INSTITUTE FOR HOMELAND SECURITY

LEVERAGING ARTIFICIAL INTELLIGENCE FOR SUPPLY CHAIN RISK MANAGEMENT

Institute for Homeland Security

Sam Houston State University

Alexander B. Kinney Ph.D

Leveraging Artificial Intelligence for Supply Chain Risk Management

By. Alexander B. Kinney Ph.D.

ABSTRACT

The rise of artificial intelligence (AI) solutions in the corporate landscape has prompted a wider discussion among public stakeholders and policymakers about the best practices for leveraging this evolving technology to coordinate the global supply chain. In area of supply chain risk management (SCRM), scholars and practitioners have only recently turned their attention to how AI can bolster, or even supplement humans in decision-making processes. While AI holds a great deal of promise in reducing the potential for severe supply chain disruptions, ethical considerations and the novelty of AI-based solutions can introduce multiple challenges for critical infrastructure organizations that may be eager to incorporate this technology. The aim of this technical paper is to describe recent advancements and emerging trends in the use of AI to quantify risk crisis management readiness and make strategic choices using identified risks in decision-making. In what follows, I will provide a review of key research findings, methodologies, and innovations made in the areas of AI and SCRM. Additionally, this paper unpacks core ethical issues including algorithmic bias, responsible data handling, and outsourcing decision-making. These are interrelated issues that critical infrastructure corporations must navigate to maintain a commitment to safety and security while increasing organizational resilience. To conclude, this paper outlines several suggested best practices for businesses that are eager to incorporate artificial intelligence into supply chain risk management protocols and discusses expected trends in the use of AI in SCRM.

INTRODUCTION

The Digital Era of Supply Chain Management

Though the emergence of operations management practices coincided with the birth of the corporate business model, the field of supply chain management truly rose to prominence in the 1980s when logistical departments were faced with the daunting task of accounting for a wider range of firm interdependencies that were brought forth by globalization (Alfalla-Luque & Medina-Lopez, 2009). The rapid scaling of corporate relationships during this moment in history introduced a new imperative for businesses to integrate their internal organizational functions with that of purchasing, manufacturing, sales, and distribution (Oliver & Webber, 1982). Now having to account for both upstream and downstream manufacturing challenges, this meant that from a strategy standpoint, organizations were no longer just competing on a firm-to-firm basis. Instead, organizations now had to engage in supply chain-to-supply chain competition if they wanted to remain viable.

Shifting our focus to the present day, the now ubiquitous integration software systems that are designed to facilitate enterprise resource management has pushed supply chain managers into the "digital era" (Agrawal & Narain, 2018 p. 455). The practice of integrating new information and communication technologies (ICTs) in standard business processes is not only seen as a pathway to gain a competitive edge, but a functional necessity to mitigate risks and ensure the survival of the firm (Varma and Khan, 2014). However, the turn toward supply chain-to-supply chain competition means that organizations increasingly find themselves partnering with small and medium size firms across the globe. Experts in the field of supply chain risk management (SCRM) have expressed caution that adopting cutting-edge ICT options without a thoughtful approach can exacerbate existing threats and/or introduce novel disruptions within their supply chain networks (Finch, 2004). This presents a uniquely challenging issue for businesses, especially those embedded in what are considered "critical infrastructure sectors" of energy, communications, water, and transportation (Cavelty, 2007).

Though most companies are now well versed in several industry standard, out-of-the-box ICT solutions, the staggering rate of innovation in this space can be daunting for organizational decision makers. Where previously it may have been common for companies to rely on recognizable, industry standard sets of products from a fairly limited group of providers, there are now a host of options coming to market seemingly every day. These include new technologies capable of facilitating real-time visibility in product support, data analytics, cloudbased data storage, and blockchain-based transactions. Scholars have argued that while these products have enabled some companies to optimize their processes, others continue to suffer from a lack of familiarity with how to identify, evaluate, and ultimately select software solutions within this evolving technological landscape (Slone, Mentzer, & Dittmann, 2007). For critical infrastructure organizations, a lack of familiarity with these products may challenge their ability to optimize processes. This can inflate costs, reduce efficiency, or worse, lead to a shortage of essential products or services that can threaten national security.

Compounding this challenge, many of the products hitting the market have now incorporate artificial intelligence (AI) as a core service offering. Cutting edge developments in AI over the last decade represents new terrain for many supply chain managers, even those that have a great deal of experience in the field. When leveraged carefully, tools that are built through AI can present compelling opportunities to offload human decision-making to software that is able to rapidly identify, mitigate, and manage perpetual risks posed by unpredictable events (Deiva Ganesh & Kalpana, 2022). As such, AI presents a new frontier for enhancing the resilience of the global supply chain to ensure that critical infrastructure sectors can continue to meet stakeholder needs (Sakhnini et al., 2020).

Problem Statement

The volume of information that supply chain managers now need to account for has only continued to grow since the COVID-19 pandemic forced most business operations into a fully online or hybrid/remote work environment (Ivanov, 2021). Coupled with increasing disruptions from natural disasters, demand fluctuation, and government policy shifts, the threats to supply

chain resilience have never been greater (Rangel, de Oliveira, & Leite, 2015; Remko, 2020). In response to these persistent challenges, scholars have advocated for practitioners to adopt AIbased solutions to modernize their supply chains (Deiva Ganesh & Kalpana, 2022). Yet, many of these state-of-the-art tools are unconventional in the world of IT, and as a result, they may be unfamiliar to both supply chain managers and policymakers tasked with regulating their use. For those operating in organizations associated with critical infrastructure sectors, integrating AI into the existing business processes may seem like a heavy lift. There are also several ethical challenges that supply chain managers need to confront when considering AI-based solutions.

