electronics

MDPI

Article

Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions

Theresa Sobb, Benjamin Turnbull and Nour Moustafa *

School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy, Canberra 2612, Australia; t.sobb@adfa.edu.au (T.S.); Benjamin.Turnbull@unsw.edu.au (B.T.)

* Correspondence: nour.moustafa@unsw.edu.au

Received: 15 October 2020; Accepted: 27 October 2020; Published: 6 November 2020

Abstract: Supply chain 4.0 denotes the fourth revolution of supply chain management systems, integrating manufacturing operations with telecommunication and Information Technology processes. Although the overarching aim of supply chain 4.0 is the enhancement of production systems within supply chains, making use of global reach, increasing agility and emerging technology, with the ultimate goal of increasing efficiency, timeliness and profitability, Supply chain 4.0 suffers from unique and emerging operational and cyber risks. Supply chain 4.0 has a lack of semantic standards, poor interoperability, and a dearth of security in the operation of its manufacturing and Information Technology processes. The technologies that underpin supply chain 4.0 include blockchain, smart contracts, applications of Artificial Intelligence, cyber-physical systems, Internet of Things and Industrial Internet of Things. Each of these technologies, individually and combined, create cyber security issues that should be addressed. This paper explains the nature of the military supply chains 4.0 and how it uniquely differs from the commercial supply chain, revealing their strengths, weaknesses, dependencies and the fundamental technologies upon which they are built. This encompasses an assessment of the cyber risks and opportunities for research in the field, including consideration of connectivity, sensing and convergence of systems. Current and emerging semantic models related to the standardization, development and safety assurance considerations for implementing new technologies into military supply chains 4.0 are also discussed. This is examined from a holistic standpoint and through technology-specific lenses to determine current states and implications for future research directions.

Keywords: cyber security; semantic systems; supply chain 4.0; blockchain; cyber-physical systems

1. Introduction

The term ‘Supply Chain 4.0’ is the physical and technological integration of systems across networks, which allows increased production, organization and profitability, characterized by autonomous actions independent from the location, prevalent integration, various automated services, and by its ability to react context to the customers’ needs and requirements [1–3]. This term was coined with the emergence of Industry 4.0 systems, specifically to denote the fourth industrial revolution and the integration of intelligent systems into supply chain systems. Such systems assist the industry and military in the production and manufacturing, emphasizing the global networks exchanging models and information as well as securely control them [4,5]. Supply chains are critical to organizations, enabling key procedures and logistics requirements to be met. In a military context, supply chains 4.0 exist as more than a means to an end in terms of profit and instead can have extended mission and life-critical consequences. Society has become inherently dependent on industrial systems-enabled computer networks for everyday digitized processes, and subsequently, this reliance incurs cyber vulnerability if such systems are compromised using complex cyber or physical hacking scenarios [1,3].

The development of, and protection against, cyber-attacks is a globally active area of research. Both nation and non-nation state capabilities continue to grow and become more proficient. At the same time, supply chains 4.0 is becoming increasingly lean, interconnected, and digitally-enabled [6]. The connection between digitally enabled supply chains (i.e., supply chain 4.0) and the increasing militarization of the cyber domain creates a research area of significance. The increasing dependency on computing and communications backbones is changing how supply chain mechanisms operate and interoperate. The devastation caused by exploiting a vulnerability in a military supply chain can have consequences beyond economics, effectively endangering human lives [7]. With the widespread procurement of defense products globally, the offensive surface for malicious actors has widened, bringing forth the potential magnification of adverse effects caused by a cyber-attack against systems of supply chain 4.0 [4].

The underpinning concepts of the global supply chain 4.0 rely upon the internet and network connectivity more than ever before. This dependency has security impacts on the effectiveness of such systems. Changes in the operating environment, technology and how systems and platforms are maintained are all playing a part in reaffirming the importance of global supply chains and implicating them as a potential target. Supply chain risk is defined as the sudden likelihood that affects the macro- or micro-level of the supply chain processes which lead to impact of any part of supply chain operations (including its Information Technology (IT) and Operational Technology (OT) [5,6]). Risk management, the process of predicting and assessing cyber risks to define risk events to avoid or minimize their effects [8], would assist in illustrating cyber risks faced supply chain 4.0. Supply chain risks are classified into two methodological types; disruption, and operation [9]. The disruption risk is caused by a natural disaster, such as earthquakes or flooding, and this type not simple to mitigate. The operational risk, such as cyber-attacks, treats with unsuccessful processes of the supply and demand operations while producing or delivering final products [8,9].

The emergence of mission assurance, agile life-cycle engineering and risk management processes, can enable standardizing the procedures of supply chain 4.0 and mitigating mission successes [10]. It also securely permits the execution of new technologies, for example, blockchain, the Internet of Things (IoT), applications of Artificial intelligence (AI), and Cyber-Physical Systems (CPS) [11], to offer automated and secure services to organizations, increasing the productivity and flexibility of supply chain 4.0 [7]. The mission assurance models could alter how militaries and defense organizations respond to Advanced Persistent Threats (APT) [12]. Applications of topics, such as the crown jewel analysis, business continuity methodology, ontological-based semantic models, service orchestration systems, and updating redundant and degenerate systems or processes can serve in achieving increased mission assurance within organizations. The technological landscape affects how militaries function and innovation within this field can bring forth both threats and opportunities to the effectiveness of military supply chain operations. There is thus an increasing need for defense organizations to have an ability to assess how new technologies may impact their supply chains so that they can integrate or mitigate as necessary [8,9].

This paper seeks to focus on the uniqueness of how militaries operate, with focusing on supply chain 4.0 and their integration with new technologies in a secure manner; where the focus is less on their networks and systems themselves but rather on the information they contain and the operational aspects they support. It provides a comprehensive literature review of the intersection between cyber security, defense mission assurance, supply chain 4.0 and semantic modeling. To achieve this, the paper explains: (1) the uniqueness of military organizational aims from a supply chain management context, given an increasingly connected world; (2) an understanding of the current state of military and defense networks as they pertain to logistics and supply chains; (3) the potential impact cyber-attacks that may have on supply chain 4.0 and discuss the increased vulnerabilities applying to the aspect of computing and communications; and (4) the variety of approaches that can be taken to assess how new technologies will affect a military supply chain. This work is novel in several ways; it outlines the emerging Supply Chain 4.0 concepts, links these to the emerging commercial and military needs, and outlines the need for semantic modeling for understanding the threats and opportunities in this space. Finally, this work outlines the underpinning technologies and outlines technology intersections in this unique areas with an increasing technological interdependence.

The structure of this paper is as follows; Section 2 outlines supply chains 4.0 and the unique characteristics of defense supply chains. Section 3 discusses the integration of supply chain 4.0 with new technological systems. Section 4 describes the risk management process and how it could be applied to supply chain 4.0. Technological-specific models for supply chain 3.0 are explained in Section 5. Finally, Section 6 concludes this work.

2. Supply Chain 4.0 Concepts and Insights

This section discusses the background of supply chains and its successor, supply chain 4.0. This section also highlights the increasing importance of supply chain 4.0 in military and commercial applications.

2.1. Supply Chains and Logistics Management

A traditional supply chain is a network of systems, process and organizations that produce value goods and services, and their delivery to their end user [3]. Supply chains are the binding link of nations; physical distribution networks and transport systems that in totality create a global network. Supply chains comprise "flows of materials, goods and information, which pass within and between organizations, linked by a range of tangible and intangible facilitators, including relationships, processes, activities, and integrated information systems" [4]. Their underpinning technologies are transport systems, communication platforms and networks, and physical distribution networks. Supply chains can generally be split into three phases; a procurement phase, production phase and a distribution phase [13].

Supply chains are part of, but different to, the concept of logistics. Supply chains incorporate procurement, manufacturing and distribution activities as part of a continuous and integrated process. The supply chain considers logistic "point-of-origin to point-of-consumption" as only part of its integration of all key business operations [14]. This includes alignment and synchronization of processes, electronic data interchange and the creation of long-term strategic partnerships. Manufacturing processes have begun to develop scaled flexibility, moving from large inventories to low lead time production and postponed product configuration; which, when coupled with demand management practices, offer maximum value for money with high degrees of flexibility.

