi, M., Maleh, Y. and Khourdifi, Y. (2025), "A new framework for agile cybersecurity risk management: integrating continuous adaptation and real-time threat intelligence (acsrm-icti)", in *Agile Security in the Digital Era*, CRC Press, pp. 19-47.

Zeadally, S., Adi, E., Baig, Z. and Khan, I.A. (2020), "Harnessing artificial intelligence capabilities to improve cybersecurity", *IEEE Access*, Vol. 8, pp. 23817-23837, doi: 10.1109/access.2020.2968045.

**Corresponding author**
Claudia Ciceri can be contacted at: claudia.ciceri@polimi.it