Research Objective

First, this paper begins by detailing a working definition of SCRM and then describes the overarching objectives of this growing field. It then provides an overview of existing AI technologies including machine learning, Petri-Nets, multi-agent systems, and rule-based reasoning methods that firms can leverage to quantify risk and strategically respond to identified threats. Next, this paper turns toward outlining specific ethical challenges that are associated with current trends and prospective developments in the use of these tools. These ethical challenges include the potential for AI to act in an unexpectedly biased fashion and to become a cybersecurity threat. Additionally, there are several noted unintended consequences of AI adoption at the individual, organizational, and societal levels that decision makers need to be familiar with. Finally, this paper turns toward suggesting several recommended practices integrating AI into organizational processes in a way that balances the need to improve resilience against the need to maintain a commitment to safe and ethical business practices.

SUPPLY CHAIN RISK MANAGEMENT USING ARTIFICIAL INTELLIGENCE: A NEW FRONTIER

The Objectives of Supply Chain Risk Management

Unplanned supply chain disruptions are one of the paramount threats to the financial performance of companies. Worse yet, in critical infrastructure sectors they can become an issue of national security. For instance, at the turn of the millennium, a lightning bolt caused a roughly 10-minute blaze at a semiconductor plant in Albuquerque, NM that was owned by Phillips Electronics NV. Based in the Netherlands, this seemingly small event nearly ground all cellular phone manufacturing to a screeching halt across Europe for an undetermined period of time (Latour, 2001). More recently, the outbreak of the COVID-19 virus upended civilization worldwide. Rapidly imposed export controls that governments implemented to boost domestic industrial output unexpectedly led to an international shortage of personal protective equipment (PPE) products as multi-national producers sought to navigate unexpected supply chain breakdowns (Gereffi, 2020). In the United States, this led to a critical shortage of N95 respirator masks that put healthcare workers in danger, strained hospital infrastructure, and ultimately, lead to a lower quality of civilian care.

Such catastrophes have motivated a growing scholarly and practitioner community devoted to the area of supply chain risk management (SCRM). Defined, SCRM is "an interorganizational collaborative endeavor utilizing quantitative and qualitative risk management methodologies to identify, evaluate, mitigate, and monitor unexpected macro and micro level events or conditions, which might adversely impact any part of a supply chain" (Ho et al., 2015 p. 5036). For the uninitiated, a supply chain can be understood as type of process through which materials, products, and information flow in an uninterrupted state (Deiva Ganesh & Kalpana, 2022). To keep this flow uninterrupted, supply chain managers must account for several categories of risks. These categories include environmental, information, supply, demand, process, and control risks that each present specific challenges to coordinating inter-firm resource flows. Table 1 provides an overview of these risks.

Table 1. Types of Risks to the Supply Chain and Corresponding Examples[1]

Type of Risk	*Examples*
Environmental	Natural Disasters, Terrorism, War
Information	Cyberthreats, Intellectual property breach.
Supply	Off-shore sourcing issues, Quality control breakdowns.
Demand	Order volatility, Innovative competitors
Process	Equipment failure, Manufacturing bottlenecks
Control	Lack of collaborative planning, "bullwhip effect"

As illustrated above, though disaster response remains a critical objective to improving supply chain resilience, the field of SCRM is also oriented toward proactive strategies (Nooraie & Parast, 2015). Increasingly, scholars and practitioners are focused on developing real-time logistical tools for predicting potential disruptions to the supply chain in order to help supply chain managers create rapid response protocols and better prepare for a growing number of supply chain threats. This focus has only grown since the COVID-19 pandemic. There are new pressures both from firm stakeholders and from government entities to accurately gauge product availability on a global scale and to strategize around uncertain timelines for product delivery to prevent another massive breakdown in resource flows that can lead to civilian harm (Gereffi, 2020; Deiva Ganesh & Kalpana, 2022). Consequently, the field of SCRM has increasingly advocated for a greater emphasis on establishing new industry standards s that rely on quantified

[1] Table reproduces a figure that appears in (Deiva Ganesh & Kalpana, 2022).

risk assessments. For this, SCRM scholars have recently turned to novel artificial intelligence (AI) solutions because they present an attractive option to resolve longstanding issues of largescale information processing, while at the same time, improving efficiency and reducing costs (Baryannis et al., 2019).

Artificial Intelligence for Improving Supply Chain Resilience

What is "Artificial Intelligence"?

Put simply, artificial intelligence (AI) is a data-driven approach to mimicking human reasoning that leverages the computational capabilities of machines and/or software (Haugeland, 1989). AI is not a new concept. It dates back to the mid-1950s when Alan Turing conducted some of the first experiments that gave birth to modern computing (Copeland, 2004). However, it has received greater public attention in recent years due to rapid advancements in computational power and breakthroughs in mathematical problem-solving that have yielded funding for universities and private companies to develop out-of-the-box AI solutions. AI technologies are now widely used across a variety of business sectors. Popular applications of AI include the development of algorithms used in recommendation systems (e.g., YouTube/Netflix), internet search engines (e.g., Google Scholar), human speech detection (e.g., Apple Siri/Amazon Alexa), and creative tools (e.g., OpenAI ChatGPT).