2.2. The Importance of Supply Chain 4.0

Supply chain 4.0 is the integration of manufacturing and communication technologies that increase the productions of traditional supply chain systems by autonomous actions independent from the location, prevalent integration, various automated services, and by its ability to react context to the customers' needs and requirements. As shown in Figure 1, the dependence in the context of a supply chain in Industry 4.0, shows that the integration between customers, suppliers, tools, factories, and engineering for connecting by physical supply network [1,3].

Supply chain 4.0 generates a disruption that makes the companies rethink the design of their automated supply chain. Many techniques have emerged that update existing processes, due to the customers expectations in speed, reliability and transparency. In addition to the need for adaptation, supply chains also have the potential to significantly increase operational efficiency and take the advantage of advantages provides by emerging digital supply chain business models [5]. For the benefits to occur, supply chains must become faster, transparent, accurate and agile. Figure 2 demonstrates the advantages and disadvantages of an integrated smart network with supply chain to design supply chain 4.0 systems.

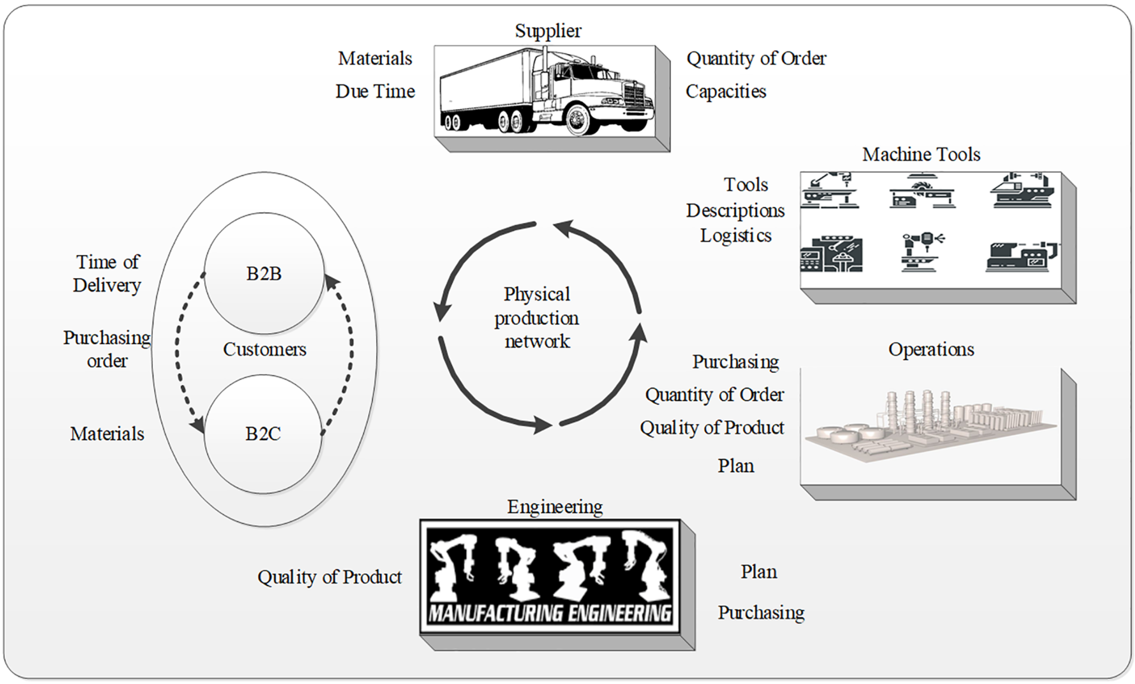

Figure 1. Conceptual architecture of supply chain 4.0.

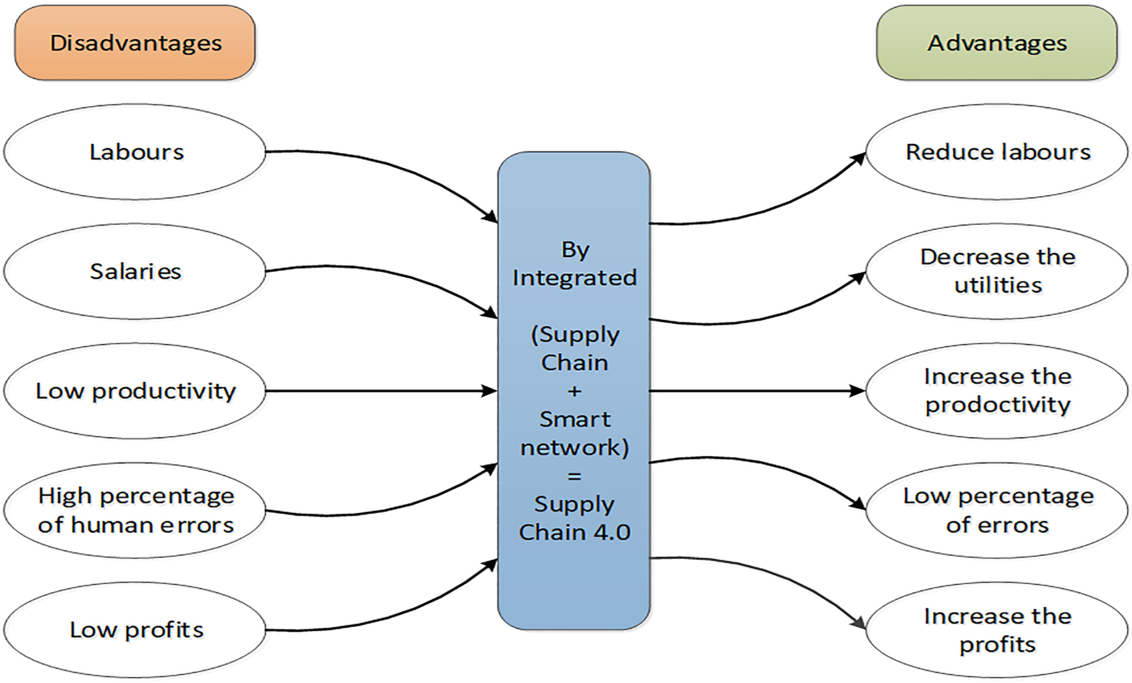

Figure 2. Integrating supply chains with smart networks, leading to supply chain 4.0 systems.

Different methodological approaches have been explored to define cyber risks from the supply chain, which is anecdotally the first stage in many accepted risk management processes [3,4]. The authors in [7] state that increased cyber threat intelligence would allow Industry 4.0 systems to increasingly automate cyber threat identification and understand immediate impacts of such systems. One of the largest challenges that faced previous studies is visible data sources or real data that help for getting accurate results for defining the cyber risk events from supply chain systems. The supply chain also impacts the foundation of information security as a technology function. Global supply chain efficiency and effectiveness measures inherently drive for standardization in equipment and processes, resulting in homogeneous networks, which increases the risk of vulnerability, but also reduces the threat surface available to an attacker. The basis of these issues have led to cyber supply chain risk management constructs specific to the field.

These cyber supply chain risk management includes the activities used to assess and mitigate risks across the end-to-end processes (including design, development, production, integration, and deployment) that constitute the supply chains for IT networks, hardware, and software systems. Effective and practical supply chain management requires the organization of network and business relationships across all stages of the chain. Complexity within supply chains brings forth issues of uncertainty that propagate throughout the entire network, potentially disrupting business operations [4]. Supply chain models must include considerations for uncertainty from suppliers, manufacturers and customers to strategically mitigate against the adverse consequences of supply chain variability [10]. The ability of an organization to uphold supply chain effectiveness relies on the quality of products, the speed of delivery to markets, and the agility alter based on consumer need [13].

The foundational principle of supply chain management is to increase the degree of coupling between nodes within each supply chain, thereby decreasing the cost to serve or the time required to alter and adapt to external factors. Coordination is vital to reduce inventory holdings, remove constraints and obtain high-quality levels. Increased supply chain visibility provides timely and accurate information to supply chain managers [10]. This increased access to information enables knowledge and responsiveness to volatility, increasing effectiveness; whilst enhanced understanding of the lean supply chain value stream enables a reduction in waste and increases efficiency. Thus, a balanced combination of lean value streams and agility is needed to operate global supply chains effectively and efficiently.