Common Applications for AI in Supply chain Risk Management

SCRM researchers have identified several potential AI-tools that are now available to supply chain managers that may, under careful circumstances, improve decision-making (Min, 2010). These include various approaches that fall under the broader technical umbrella of machine learning, Petri-Nets, multi-agent systems, and automated rule-based reasoning techniques. Table 2 provides an overview of these approaches and identifies their application to SCRM. As this table illustrates, AI-based solutions have several use cases that supply chain managers can implement in a multi-phased approach to risk management.

Table 2. AI approaches and Applications to Supply chain Risk Management[2]

AI Method	*SCRM Task*	*Exemplary Use Cases*
Machine Learning	Risk Identification	Information aggregation, extraction, management.

[2] Table presents a simplified version of a figure that appears in (Deiva Ganesh & Kalpana, 2022)

Petri-Nets	Risk Assessment	Event simulation, process improvement.
Multi-Agent Systems	Risk Monitoring	Real-time decision support.
Rule-Based Reasoning	Risk Mitigation	Prioritizing identified risks, planning.

Machine learning is arguably the most flexible AI-solution available and has a demonstrated utility for improving organizational agility in risk identification (Ojha et al., 2017). The goal of machine learning is to leverage the problem-solving capacities of computers to gain insights into large volumes of information by providing programs with enough data that they can make probabilistic distinctions between specific outcomes (Min, 2010). In other words, supply chain managers can implement programs that are specifically designed to read language prompts. These language prompts are used to train these programs to recognize concepts, automate decisions, and create inferences based on the information that humans provide them. Sometimes referred to as "data mining," (Chen, Han, and Yu, 1996), machine learning techniques can process (and derive insights) large datasets in a timely manner that would otherwise be unachievable through human effort alone. As such, they represent an attractive option for companies that want to develop deeper insights into where risks exist in their supply chain processes.

Petri-Nets are closely related to machine learning techniques but differ in their objectives. While traditional machine learning techniques are commonly focused on reducing the complexity of information, Petri-Nets are a tool for simulating realities through a computational process known as "deep learning" (Guang et al., 2021). For supply chain managers, Petri-Nets can be deployed through programs that are designed to represent or continuously model supply chain interdependencies by feeding them real-time data (Mazzuto, Bevilacqua, & Ciarapica, 2011). This can be useful in the event that a company wishes to conduct a stress-test of their supply chain to identify potential improvements (Deiva Ganesh & Kalpana, 2022). Petri-Nets also can allow supply chain managers to engage in case studies that are based around simulated disruptive events to identify how existing processes could (or rather could not) respond.

Multi-agent systems are comprised of mixture of software entities that are configured to operate autonomously as a comprehensive system. Multi-agent systems have the potential to automatically make routine decisions and coordinate with specified entities that humans have control over (Giannakis & Louis, 2016). Stated differently, multi-agent systems allow for humans to outsource recurrent tasks to computers or robots to reduce the complexity of the supply chain. By allowing software programs to take on specific roles that would otherwise be in controlled by human decision makers, supply chain managers are less encumbered and can shift their focus to physical tasks or creative work that computers are not yet able to adequately perform. Specifically, multi-agent systems hold deep promise for company and sector specific risk monitoring protocols (Deiva Ganesh & Kalpana, 2022). Agent-based software solutions are able to help supply chain managers coordinate alternative travel routes, determine the best use of resources, and send out alerts in the event of a large-scale disruption like a terrorist threat or

attack (Schurr et al., 2005). As a result, multi-agent systems hold a great deal of promise for risk monitoring protocols.

Rule-based reasoning techniques aim to exploit the knowledge of past and existing events to project (and importantly quantify) potential future events. These techniques can be employed through computer programs that leverage inference models as a vehicle to parse through data. Rule-based reasoning techniques apply logic models to generate conclusions about a given situation from these datasets (Behret et al., 2012). In other words, platforms that employ rulebased reasoning techniques can allow supply chain managers to develop more comprehensive understandings of their supply chains by cataloguing known threats and providing insights into where potential unknown threats exist. For instance, data about existing disruptive events like natural disasters or geopolitical conflicts can be used to create standardized evaluations of risk that are based on parameters such as the frequency, detectability, and severity (Gallab et al., 2019). Additionally, rule-based reasoning platforms can help supply chain managers categorize potential risks into high, medium, or low ratings (Behret et al., 2012). In turn, these categories can help human decision makers rate different suppliers and customers, prioritize specific interventions to potential risks, and visualize areas of concern within the supply chain through the use of dashboard applications (Chakrabarti et al., 2022).

ETHICAL CHALLENGES ASSOCIATED WITH ADOPTING AI TECHNOLOGIES

Ethical Issues with the Code Behind AI Tech

There are several known ethical issues that are often hardcoded into AI technologies that need to be confronted. While AI holds a great deal of promise for delimiting humans to focus on essential tasks by outsourcing decisions to machines, the form and function of AI can exacerbate, rather than mitigate organizational threats if deployed in an uncritical manner. These include the potential for the algorithms behind AI to exhibit biases and issues with data privacy and cybersecurity.