2.3. Supply Chain 4.0 of Defence and Global Defence

The supply chain 4.0 enables military strategy, operations and tactics. Without an effective and efficient logistics and supply chain, military operations cannot be sustained. Military supply chains have different outcomes for civilian equivalents and operate with a distinct end-state to consider. Military requirements include readiness for conflict, supply chain flexibility, item diversity and unstable demands; demonstrating a divergence from standard civilian outcomes [15]. Subsequently, the attacks on military supply chains often target these unique requirements to have a measurable effect on armed force operations. The outcomes resulting from a supply chain 4.0 failure differ depending on the nature and purpose of a supply chain. While many commercial supply chains exist for the delivery of profit-enabling goods [16], products delivered through defense ones can influence the tactical and operational capability of a force, which therefore has a direct impact on human life and mission success.

Unlike many commercial supply chains, military platforms are less focused on profit maximization and more focused on security, which can bring forth conflicts of interest in joint civilian and defense ventures [17]. Strategy and logistics are intimately linked. Changes in global supply chains have a flow-on effect on military strategy and operations. The improved capacity to deploy forces, enhancement of survivability and the provision of more capable and interoperable logistic forces is linked to the goal of optimizing the logistics information system architectural framework. The organisation, oversight and ultimate delivery of logistics and supply chain functions for military applications necessitates strongly interconnected logistics information systems with strong security. For example, the Royal Australian Air Force publication outlining their approach to logistics mentions little on how the defense supply chain is secured and contains no mention of cyber security.

The global defense supply chain is central to the competitive advantage of corporations and is an interactive system enabling business processes within corporations to convert resources into products and services [4]. The transition to a service economy, which is based on information rather than inventory, has expanded virtualization in the supply chain through providing increased agility, process integration, supply chain virtualization and digitization, and market sensitivity [13]. The sharing of information over the supply chain leads naturally to the virtualized supply chain model, which logically leads to the integration of processes. Collaboration across the supply chain integrates buyers, suppliers, distributors and product designers through common systems and shared information. The concept of an extended enterprise relies on increased levels of trust and information sharing. The benefit is the extension of the organizational value chain into and across other organizations and industries. The integration of network actors and nodes into a common system provides a new level of competition, where the route to sustainable advantage lies in being able to leverage the respective strengths and competencies of network partners to achieve greater responsiveness to market needs.

Whilst militaries around the world will continue to follow industry by seeking to reduce inventory and increase efficiency, many strides have been made within functions and processes. The authors posit that more opportunities for improvement remain in end-to-end supply chain integration—spanning all DoD organizations and its suppliers—of processes that jointly affect total supply chain costs and performance. This is a broad goal that incorporates many suppliers and industries. A variety of efforts are underway to enhance these efforts. The Consistently Optimized REsilient Secure Global Supply-Chains (CORE) Project seeks to realize efficient, fast and reliable supply chains that are also agile, lean, resilient, sustainable, compliant and trusted. CORE works through a series of demonstrators using representative operating scenarios to show how a global secure supply chain can be achieved. The World Economic Forum (WEF) has developed a blueprint for resilient supply chains, incorporating partnerships, policy, strategy and technology [18].

There are several emerging ontologies and semantic models that seek to define and semantically model aspects business functionality, military supply chains, and emerging technologies such as Industry 4.0. When formalizing business processes, Business Process Model and Notation (BPMN) 2.0 is the most famous mechanism. There are numerous BPMN extensions that extend the formalized notation to incorporate modern concepts, including cloud platform integrations [19] and IoT platform usage [20]. There are emerging processes seeking to integrate BPMN into military missions and processes, although these are not available for peer review and analysis at the time of writing [21]. Alternative approaches to BPMN include The Open Group Architecture Framework (TOGAF) [22], and the military-focused Department of Defense Architecture Framework (DoDAF). These represent higher levels of abstraction than BPMN, but are widely accepted standards. Given the rapid growth and fast-paced research and development cycle currently being experienced in Industry 4.0, there is no updated, comprehensive ontology that captures this sector [22]. Instead, the majority of formal modeling approaches and ontologies in this space are focused on one aspect.

2.4. Supply Chain 4.0 Dependencies

There is a harsh underlying reality that impacts defense capability acquisition and development, despite the powerful drivers and tremendous advances evident in the evolution of the global supply chain. The US Department of Defense (DoD) has stated that in many acquisition processes, approximately 70% of electronics systems are outdated, superseded or out of production before the final system has been fielded. This has ramifications not only for system operations, but sourcing spare parts or ordering additional systems at a later date.

Despite the increased visibility across the integrated supply chain, the degree of transparency remains limited for a variety of reasons. In some cases, commercial drivers may inhibit information sharing. Proprietary data protection can obscure information and reduce assurance despite the existence of the data within the supply chain. Indeed, in some cases, the scale of global supply chains can work against smaller governments, such as Australia, where the volume of transactions is insufficient to provide adequate leverage to compel global providers to share information or work collaboratively.

Supply chains also include computational, IT and networking equipment. Concern over supply chain poisoning and other related vulnerabilities in procurement specifically in IT goods has seen multiple governments consider and implement bans on Huawei technologies from government and public platforms. This approach has been considered both overly broad and also potentially ineffective, as it does not address all types of supply chain attack.

2.5. Challenges of Defense Enterprise

There is a lack of current logistics strategy within defense organizations that addresses enterprise-level logistics challenges, therefore making it difficult to translate lessons from Defense's history and current industry into an integrated management model [23]. As supply chains exist as complex Systems of Systems (SoS), cyber vulnerabilities can have enterprise-level effects, especially when components of supply chains rely on Internet of Things data. The integration of supply chain subnetworks, technology and infrastructure within larger military ecosystems poses challenges to their effective security. Potential techniques to mitigate the threats posed by system integration within complex supply chain systems include the implementation of Enterprise Architecture (EA) approaches [24]. Common considerations of EA implementations comprise of isolation to reduce policy interference, context to modify policies as necessary, and agility to respond to changes effectively. In the past, grid services constituted an option for the securitization of complex EA, but these approaches do not establish a complete solution in modern scenarios [25].

IoT integration is a growing trend within commercial supply chains; and it is expected that these technology firms will, over time, enter into military supply chains. Therefore, the vulnerabilities present within IoT devices have the potential to compromise defense supply chain systems and networks. There are a variety of factors that can influence the vulnerability of IoT devices within supply chains, including specification limitations and resource constraints, cloud computing and processing implications, big data privacy, and price minimization [26–28]. While mitigations exist for these potential vulnerabilities, they can come at a cost to data transmission quality, finance, interoperability, resource requirements and elasticity, complexity, and holistic system feasibility [29–33]. The diversity of systems and technologies within military supply chains pose significant risks to the security of those chains. It is therefore imperative that supply chain security is built from the lowest level of individual nodes and components, up to the holistic ecosystem so that no vulnerability is overlooked that could have catastrophic consequences to the military's operations.

3. Integration of Supply Chain 4.0 with Technological Systems

Supply chains 4.0 consist of SoS and rarely exist as single entities. Subsequently, these systems need to be integrated for security to be effective, otherwise the weak link will always be targeted. The factors most commonly affecting the integration of supply chains include; information sharing, coordination, trust, willingness to collaborate, communication and common business goals [34]. The evolving military landscape introduces a variety of factors that influence the operation, vulnerability and resilience of defense supply chains. These factors include the connectivity and convergence of systems, partners and outsourcing, component lifespans, vectors for threat actors, and defense enterprise challenges.

3.1. Supply Chain 4.0 Connected Systems

Military supply chains rarely exist as a singular system and instead encompass the amalgamation of multiple SoS. The nature of this system amalgamation brings for enterprise-level challenges regarding the maintenance of such complicated supply chains. In both public and private organizations, externally connected systems contain their own capabilities, interoperability factors and availability needs that can generate challenges to integration [35]. There is no clear boundary between the SoS that make up a holistic defense supply chain 4.0, and the other information technology that is inevitably connected to it. As such, defense supply chains cannot be considered as lone entities, as they are often connected to systems that serve to inform the supply chain, rather than constitute it.