The ability for algorithmic systems to yield socially biased outcomes is a known problem with automated decision-making platforms and has become a dominant research topic for information systems researchers (Someh et al., 2019). More commonly referred to as “algorithmic bias” (Kodzadeh & Ghasemaghaei, 2022), this refers to the potential for AI to inaccurately categorize or classify information by privileging or disadvantaging outcomes without a justifiable reason. This can occur in two ways. First, social biases that exist in a non-algorithmic context such as stereotypes, prejudices, and discrimination can become translated into the mathematical features, weights, and functions in AI models. Second, AI models themselves can be unstable when the sources of data that are used to formulate predictions lacks integrity (e.g., missing data points, underrepresenting cases from key populations of interest etc.). As a result, algorithmic bias can both produce and reproduce harms.

There are also cybersecurity risks and information privacy issues embedded in AI solutions as well. Though advances in the sophistication of predictive models and computational processing have greatly increased the capability of AI to process large scale datasets, this can turn AIenabled products into threat vectors that may be vulnerable to cyberattacks by malicious actors. This can

lead to data breaches that expose sensitive data about companies and their partners to criminal actors and unexpectedly cripple supply chain processes (Jin, 2018). Beyond this, the volume of consumer data can be aggregated, utilized, and shared through these products raises legitimate concerns about data rights (Du and Xie, 2021). The unanticipated use of consumer data can introduce numerous risks that include the unauthorized information use by third-party entities and intellectual property theft. Aside from upending trust between transacting parties, these issues can ensnare a company into costly and time-consuming litigation efforts.

The Social Consequences of Adopting AI

As AI is relatively new in the business landscape, there are few industry standards for AI adoption yet (Cheatham et al., 2019). Cheatham et al., (2019) find that in this vacuum of knowledge, corporate executives are often willing to overlook the potential risks associated with adopting AI technologies and/or overestimate risk-mitigation capabilities because they may offer a financially competitive edge. Likewise, business leaders are likely to underestimate the technical support needs associated with AI products and/or develop a false sense of security that in-house IT employees and analytics teams can step in to address problems that these products introduce. This can lead to a number of unintended consequences that can create risks at the individual, the organizational, and the societal levels. Table 3 presents an overview of these risks.

Table 3. The Unintended Consequences of AI Implementation[3]

Individuals	***Organizations***	***Society***
Physical safety Reputation Career prospects	Firm performance Legal compliance Reputation	National security Economic stability Infrastructure integrity Political stability

At the individual level, an uncritical strategy for AI implementation can pose several risks. Within an organization, an employee can experience physical harm if an AI system makes an incorrect evaluation of risks or fails to adequately identify them. For instance, a person operating heavy machinery may experience injuries if they are not able to identify circumstances where AI systems should be overridden either because the systems are too complex, or they are too distracted. Moreover, people can suffer reputational damages from AI-related mistakes. For

[3] A similar table appears in (Cheatham et al., 2019).

instance, given the occasional unpredictability of algorithms, an overreliance on AI to make critical decisions may cause an employee to struggle to explain the rationale for courses of action if it leads to a negative outcome. This could foster mistrust among colleagues about job competency and reliability. Finally, there are widespread ethical concerns associated with the potential effect of AI on the employment landscape. This is scholars have referred to as "technological job loss" (Ogle, 2018). By outsourcing decision-making to thinking computers, managers may become aware of previously unknown cost-savings opportunities which could threaten the career prospects of many people should they be displaced by a software system.

At the organizational level, malfunctioning or improperly calibrated AI solutions can become a threat to firm performance. Though generally AI has been found to have a positive impact on shareholder value, firm profitability, and cost savings (Kim, Park, and Kim, 2022), these products can unwittingly throw organizations out of compliance with rules and regulations regarding interfirm competition due to their novelty in the corporate landscape (Petit, 2017). One concerning way that this occurs in when firms are not adequately prepared for the unpredictable event that the algorithms driving AI products begin to communicate with one another and/or

---

learn autonomously. Popularly coined by scholars as "algorithmic collusion," this can expose firms to legal liability (Calvano et al., 2020). For example, algorithmic collusion can result in accidental price fixing among firms that are supposed to be in competition with improper human monitoring. The resulting antitrust lawsuits that could emerge from this type of anticompetitive conduct poses a particularly potent threat to firms. Likewise, an overreliance on AI at the organizational level can introduce cybersecurity risks for firms. The leak of sensitive operational data, or worse, the loss of operational control due to a cyberattack may cause firms to suffer irreparable reputational harm. This can deteriorate trust with the trade partners, consumer groups and the public sector at large.

Finally, and most importantly, AI has emerged as a transformative force that has the broad potential to inflict societal harms if improperly used. For instance, while organizations have increasingly turned to AI in risk mitigation efforts, these algorithms can also be used exploit vulnerabilities in the critical infrastructure that the public relies upon. Scenarios that have been considered in research include AI-hosted attacks on power grids, telecommunications systems, and financial networks (Kaloudi & Li, 2020). The potential for AI to simultaneously act as a shield and a weapon in cybersecurity efforts is what scholars have referred to as the "doubleedged sword" (Taddeo, McCutcheon, and Floridi, 2019). That is, while AI harbors the potential to revolutionize how we safeguard critical infrastructure sectors from threats, it also has the capacity to facilitate new avenues of attack that threaten national security, and economic and political stability.