The concept of the Future Operating Environment significantly influences capability development efforts and direction. There is a strong need to understand the future operating environment when considering future force capabilities and structure, and also when considering current and future prioritization. The Army Cyber Institute describes the term "widening attack plain" to characterise an increased attack surface caused by the combination of increased numbers and diversity in systems, people and threats. This work concludes that "the biggest vulnerability of these systems is the very thing that will promote their use and adoption: efficiency. Market forces and business management reward efficiency, whether this is cutting costs or increasing production; both efficiency and productivity are highly valued. As these systems undergo a wave of automation with efficiency as the driving factor, they become increasingly easy to attack for threat actors. Stated simply: Efficiency is easy to hack" [36].

Emerging technology is also altering the future operating environment. The integration of Artificial Intelligence (AI) and Machine Learning systems, significant increases in the effectiveness and cost of drones and robotics, in conjunction with the ubiquity of Internet of Things (IoT) devices and capability, creates new developments that will translate into Supply Chain 4.0. International supply chains have the capability to benefit from each of these technologies in the future. This is described as "the network-based nature of the industry provides a natural framework for implementing and scaling AI, amplifying the human components of highly organized global supply chains" [36]. Such technologies present their own risks, allowing attackers additional vectors of attack, and in a military context, potentially allow hybrid cyber and kinetic offensive measures, AI systems that support targeting and speed up intrusion, and the weaponization of data. Equipment obtained by militaries is often sourced from vendors with complex and non-transparent supply chains, with components transiting through SoS before they are delivered to their final destination. It can be therefore difficult to determine accountability for the quality and integrity of individual components of products, and thus a shipment of electronic devices may be compromised before they even enter the military's supply chain 4.0 [37]. The integration of supply chain 4.0 processes seeks to enable a mutually beneficial environment that captures "the synergy of intra- and inter-company business processes to optimize the overall business process of the enterprise", which should be agile, lean, and resilient [38].

3.2. Convergence of Supply Chain 4.0

A supply chain 4.0-enabled convergence brings together different silos to form a view of the complete, or end-to-end supply chain. The Best Practices for Supply Chain Risk Management has observed the convergence of Operational Technologies (OT), which manage processing systems, industrial power generation and routing, manufacturing operations and control equipment; with Information Technologies (IT), which manage software systems and networks; and the supply chain, which manages the provision of suppliers, services and the movements of goods and components. The convergence of supply chain execution is necessary because of the cost and competitive advantages obtained through scaled efficiency gains across global supply chains. End-to-end visibility and integration from manufacturing to distribution enhance cross-functional collaboration, which brings agility and flexibility that is unattainable in large scale supply chains that carry high volumes of slow-moving inventory.

In military parlance, a Common Operating Picture (COP) is one step towards the supply chain convergence, by providing a single integration point for the current state of logistics processes. COPs are heavily used in military systems, missions and processes. However, a COP underplays the amount of integration and automation imagined by those developing our future systems. The degree of interconnectivity and integration in a converged supply chain future, across the globe, extends well beyond the concept of a COP. In short, the systems that militaries currently rely upon to track and monitor processes are not designed to work with the sheer volume and connectivity that future supply chains will have. The connection between physical and non-physical things creates new vulnerabilities that are incredibly difficult to describe and manage without 21st-century tools. The desire to manage risk through Microsoft Excel spreadsheets and PowerPoint belies the complicated nature of these systems. For example, the Joint Strike Fighter Program seeks to allow operating militaries to pay for performance rather than spare parts. This means that Lockheed Martin owns the management of that global supply chain, rather than the nations operating the aircraft platform. This has a significant impact on the sovereignty of the capability, and the ability for aircraft to be maintained in the event of a crisis that strains supply chain capabilities.

3.3. Partners and Outsourcing of Supply Chain 4.0

Supply chains are rarely constituted by a singular organization, and often instead rely on the acquisition of products from external suppliers and vendors. Supply chains consist of SoS, and rarely exist as single entities. Subsequently, these systems need to be integrated for the supply chain management approaches to be effective and feasible. Some of the factors most commonly affecting the integration of supply chains include; information sharing, coordination, trust, willingness to collaborate, communication and common business goals [34]. Four main categories of risk can be considered to armed force supply chains, being; partner risk, divulging secret risk, conflict of interest risk and management risk. These can manifest through a lack of cohesion between organizations about standards for cyber security, attackers achieving military outcomes through the targeting of civilian partners, conflicting perceptions of protective measure necessity and dispersion of trust through sub-contracting [1].

Application Programming Interfaces (APIs) aid in the development and utilization of software. APIs are often open so that application developers external to the platform organization can customize the application software for their own needs. This, however, raises concerns about loss of control of the platform through API accessibility [39]. Because of the misalignment of goals between military supply chains and commercial supply chains, being operational outcomes and profit respectively, a disconnect between defense organizations and their contractors and outsourcers can provide further opportunity for vulnerability [1]. A security breach within a military context can have significant consequences on people's lives and national interests. Conversely, within a commercial operation, the consequences are likely to be more financially centric. This issue is exemplified by an Australian Defense Force security breach in 2016, in which attackers achieved their objectives by targeting a vulnerability in one of the ADF's contractors.

Military supply chains can also be compromised due to the number and locations of the multitude of suppliers used to construct a product. Approximately 70% of international trade involves semi-finished products that are in the process of being remodeled into their final form. The globalized economy and transnational supply chains mean that even the simplest of products can have components from different countries and vendors. For example, a Dell Inspiron 600m Notebook contains components created in over ten countries, including the Philippines, Malaysia, China, South Korea, Singapore, Thailand, and India. Even the F-35 Strike Fighter aircraft; utilized by countries including the United States of America, the United Kingdom, and Australia; contains parts manufactured from around the globe, including China.

3.4. Supply Chain 4.0 and Cyber Threats

The cyberspace landscape is one that is constantly evolving, with developments and exploits being revealed regularly. In the year 2018 alone, 3297 vulnerabilities were recorded in the Common Vulnerabilities and Exposures database [40]. Cyber-attacks are increasing in both number and complexity year-over-year, becoming more sophisticated, and creating a variety of impacts on individuals, businesses and government [41]. Secondary targeting, which refers to malicious actors compromising enabling targets that can give them access to an organization with greater value, is a cyber assault vector that is pertinent to defense supply chain systems. In this case, an attacker may compromise a military system through one of their partners within the supply chain who has less developed and hardened network security.

Security through obscurity stems from historical perspectives that secrecy was the best form of security practice. Examples of security through obscurity may include modifying variables from default values or assigning unusual ports to services. The technique is often applied to systems of which people are ignorant such as SCADA systems. Whilst security through obscurity may act as a delaying tactic against adversaries, it does not constitute an adequate defense for a system [42]. Malicious actors do not always require a complete understanding of a system to attack it and reach their goals [43].

The last decade has seen a rise in the quantity, effectiveness and breadth of cyber offensive activities. The variety of Advanced Persistent Threats (APTs), issue-motivated groups and organized crime groups investing time and resources into cyber-attack are high [44]. The proven effectiveness of cyber strikes to achieve military ends cannot be disputed. Given this effectiveness, the supply chain, a fundamental component of the modern military, is a potential target. The interconnections of supply chain management; a nexus between government, defense and commercial systems, provides a potentially wide assault surface. Cyber defense is likened to asymmetric warfare, with malicious actors needing only to focus on the weakest node in a protected system.

Cyber-attacks within the commercial space often have some form of monetary outcome, be it direct, such as through ransomware; or indirect, such as through industrial espionage [45]. The WannaCry attacks of 2017 highlight how offensives can be driven by finance. In this attack users' access to data was blocked via encryption, which could only be regained after the payment of a monetary ransom [46]. In another example of hacking, the automotive sector has significantly replaced previously manual systems with electronic control units, many interconnected and potentially internet-connected. This adds new vectors for cyber-attack in physical systems, with little transparency or insight into how these systems operate. The long term impacts of the integration of significant IT into vehicles is not yet known.

Similarly, drones, robotic systems and other remotely operated systems also have similarly unknown cyber-attack surfaces. The warehouse of the future will be largely automated, staffed by sensors, actuators and robotic devices. Hypothetically, a cyber-attack against logistics systems could impact operations, divert critical equipment en route, move equipment through compromised routes, or disrupt the operations of a system and pause all logistics movement.

Given that it is expected that significant aspects of the future supply chain will be significantly automated, and susceptible to cyber-attack, the emerging paradigm for many military platforms is to assume that the security perimeters have been breached. Regardless of whether data is corrupted by an attack or random error, logistics support should be sufficiently resilient and robust to data corruption to continue providing adequate support to combat operations. In the event of a coordinated kinetic and cyber offensive, the ability of an adversary to manipulate or disrupt supply chains provides a competitive advantage, both in the operational environment and its immediate supply trajectories.

4. Risk Management for Supply Chain 4.0

This section explores the risk management process and how it would be applied to supply chain 4.0, and evaluates its applicability within a military supply chain scenario.

4.1. Risk Analysis

Risk analysis frameworks serve to aid organizations in determining their potential vulnerabilities and assessing how those vulnerabilities may affect the organization and its systems. Considerations for analysis techniques include determining whether the organization's information security focus is to prevent an intrusion from happening in the first instance, to respond effectively when one does occur, or both. The changing nature of risk analysis has seen a shift in mindsets from asset protection to business process or mission protection. The mission objectives used for these assessments influence the assessment weighting, with factors such as mission length and immediacy changing these ratings. Risk matrixes can also be used to evaluate the status of potential risks and their impacts within a system. In traditional risk assessment matrixes, severity and frequency are used to categorize risks, and fuzzy logic can be used to extend the possibilities beyond set classifications [47].

Crown Jewel Analysis refers to assessing cyber assets that are mission-critical to the system and using that information to inform further risk assessments in the kinetic, cyber and supply chain domains. The mission objectives used for these assessments influence the assessment weighting, with factors such as mission length and immediacy changing these ratings. Risk analysis frameworks serve to aid organizations in determining their potential vulnerabilities and assess how those vulnerabilities may affect the organization and its systems. Cyber Supply Chain Risk Management (CSCRM) is defined as the organizational strategy and programmatic activities [used] to assess and mitigate risks across the end-to-end processes that constitute the supply chains for IT networks, hardware and software systems. Considerations for analysis techniques include determining whether the organization's information security focus is to prevent an intrusion from happening in the first instance, to respond effectively when one does occur, or both.

Pettit, Fiksel & Croxton's Supply Chain Resilience Framework has three potential end states that determine whether a risk is excessive, performance is improved or profitability is eroded, depending on the potential risk state of the system. Capability factors that should be considered within the risk assessment that may not always be monetary, especially in military supply chains; with factors such as recovery, capacity, sourcing flexibility and organization impacting overall capability [48].

Given the increases in maturity cyber risk models that have occurred over the last decade, the future challenges of emerging techniques and paradigms regarding cyber breach incident response and harm minimization are apparent. New paradigms for addressing and minimizing the impact of cyber security events often necessitate changes to technology, process and network architectures. Understanding complex, adaptive, interconnected business processes such as supply chains in existing and emerging paradigms is not a trivial process and an active area of research.

4.2. Risk Management Models

Existing supply chain management models can be implemented into organizations to strengthen supply chain processes. First, the Six Sigma DMAIC model involves defining objectives of improvement to a process, then measuring, analyzing, improving and finally controlling the process [49]. In a 2006 analysis of the suitability of applying the Six Sigma methodology to the UK defense supply chain, it was determined that while the methodology could be utilized, there were limiting factors that reduced the likelihood of its implementation, including stock holding policies and activity levels [50].

The Cyber Kill Chain is a for defining the stages of a cyberspace-based attack. The phases of the Cyber Kill Chain are; reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Re-evaluations of the model within Cyber-Physical Systems have recommended changes to established understanding of attacks, especially within the realms of control systems and physical systems where outcomes have tangible consequences [51]. An alternative to the Cyber Kill Chain is the Supply-Chain Operations Reference model (SCOR), described as a cross-industry framework for evaluating and improving enterprise-wide supply-chain performance and management. SCOR outlines the following defined components, and how they inter-relate; processes, benchmarking metrics, management practices and software product mappings. The aim of SCOR is to "communicate, compare and develop new or improved supply-chain practices" [9].

4.3. Assessment of Existing Risk Management Models

Risk analysis and management models can be used to assess the potential hazards that may be introduced with the implementation of new technology into military supply chains. There are a variety of frameworks available, including CSCRM, risk matrices, Crown Jewel Analysis and the Supply Chain Resilience Framework. While these models will aid in the assessment of risk, they do not provide a holistic and balanced assessment of all the tangible and intangible considerations required when considering the implementation of new technology to military supply chains.

There have been several attempts to semantically model risk assessment processes and paradigms, with some success [52–54]. Considering the complexity, nuance and the context required for individual commercial, government domains and regulatory requirements, this is an ongoing area of research and development. The integration of cyber into these processes adds additional complexity, mapping and modeling needs.

Existing management models for cyber security and supply chain management generally focused exclusively on either cyber security or supply chains 4.0, but not on the intersection of both. There was some cross-compatibility between the models discussed however none identified the military context of supply chains specifically. While elements of these models may contribute to the understanding of how new technology may impact military supply chains, they do not constitute a complete solution and therefore the research gap remains.

5. Technological-Specific Models Used for Supply Chain 4.0

Defense supply chains are vulnerable through multiple attack vectors, and thus these vectors all need to be considered as part of the process of building military supply chain resiliency. Technology is an area that experiences constant growth. This is exemplified by Moore's law, in that computer boards are becoming more economical and accessible, which drives forward the development of new devices [55].

Since a holistic model could not be identified for the assessment of any technology's impact on military supply chains, this section will involve the examination of technology-specific models to identify key traits that could be cross applied into a technologically general model. Key criteria for this assessment will include the model's focus on supply chains 4.0, a military context, and purpose as an assessment framework.

5.1. 5G and Wireless Communication Systems

The fifth generation of wireless networks (5G) is an underpinning technology of the rise of the Internet of Things, Industry 4.0, and linked global supply chains. 5G promises to provide high-bandwidth, low-cost communications for heterogeneous systems through the utilization of higher frequency bands [56]. With the introduction of 5G, the required infrastructure for large scale track and trace systems, such as those needed for military supply chains, will become accessible for use. With the delivery of 5G networks comes both a greater availability of data and the presentation of new risks for IoT devices in supply chains.

One of the primary use-cases for 5G is the development of 'track and trace'; the real-time ability to locate goods in transit or inventory. Track and trace provides the opportunity to reduce the capacity of adversaries to perform supply chain poisoning or reduce supply chain performance for competitive advantage [57]. However, there are also potential disadvantages to the implementation of such technologies that may necessitate further research. Track and trace allow for the real-time monitoring of components within supply chains. Within a military context, this can have significant operational consequences, with such systems potentially being relied on for mission-critical activities, such as fuel delivery and ammunition transportation. Track and trace allow for more accurate forecasting and planning of activities and increases visibility within the supply chain. Some systems combine 5G with radio frequency identity (RFID) tags or similar systems to uniquely identify objects moving throughout networks [58].

5.1.1. Threats against 5G and Wireless Communication Systems

5G infrastructure relies on substantial, existing infrastructure, functionality at the required capacities [56]. Defense and military systems are potentially deployed to environments where such infrastructure either does not exist or is contested itself. Operating without externally operated networks adds challenges, as does the concept that such infrastructure may be owned, operated under the control of potential adversaries.

Cyber offensives focused on RFID infrastructure often assault the privacy, authentication or availability of track and trace processes and infrastructure [59]. These attacks can be manifested through actions such as accessing confidential tracking and inventory data, creating illegitimate tag identities and halting RFID services from being accessed when required to by legitimate vendors [15,59]. Remote identification, eavesdropping, denial of service, spoofing, replay and tracking assaults, are all potential threats to supply chains and their routed goods and services [15]; the latter potentially including military platforms.

Unfortunately, 5G infrastructure has limitations that impact its practicality for defense track and trace implementations. 5G experiences significant penetration loss, and relies on large scale application of multiple input-multiple output technologies to function at required capacities [56,60]. These requirements pose potential difficulties in operational military environments, where the appropriate level of infrastructure may not exist. Therefore, lower telecommunication generations may need to be relied upon, incurring slower data transfer speeds and potentially damaging the progression of an operation.