A WAY FORWARD: ANTICIPATING THE FUTURE OF AI IN SCRM

Best Practices for Integrating AI into Business Processes

In the management literature, scholars have recently turned to stakeholder theory and social contracts theory to develop a series of best practices for AI implementation in businesses (Wright & Schultz, 2018). According to stakeholder theory, any group or individual who can be affected by the achievement of a firm's objectives has the right to expect that the firm will consider the moral implications of these objectives. Likewise, according to social contracts theory, the privileges associated with doing business should be counterbalanced by a normative (or standardized) approach to business ethics. Accordingly, Wright & Schultz (2018) advocate for several recommended practices for AI adoption. Among these, three recommendations are pertinent to supply chain managers that seek to leverage the proposed benefits of AI in risk management protocols while also buffering against potential ethical concerns. These include: 1. Transparent acknowledgement, 2. Workforce investment and retraining, 3. Embracing regulation and oversight.

Transparent Acknowledgement

With the understanding that outsourcing decision-making and automating tasks is only going to increase as AI evolves, stakeholder theory argues that firms should be prepared. Refusing to explore the opportunities that AI creates to improve organizational agility, resilience, and efficiency is tantamount to negligence. Beyond this, firms also face additional risks associated with becoming obsolete. Relying on antiquated technologies to support core organizational tasks can become a threat not just to the long-term survival of a firm, but also to entire supply chains. In critical infrastructure sectors, firms are essential product or service providers and could be rendered non-operational due to a breakdown. Transparently acknowledgement refers to a sector wide, cross-organizational effort to publicly recognize AI as an inevitable industry standard. Importantly, this does not mean uncritically adopting AI technologies. Rather, through transparent acknowledgement firms can balance the process of identifying and selecting the appropriate AI solutions to meet their risk mitigation needs against the imperative to maintain awareness and exercise strategic caution. Transparent acknowledgement may help initiate what management scholars call "interorganizational spillover" (Shi, Wajda, & Aguilera, 2022). This refers to the "unintended impact of an event in a focal organization on the perceptions and decisions of other organizations that belong to the same categories as the focal organization (i.e. peer organizations) as well as their stakeholders" (p. 185). Stated differently, transparent acknowledgement can become the catalyst for normalizing AI among other firms that may be more apprehensive. This could have a twofold benefit of leading to more cross-industry knowledge, while also pressing for more tailored AI solutions that can meet the specific needs of unique sectors.

Workforce Investment and Retraining

The growing rate of adoption has serious implications for the human workforce in the future. These issues concern how to manage the producers of AI products. For instance, though concerning, algorithmic bias simply reflects the humanity behind the math rather than a fatal flaw in technology itself. With careful attention to how these systems are designed and a robust critical human evaluation of the outputs these systems make, supply chain managers can greatly reduce the impact of algorithmic bias in the decision-making process. These issues also concern who is affected by AI tech. There is a clear need for investment in training and retraining initiatives to prepare employees on how to responsibly use AI. Suggested ways include developing reeducation programs to provide existing workers with the skills to adapt to the transition toward an AI enabled workplace and retraining programs to that give displaced workers new skills that they can carry into different company roles or into different sectors entirely. Doing so has several intended benefits. Workforce investment and retraining can increase AI literacy while also ensuring that those working with this technology have the necessary skill set to simultaneously mitigate risks and not introduce risks.

Embracing Regulation and Oversight

While businesses are increasingly embracing AI technologies, so too are government entities. Regulatory bodies are taking steps to introduce governance frameworks that balance fostering innovation and economic growth against the need to establish guardrails that mitigate risks and improve accountability. As a result, businesses may be able to proactively begin the process of collaborative governance by demonstrating frameworks for adopting AI that similarly address these interrelated concerns. Defined, collaborative governance refers to public and private stakeholders working together with public agencies to engage in consensus building around the appropriate course of action (Ansell & Gash, 2008). Recent initiatives in the United States point to an opportunity for private businesses, and especially firms operating in critical infrastructure sectors, to collaborate with government entities by welcoming regulation and oversight. Recently, the U.S. congress passed several acts that are aimed at harnessing the potential positives of AI while establishing necessary constraints. Among them, the FUTURE of AI Act established a federal advisory committee to study trends in AI use and propose potential new regulations. Federal agencies have also taken steps to broaden their engagement with AI and ethics. In February of 2024, the Department of Justice announced that they had appointed their first official chief AI officer (Goudsward, 2024). Businesses can build trust with regulators by engaging in self-regulatory practices that demonstrate responsible AI use. Combining selfregulating practices with exercises in traditional competition, businesses may offer regulators a glimpse into potential industry standards that could be codified into law while minimizing industry disruptions. According to social contracts theory, this is referred to as weighing productivity against so-called “hypernorms” of fairness and healthy working environments (Wright & Schultz, 2018). By taking this tact, companies may be able to increase stakeholder representation in ongoing discussions about how to regulate AI in the business landscape by signaling that they have unique expertise and have done due diligence to consider the ethics of these technologies. Moreover, developing a closer relationship with regulators has the additional

benefit of including public agencies in risk management protocols that can improve response times and minimize negative outcomes.

Future Trends in AI Enabled SCRM

Employing the recommended practices outlined in the previous section will help to usher in the future of AI in SCRM. This largely centers around the concept of "Industry 4.0"– or the evolution of supply chain processes toward fully autonomous operation through the incorporation of smart technologies (Tjahjono et al., 2017; Akbari & Do, 2021). Scholars have argued that Industry 4.0 emphasizes not just expanding global networks of companies, but a new global network of machines that are specifically configured to share information and to control each other when carrying out specific tasks. At the core of Industry 4.0 paradigm is the integration of AI technologies into business processes such that production facilities and human actors are operating in holistic Cyber-Physical-Systems (CPS). CPS refer to "a new generation of systems with integrated computational and physical capabilities" that can impact the physical world through computation (Baheti & Gill, 2011 p. 1). According to Tjahjono et al., (2017), the emergence of CPS will occur through four separate avenues that will transform the business landscape:

1. The establishment of vertical networks of smart production systems. Manufacturing processes will be able to facilitate mass product and service customization through intelligent systems that will carry out not only production, but also maintenance tasks in the supply chain. Critical materials and resources will be decentralized and become universally available to production facilities through smart grids and novel storage technologies.

2. The horizontal integration of businesses into new global value chain network. Business models will continue to evolve into an ecosystem model that centers humans as essential, creative planners, controllers, and decision makers that are unspecific to outputs, but targeted on maintaining CPS processes.

3. Corresponding changes to the research and development cycle. CPS will allow engineering support to occur simultaneously throughout the value chain and facilitate innovation and improvement in design, development, and manufacturing processes. New products and systems will be based on BigData analytics and prioritize task automation to improve resilience.

4. The automated systems that emerge will facilitate rapid manufacturing, customization, and adaptability. These will reduce the overall costs of managing the supply chain while also providing novel opportunities to create value.

Though many of these dimensions are still aspirational in nature, significant advancements in AI have increased the plausibility of realizing the full transformation toward Industry 4.0 (Akbari & Do, 2021). Scholars have also argued that unlocking the full suite of risk management and threat mitigation techniques in this new industrial era will require revamping business processes around a logic of sustainability (Akbari et al., 2017). Though sustainability operates as somewhat of a buzzword in public discourse, it simply refers to strategies that simultaneously further business interests while achieving environmental, social, and economic improvements. Unsurprisingly, AI will be essential to this effort (Akbari & Do, 2021). Beyond risk detection and prediction, AItechnologies offer a potentially novel avenue for businesses to pursue strategies of sustainability that may affect the probability that risks emerge in the first place. For instance, AI will likely play an important role in reducing the carbon footprint of companies by accelerating the development of "green" technologies like carbon capture and storage processes that can be deployed widely across industries (Yao et al., 2023). These can have a palpable impact on reducing workforce-related burdens on the environment by streamlining operational practices (Ogbeibu et al., 2023).

CONCLUSION

Artificial intelligence (AI) represents a vast technological landscape. While innovations being built through AI have the potential to transform decision-making business environment, the novelty of AI can be daunting to supply chain managers working in critical infrastructure sectors. This paper outlines the types of risks that supply chains commonly face and describes several opportunities for AI-facilitated supply chain risk management (SCRM) practices identified in contemporary scholarship. It also describes several ethical challenges including algorithmic bias and the unintended consequences of AI-implementation that can affect individuals, organizations, and society. Finally, this paper provides an overview of suggested practices for businesses when deciding to implement AI and offers a glimpse into how employing these practices will inevitably transform supply chain risk management in the future.

REFERENCES

Agrawal, P., & Narain, R. (2018). Digital supply chain management: An Overview. *IOP Conference Series: Materials Science and Engineering*, *455*(1), 012074. https://iopscience.iop.org/article/10.1088/1757-899X/455/1/012074/meta

Akbari, M., Clarke, S., Dang, D., & Nkhoma, M. (2017). *Empirical social network analysis in sustainable supply chain in Vietnam—RMIT University*. 1–18. https://researchrepository.rmit.edu.au/esploro/outputs/conferenceProceeding/Empiricalsocial-network-analysis-in-sustainable/9921863043201341

Akbari, M., & Do, T. N. A. (2021). A systematic review of machine learning in logistics and supply chain management: Current trends and future directions. *Benchmarking: An International*

Journal, *28*(10), 2977–3005. https://doi.org/10.1108/BIJ-10-2020-0514 Alfalla-Luque, R., & Medina-López, C. (2009). Supply Chain Management: Unheard of in the 1970s, core to today's company. *Business History*, *51*(2), 202–221. https://doi.org/10.1080/00076790902726558

Ansell, C., & Gash, A. (2008). Collaborative Governance in Theory and Practice. *Journal of Public Administration Research and Theory*, *18*(4), 543–571. https://doi.org/10.1093/jopart/mum032

Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The Impact of Control Technology*, *12*(1), 161–166.

Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. *International Journal of Production Research*, *57*(7), 2179–2202. https://doi.org/10.1080/00207543.2018.1530476

Behret, H., Öztayşi, B., & Kahraman, C. (2012). A Fuzzy Inference System for Supply Chain Risk Management. In Y. Wang & T. Li (Eds.), *Practical Applications of Intelligent Systems* (pp. 429–438). Springer. https://doi.org/10.1007/978-3-642-25658-5_52

Calvano, E., Calzolari, G., Denicolò, V., & Pastorello, S. (2020). Artificial Intelligence, Algorithmic Pricing, and Collusion. *American Economic Review*, *110*(10), 3267–3297. https://doi.org/10.1257/aer.20190623

Cavelty, M. D. (2007). Critical information infrastructure: Vulnerabilities, threats and responses. *Disarmament Forum*, *3*, 15–22. https://www.academia.edu/download/3444596/pdfart2643.pdf

Chakrabarti, A., Ahmad, F., Jarke, M., & Quix, C. (2022). Monitoring Large Scale Production Processes Using a Rule-Based Visualization Recommendation System. *SN Computer Science*, *4*(1), 32. https://doi.org/10.1007/s42979-022-01419-z

Cheatham, B., Javanmardian, K., & Samandari, H. (2019). Confronting the risks of artificial intelligence. *McKinsey Quarterly*, *2*(38), 1–9.

Chen, M.-S., Han, J., & Yu, P. S. (1996). Data mining: An overview from a database perspective. *IEEE Transactions on Knowledge and Data Engineering*, *8*(6), 866–883. https://doi.org/10.1109/69.553155

Copeland, E. by B. J. (Ed.). (2004). *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life plus The Secrets of Enigma*. Oxford University Press.

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

Du, S., & Xie, C. (2021). Paradoxes of artificial intelligence in consumer markets: Ethical challenges and opportunities. *Journal of Business Research*, *129*, 961–974. https://doi.org/10.1016/j.jbusres.2020.08.024

Finch, P. (2004). Supply chain risk management. *Supply Chain Management: An International Journal*, *9*(2), 183–196. https://doi.org/10.1108/13598540410527079

Gallab, M., Bouloiz, H., Alaoui, Y. L., & Tkiouat, M. (2019). Risk Assessment of Maintenance activities using Fuzzy Logic. *Procedia Computer Science*, *148*, 226–235. https://doi.org/10.1016/j.procs.2019.01.065

Gereffi, G. (2020). What does the COVID-19 pandemic teach us about global value chains? The case of medical supplies. *Journal of International Business Policy*, *3*(3), 287–301. https://doi.org/10.1057/s42214-020-00062-w

Giannakis, M., & Louis, M. (2016). A multi-agent based system with big data processing for enhanced supply chain agility. *Journal of Enterprise Information Management*, *29*(5), 706–727.

Goudsward, A. (2024, February 22). US Justice Dept names first AI officer as new technology challenges law enforcement. *Reuters*. https://www.reuters.com/world/us/us-justice-deptnames-first-ai-officer-new-technology-challenges-law-enforcement-2024-02-22/ Guang, M., Yan, C., Wang, J., Qi, H., & Jiang, C. (2021). Benchmark datasets for stochastic Petri net learning. *2021 International Joint Conference on Neural Networks (IJCNN)*, 1–8. https://ieeexplore.ieee.org/abstract/document/9533785/?casa_token=nT8Bra01UbUAAAAA:R3-4xbLQDaFIhyinIfBrTvX-9RLLFM0chep6spW4-C5kumJdJEvaqb-HBOr6CDES_syNM8kUtw

Haugeland, J. (1989). *Artificial Intelligence: The Very Idea*. MIT Press.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research*, *53*(16), 5031–5069. https://doi.org/10.1080/00207543.2015.1030467

Ivanov, D. (2021). Supply Chain Risks, Disruptions, and Ripple Effect. In D. Ivanov (Ed.), *Introduction to Supply Chain Resilience: Management, Modelling, Technology* (pp. 1–28). Springer International Publishing. https://doi.org/10.1007/978-3-030-70490-2_1

Jin, G. Z. (2018). Artificial intelligence and consumer privacy. In *The economics of artificial intelligence: An agenda* (pp. 439–462). University of Chicago Press. https://www.nber.org/system/files/chapters/c14034/c14034.pdf

Kaloudi, N., & Li, J. (2020). The AI-Based Cyber Threat Landscape: A Survey. *ACM Computing Surveys*, *53*(1), 20:1-20:34. https://doi.org/10.1145/3372823

Kim, T., Park, Y., & Kim, W. (2022). The Impact of Artificial Intelligence on Firm Performance. *2022 Portland International Conference on Management of Engineering and Technology (PICMET)*, 1–10. https://ieeexplore.ieee.org/abstract/document/9882634/

Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: Review, synthesis, and future research directions. *European Journal of Information Systems*, *31*(3), 388–409. https://doi.org/10.1080/0960085X.2021.1927212

Latour, A. (2001). Trial by fire: A blaze in Albuquerque sets off major crisis for cell-phone giants. *Wall Street Journal*, *1*(29), 2001.