5.1.2. Assessment of 5G and Wireless Communication systems

Current solutions to address these areas of concern have manifested through the cross application of existing solutions from other cyber security fields, such as the introduction of cryptography [61]. However, commercial track and trace RFID tags can lack the required computational power to enable public-key cryptography due to its high complexity leading to small performance and large amounts of power consumption. As 5G technologies serve to enable concurrent track and trace data, threats to these systems can degrade real-time military capability requirements. This is an active area of research. Many studies into track and trace are narrow in their breadth, and their outcomes cannot be cross-applied to other emerging technologies for the military supply chain, especially when considering the consequences of 5G integration.

The US Department of Defense has attempted to implement the widespread application of RFID Track and Trace into its supply chain, dictating that all suppliers must conform with passive RFID tag requirements. This practical implementation brought forth challenges during its integration phase, indicating that there was a lack of accurate understanding in regards to how the technology would affect the supply chain; suggesting that further adoption assessments were required [62].

5.2. Cloud Computing

Cloud computing refers to the "applications delivered as services over the internet and the hardware and systems software in the datacentres that provide those services" [63]. Elements of cloud computing include containerization, computation, analytics, network connectivity, and storage; these are manifested into service categories, such as software as a service, platform as a service, networks as a service and infrastructure as a service. Innovations in areas such as edge and fog computing, which provide location-specific advantages to cloud, present new opportunities for technological applications, such as Fog-2-Fog collaboration [64]. In general, benefits of cloud computing include flexibility, location independence, scalability and cost effectiveness. However, cloud computing also brings forth new security threats for IoT devices.

5.2.1. Threats Against Cloud Computing

There are vulnerabilities in cloud computing systems that incur risk, including; service stability issues, memory allocation errors, network connectivity problems, server management issues, authentication query overflows and denial of service attacks [65]. Data routing between the source of IoT data and the cloud datacentres that process this data relies on secure and private end to end networking protocols [63]. Because of the variety of protocols that IoT devices and sensors may be utilising; such as WirelessHART, ZigBee, IEEE 1451 and 6LOWPAN; gateway device support can differ between these protocols. Smart Gateways and fog computing architecture are one proposed solution to increasing the interoperability of different IoT devices and sensors, but this comes at the investment of additional resources into the IoT cloud's infrastructure.

Since cloud systems involve the amalgamation of significant data reserves from multiple hosts in a highly virtualised environment, identity management becomes a substantial responsibility to providers. Clouds rely on multi-tenancy systems to effectively resource-share, meaning that different users are not separated at a hardware level. Multi-tenancy can bring forth confidentiality threats, as information can be breached and disclosed through data remanence when resource sharing allocations change. One method suggested for reducing data remanence is to encrypt data and then destroy the keys, so that even if it is accessed at a later date, it cannot be recovered.

Availability is another challenge for cloud for IoT [66]. IoT technologies that rely on cloud need regular access to these services for the provision and acquisition of data. Subsequently, when clouds for IoT go offline or become unavailable, the functionality of the affected IoT devices can be degraded. The nature of cloud computing makes it difficult for reliability models to generate accurate failure patterns, meaning that service dropouts can be unpredictable and availability can be hindered for several hours. Due to the ubiquitous integration of new IoT devices into many elements of society, the disruption of IoT cloud service can have devastating effects to users, such as stopping them from interacting with security or safety systems.

Denial of service attacks represent a particular threat to cloud computing systems that enable IoT technologies, due to the growing scale of new devices being adopted. Even though cloud services have a degree of elasticity for changing resource requirements, this does not incur immunity to denial of service attacks. Cloud decentralisation is one strategy for reducing the denial of service attack surface, but this can come at the expense of other security risks, such as reducing resource elasticity and more targeted attack behaviours [67].

5.2.2. Assessment of Cloud Computing Solutions

Cloud computing is destined to integrate into military supply chains as contracted vendors increasingly utilise these services for increased efficiency and cost reduction. As cloud computing continues to influence the integrated technological landscapes of businesses, government entities and citizens, understanding how introduction of cloud computing services may affect these stakeholders is essential.

An additional foundational technology for Industry 4.0 is fog computing. Fog computing [68] is a paradigm that extends cloud computing with compute and storage located closer than, but highly integrated with, the cloud. Time-sensitive tasks can be processed in the fog, and other aspects are linked to the cloud, linking the advantages of the cloud closer to the data sources. When applied to Industry 4.0, the low latency outcomes have several tangible benefits [69]. Fog computing has been considered and assessed in scenarios relating to UAV integration into disaster scenarios [64]. This study involved considering the impact that fog extensions to the edge of cloud within disaster contexts, such as floods, and how these technological advancements may induce increased Quality of Service (QoS) in disaster prediction and recovery planning. The research highlights several factors for consideration when assessing suitability of these fog implementations, including technical requirements such as frequency and range, collaboration of nodes, and coordination requirements including latency and reliability. While this research does not specifically focus on military supply chain scenarios, it serves a beneficial purpose in presenting key considerations for assessing how a new technology, such as fog, may impact existing systems.

The fog COMputIng Trust manageMENT (COMITMENT) approach serves to improve Quality of Service and Quality of Protection History metrics to improve the security of fog architectures as an extension of cloud [70]. This study has no military or supply chain focus, however the methods described within the approach are designed to have holistic and broad applications, making them useful for consideration in a variety of scenarios.

Tariq [71] proposes an Agent Based Information Security Framework for Hybrid Cloud Computing, which serves as a decision system through which threats can be assessed and responded to within cloud environments. The work is heavily focused on risk, and lacks consideration of consequences that extend beyond assets, threats and vulnerabilities within this context. The study also does not focus on defence supply chain scenarios. However, outcomes derived from the research's focus on judging the effectiveness of different risk assessment methods is useful when considering threats to cloud computing architectures, and could be considered within wider cyber security scenarios.

5.3. IoT and Industry 4.0 Systems

The IoT refers to the interconnection of computers online that obtain information about the physical world through observation, such as through sensors [72]. IoT enables the collection of data from reality, which encourages a shift in consumer experiences and a tendency towards situational trait customization. Fundamentally, IoT provides computation and internet activity into existing devices, allowing for heterogeneous networking devices to communicate at scale. IoT is also being incorporated into the manufacturing and distribution of goods. The utilization of IoT platforms has been credited for increases in industrial efficiency of up to twenty percent. Increasingly networks including enabling technologies such as wireless sensors and use of the cloud, are relied upon for the running of facilities, including within industrial control systems [73].

The IoT is itself an underlying technology for the emerging concept of Industry 4.0, which is establishing smart manufacturing processes. Industry 4.0 is also underpinned other enabling technologies in addition to IoT, including cloud, big data analytics, and cyber-physical systems [74]. Industry 4.0 promises great things; manufacturing on-demand, zero-energy buildings, smart-cities and automation across all facets of daily life. IoT enables the collection of data from reality, which encourages a shift in consumer experiences and a tendency towards situational trait customization. The technologies that enable the expansion of the IoT include Radio Frequency Identification tagging (RFID), sensors, Near Field Communication (NFC), cloud computing, Wi-Fi and Cellular Networks [75]. IoT is also being incorporated into the manufacturing and distribution of goods; allowing for customized and flexible product development processes [73].

A complimentary technology for Industry 4.0 is the growth and continued improvement of development on demand. Highly optimized and customizable manufacturing and supply chain management applications are increasingly allowing for immediate re-tooling and per-device tailoring. Linking these technology foci with developments in 3D printing, laser cutting, and other computationally controlled manufacturing allows for changes in their development and supply processes. 3D printers have the potential to create agility in supply chains, allowing equipment and spare part printing locally. This concept has been demonstrated with the 3D printing of tools on the International Space Station, designed on Earth. The increasing network connectivity that would allow remote printing and the creation of objects also increased a cyber-attack surface. 3D printing technologies will alter both the capabilities and the risks associated with supply chain management. The increasing network connectivity creates new ways to disrupt agile supply chains.

The implementation of Industry 4.0 within military supply chains has the potential to enable agile, quick response supply and product development, in addition to transforming military consumers into 'prosumers', being production consumers. The degree of customization provided by Industry 4.0 poses opportunities for defense forces as their equipment may be more easily and readily be adapted to their environment and logistics support can be more reliably planned. In the scope of military supply chains, Industry 4.0 is likely to change how products are sourced and manufactured. Future dynamic topology designs for Industry 4.0 may provide the flexibility and mobility needed for supply chain operation within agile military environments. However, Industry 4.0 also has some potential security issues [76], and the systemic effects of cyber protective measure breaches across Industry 4.0 implementations are not fully known.