Mazzuto, G., Bevilacqua, M., & Ciarapica, F. E. (2012). Supply chain modelling and managing, using timed coloured Petri nets: A case study. *International Journal of Production Research*, *50*(16), 4718–4733. https://doi.org/10.1080/00207543.2011.639397

Min, H. (2010). Artificial intelligence in supply chain management: Theory and applications. *International Journal of Logistics Research and Applications*, *13*(1), 13–39. https://doi.org/10.1080/13675560902736537

Nooraie, S. V., & Mellat Parast, M. (2015). A multi-objective approach to supply chain risk management: Integrating visibility with supply and demand risk. *International Journal of Production Economics*, *161*, 192–200. https://doi.org/10.1016/j.ijpe.2014.12.024

Ogbeibu, S., Emelifeonwu, J., Pereira, V., Oseghale, R., Gaskin, J., Sivarajah, U., & Gunasekaran, A. (2024). Demystifying the roles of organisational smart technology, artificial intelligence, robotics and algorithms capability: A strategy for green human resource management and environmental sustainability. *Business Strategy and the Environment*, *33*(2), 369–388. https://doi.org/10.1002/bse.3495

Ogle, D. (2018). Management Challenges in Technological Job Loss. *2018 IEEE Technology and Engineering Management Conference (TEMSCON)*, 1–6. https://ieeexplore.ieee.org/abstract/document/8488446/?casa_token=ueNu1F9JJUgAAAAA:Qfn-j-L21KB8c38rFZmxBwfn35PoRKAFx6csCmw8TXvC0xRN80bNWlfVpPvqLIRffIfuBd9Bbw

Ojha, R., Ghadge, A., Tiwari, M. K., & Bititci, U. S. (2018). Bayesian network modelling for supply chain risk propagation. *International Journal of Production Research*, *56*(17), 5795–5819. https://doi.org/10.1080/00207543.2018.1467059

Oliver, R. K., & Webber, M. D. (1982). Supply-chain management: Logistics catches up with strategy. *Outlook*, *5*(1), 42–47.

Petit, N. (2017). Antitrust and Artificial Intelligence: A Research Agenda. *Journal of European Competition Law & Practice*, *8*(6), 361–362. https://doi.org/10.1093/jeclap/lpx033

Rangel, D. A., de Oliveira, T. K., & Leite, M. S. A. (2015). Supply chain risk classification: Discussion and proposal. *International Journal of Production Research*, *53*(22), 6868–6887. https://doi.org/10.1080/00207543.2014.910620

Remko, van H. (2020). Research opportunities for a more resilient post-COVID-19 supply chain – closing the gap between research findings and industry practice. *International Journal of Operations & Production Management*, *40*(4), 341–355. https://doi.org/10.1108/IJOPM-032020-0165

Sakhnini, J., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). AI and Security of Critical Infrastructure. In K.-K. R. Choo & A. Dehghantanha (Eds.), *Handbook of Big Data Privacy* (pp. 7–36). Springer International Publishing. https://doi.org/10.1007/978-3-03038557-6_2

Schurr, N., Marecki, J., Tambe, M., Scerri, P., Kasinadhuni, N., & Lewis, J. P. (2005). The Future of Disaster Response: Humans Working with Multiagent Teams using DEFACTO. *AAAI Spring Symposium: AI Technologies for Homeland Security*, 9–16. https://cdn.aaai.org/Symposia/Spring/2005/SS-05-01/SS05-01-002.pdf

Shi, W., Wajda, D., & Aguilera, R. V. (2022). Interorganizational Spillover: A Review and a Proposal for Future Research. *Journal of Management*, *48*(1), 185–210. https://doi.org/10.1177/01492063211040554

Slone, R. E., Mentzer, J. T., & Dittmann, J. P. (2007). Are you the weakest link in your company's supply chain? *Harvard Business Review*, *85*(9), 116.

Someh, I., Davern, M., Breidbach, C., & Shanks, G. (2019). Ethical Issues in Big Data Analytics: A Stakeholder Perspective. *Communications of the Association for Information Systems*, *44*(1). https://doi.org/10.17705/1CAIS.04434

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), Article 12. https://doi.org/10.1038/s42256-019-0109-1

Tjahjono, B., Esplugues, C., Ares, E., & Pelaez, G. (2017). What does Industry 4.0 mean to Supply Chain? *Procedia Manufacturing*, *13*, 1175–1182. https://doi.org/10.1016/j.promfg.2017.09.191

Varma, D. T. N., & Khan, D. A. (2017). *Information Technology in Supply Chain Management* (SSRN Scholarly Paper 2921128). https://papers.ssrn.com/abstract=2921128

Wright, S. A., & Schultz, A. E. (2018). The rising tide of artificial intelligence and business automation: Developing an ethical framework. *Business Horizons*, *61*(6), 823–832. https://doi.org/10.1016/j.bushor.2018.07.001

Yao, P., Yu, Z., Zhang, Y., & Xu, T. (2023). Application of machine learning in carbon capture and storage: An in-depth insight from the perspective of geoscience. *Fuel*, *333*, 126296. https://doi.org/10.1016/j.fuel.2022.126296

AUTHOR BIOGRAPHY

Alexander B. Kinney, Ph.D., is an Assistant Professor in the Department of Criminal Justice and Criminology at Sam Houston State University. His research unpacks the dynamics of social control in gray markets, uses automated text modeling algorithms to study the logics of deviant behavior, and theorizes punishment in a cross-historical context. Recently, his work has been published in *Social Problems*, *Crime & Delinquency, Law & Policy,* and other journals.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Kinney, Alexander B. (2024) Leveraging Artificial Intelligence for Supply Chain Risk Management (Report No. IHS/CR-2024-1003).
The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/TP3Q4