5.3.1. Threats against IoT and Industry 4.0 Systems

Current IoT research challenges include standardizations, security issues, and data leak risks. Barriers to ubiquitous internet connections, such as through the security restrictions of connections, tactical considerations and network dropouts, have the potential to severely disrupt the conduct of armed force operations, particularly in field environments [77]. The confidentiality of military information also presents a challenge to IoT integration, with the potential for unauthorized capturing of defense information by devices [78]. Within the military context, IoT adoption is affected by several factors that reduce the feasibility of implementation, and subsequently, IoT technologies need to be carefully integrated and leveraged into the ecosystems of armed forces.

IoT devices rely on a network of infrastructure beyond themselves, including analytics platforms, data filters, and cloud frameworks. This places limitations on isolating military capability and services from commercial platforms and therefore increases the inherent trust that militaries need to have in third party service providers for their technologies to operate [77]. Furthermore, the service lifespan of such systems used by armed forces may be directly impacted by these third parties and their management of existing infrastructure. This brings forth further questions about jurisdiction over these systems, which constitute military capabilities, as to what modifications to and interactions with them are allowable by third party enablers.

The integration of fog computing into IoT and Industry 4.0 environments has both security implications and may also provide security enhancement in military environments. The use of fog architectures has potential for remotely deployed areas when strong cloud access cannot be guaranteed [79]. However, there are also several emerging fog architectural benefits that may provide additional performance and security benefits [70]. There are also strong areas of semantic research in this space and related areas [80], seeking to define and contextualise the domain.

Processing of data from IoT sensors and devices also poses challenges for militaries, due to the tactical requirements for real-time data and the technological requirements of third-party processing, filtering, and analytics [77]. In some military scenarios, it is not feasible to collect data, send it overseas to be processed, before returning that data to the original location. This requires a reliance on a complex chain of events, including traversal of multiple networks, including protected and public; encryption; trust in third party security; data warehousing and data mining analytics. The interconnectivity of remote manufacturing facilities and the ability to instantly reprogram and re-task manufacturing and commercial components in real-time also play essential roles in the construction of goods to set specifications. Connectivity and mobility are two key features of the product development process, which influences manufacturing designs within Industry 4.0. The benefits of development on-demand and Industry 4.0 technologies are in the reduction of movement and storage of specific goods, but the potential risks are yet to be assessed at a granular level [81].

5.3.2. Assessment of IoT and Industry 4.0 Solutions

Abdel-Basset et al. [82] suggested that the way to assess the impact on supply chains from the Internet of Things is from the “neutrosophic Decision-Making Trial and Evaluation Laboratory (N-DEMATEL) technique with analytic hierarchy process (AHP)”. AHP serves to determine both the cause and effect relationships of a supply chain’s security requirements through weighted criteria. The DEMATEL technique has been applied to multiple supply chain scenarios, including spare parts industries, eco-friendly supply chain management and consumer goods that require fast turnaround [83]. This technique, therefore, has the potential to be applied to military supply chain scenarios for various technologies, but would likely need to be incorporated within a larger model that addresses the unique characteristics of defense supply chains, such as in operational environments. Cyber risk assessments for IoT devices have also been proposed as strategies to determine the impact that these IoT technologies have on military supply chains.

5.4. Cyber-Physical Systems (CPS)

CPS' refer to systems that involve the integration of the computing and physical world through cyber-enabled control mechanisms . This crossover enables the "ability to interact with, and expand the capabilities of, the physical world through computation, communication, and control" [84]. CPS allows people to control and transform their physical environment through computer devices. They exist in a multitude of industries including energy, finance, manufacturing and transport [85].

CPS is often conflated with Supervisory Control and Data Acquisition (SCADA) systems, rather than it's logical successor, the Industrial Internet of Things (IIoT). Industrial equipment and critical infrastructure are heavily dependent upon SCADA and Industrial Control Systems (ICS), which often rely on Demilitarized Zones (DMZ) and air gaps between networks for security. The benefits of implementing SCADA within complex control systems include increased functionality, scalability, performance and openness. Additional advantages of SCADA systems include large data stores, the flexibility of data display, the potential for sensor connectivity, the ability to incorporate "real data simulations", the multiplicity of data types available and offsite accessibility.

CPS can be utilized within several areas of supply chains, especially within the manufacturing sphere. These systems have the potential to change how people interact with products and processes within the supply chain, potentially improving service level performance and flexibility [86]. Several CPS exist in armed force platforms. Maritime platforms, airborne systems, air-control and radar sensors, and other transport networks are all within this realm. The inability to maintain a supply of, adequately secure CPS platforms over the expected lifespan of military systems, sometimes decades, impacts both operational ability and transportation, an underpinning element of the supply chain itself.

5.4.1. Threats against Cyber-Physical Systems

Despite their benefits in safety and reliability, SCADA systems are often susceptible to cyber-attack. The majority of SCADA installations are tailored for long lifespans, minimal maintenance except when issues in production occur, and with a focus on availability. Such designs generally does not consider the application and network protection, and systems are often unpatched to the current state. Although related to IoT and Industry 4.0, CPS embodies cyber-physical connections across a different platform, one related to critical infrastructure and operational applications [87]. Such systems are on average older, utilize less-complex protocols, and are designed with a long lifespan in mind. This has numerous, acknowledged disadvantages from a cyber security perspective including; fewer updates, a difficult process for applying updates, long lifespans making replacement challenging, and the critical nature of these systems making the impact of an offensive potentially significant.

Threats to cyber-physical systems such as supply chains can cross over between domains, such as through cyberspace, the physical environment and the electromagnetic spectrum. Examples of these trans-domain threats include worm attacks on transportation networks, jamming of tracing signals and compromising of software integrity during production [88]. Emerging CPS are also not immune to attacks, with assaults having the same potential impact, especially on systems that operate in the logistics and supply chain management realms. Drones and semi-autonomous systems (including robotic ones) may provide strike surfaces for a cyber-attack, with the future warehouse being largely robotic. This poses potential risks from blended or hybrid attacks; hypothetically, a synchronised attack could divert critical equipment from its intended location before directing a kinetic attack to these areas. Disruption to semi- or fully-automated supply chain systems would be costly and take significant time to repair. the leaner the system, the more prone to this form of disruption.

5.4.2. Assessment of Cyber-Physical System Solutions

Much of the assessment relating to CPS relates to system modeling to determine suitability. Modeling is one technique that can be used to investigate how technology will interact within a system. In one study, challenges to effective modeling of CPS include the diversity in systems and programming, ability to adequately represent concurrency in real time Operating Systems, and system sensitivity induced by timing issues. Technological solutions to combat these challenges include the use of "hybrid system modeling, concurrent and heterogeneous model, the use of domain-specific ontologies and the joint modeling of functionality and implementation architectures" [89]. While each of these modeling techniques has been evaluated within a supply chain fuel management system for military aircraft, this modeling system does not constitute a complete assessment of how technology will impact whole military supply chains.

In a different study, several modeling techniques for CPS were examined within a power systems environment to determine their value and suitability, including complex network models, finite state machine models, network attack models, analytical models and variable structure system models, among others [90]. While power systems are an important component of supply chains, the focused scope of this study reduces its applicability across the variety of different systems and processes involved within the supply chains. Both of these studies demonstrate how modeling can be used to aid in determining how CPS will exist within different environments, but they do not constitute a holistic assessment. There is still significant value in identifying the modeling techniques most suited for defense supply chain environments, however, these models can only serve as one component of these assessments, as they do not address other consideration factors such as risk.

5.5. Blockchain Technology

Blockchain refers to a "data structure that makes it possible to create a tamper-proof digital ledger of transactions and share them" [91]. While widely known for its applications in cryptocurrency, blockchain technologies are applicable to many use-cases, systems and processes, including that of supply chains. Blockchain is in effect a distributed transaction-based ledger managed through synchronized states, via the use of cryptographic hash functions and digital signatures. It involves the decentralization and distribution of ledger content across peer-to-peer networks, and applies cryptography to records, with private keys acting as digital signatures. The blocks within a blockchain contain several key pieces of information, which are then stored across its peer network. The blocks contain two segments, being their headers, which contain the previous block's hash value, the current block's hash value, the next block's hash value and a cryptographic 'nonce'; and their bodies, which contain transaction data including public keys, hashes and signatures [92].

While widely known for its applications in cryptocurrency, with use cases such as Bitcoin, blockchain technologies can be applied to a variety of systems and processes, including that of supply chains [92]. For example, it can serve as a digital ledger to record financial transactions between different vendors within a military supply chain environment, such as between contractors and a military unit. Blockchains provide a degree of verification within a network, even if the network is comprised of untrusted components. This ability to verify action is based on two components; the principle of consensus and either proof of work or byzantine fault tolerance. However, when applied to the context of the military supply chain, blockchain does not guarantee cyber security. Additionally, the specific blockchain implementation also requires consideration, as outlined with careful planning and governance to establish the parties participating in the consensus process. Without proper governance, there may be a possibility of politically centralizing some of the key functionality of the blockchain, limiting its capabilities, and providing a false sense of security.

A blockchain is a tool that can be applied to a diverse number of applications. A specific implementation of blockchain technologies, known as smart contracts, is discussed later in the following section. It can be combined with IoT to enable enhanced tracking and tracing of components within the supply chain. Implementations within the supply chain can increase security and enable resilience to cyber-attacks through the identification of vulnerable or potentially exploited components at all stages of the supply chain [91]. One proposed use of blockchain within supply chains involved the deployment of UAVs to collect track and trace data from RFID tags on industrial items [93].

5.5.1. Threats against Blockchain

There are some challenges posed to the application of blockchain technologies, including data privacy, operational resiliency, and governance of the systems. Undertaking application transition from legacy systems to blockchains can introduce organization inertia, and cost-benefit analysis is a tool that can benefit in those situations [94]. The decentralized nature of blockchain, combined with the overhead of operation, does not lend itself to all use-cases. Additionally, the design of blockchain in defending from some malicious attacks does not make it immune from others. Assaults such as the '51% Attack', identity theft and hacking of programming codes all pose risks to the integrity of blockchain processes [95].

There are several emerging semantic modeling efforts in this space [96]. The benefits of one or more semantic models related to blockchain are numerous; a strong semantic model highlights potential architectural weaknesses, provides clarity for implementation and addition, and will assist in integrating new technologies into existing platforms or systems.

5.5.2. Assessment of Blockchain Solutions

Determining the contexts in which blockchain is most effective is limited by the current literature, with a focus instead on how blockchain has been implemented into organizations rather than assessing its possible applications and impacts [97]. While blockchain technologies are experiencing increased interest for applications to industry, there are minimal evaluation techniques available to identify whether blockchain is suitable for implementation into a system [98]. One framework proposed is a decision tree, illustrated in Figure 3. This framework outlines which use-cases are suitable and also which are unsuited for the integration of a blockchain technology. A use case for this framework is supply chains, in which blockchain is identified as suitable for application [98]. While this framework provides relevant criteria for a supply chain application, military assessments would require more specific considerations of requirements, such as from an operational or tactical perspective. There is research into the semantic definitions of blockchain, but these are still progressing and are yet to see full implementation outcomes [96].

While there are existing blockchain evaluation procedures available, development in this area is ongoing [99]. The feasibility of blockchain within an organizational context can be assessed through considering the necessity of data management and data verification, the nature of innovative culture within the organization, and the correlation of suitable use cases with the organization's goals [99]. Instead of identifying the factors that may influence the suitability of blockchain application within government bodies such as militaries, this study only relays a warning of slow adaption [99]. Therefore, there is a need for a specific military perspective regarding this evaluation process.

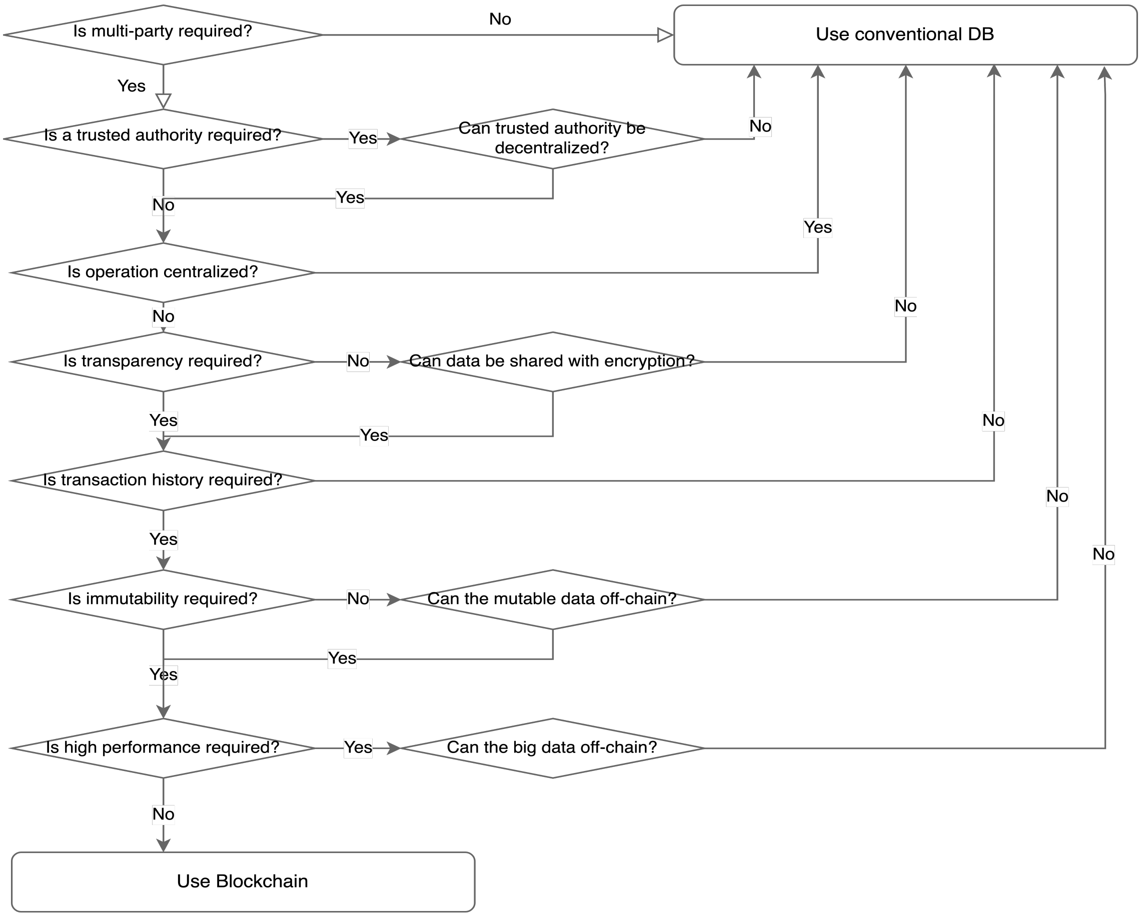
Is multi-party required?
No
Use conventional DB
Yes
Is a trusted authority required?
Yes
Can trusted authority be decentralized?
No
Yes
No
Yes
Is operation centralized?
No
No
Is transparency required?
No
Can data be shared with encryption?
Yes
Yes
No
Is transaction history required?
No
Yes
No
Is immutability required?
No
Can the mutable data off-chain?
Yes
Yes
Is high performance required?
Yes
Can the big data off-chain?
No
Use Blockchain

Figure 3. Blockchain suitability evaluation framework.

5.6. Smart Contracts

Smart contracts refer to "pieces of software that represent a business arrangement and execute themselves automatically under pre-determined circumstances" [100,101]. In the implementation, smart contracts are developed on blockchain technologies. Utilization of blockchain smart contract-based technologies, such as Ethereum, enable the creation, evaluation and execution of smart contracts for non-monetary transactions, which suit applications in supply chain management. Smart contracts can be used to validate product flows throughout the supply chain, ensure the quality and integrity of the chain, and finally monitor the status of items within the chain [101]. In the implementation, smart contracts are developed on blockchain technologies and enable programmability and customization of transaction criteria [102].

As smart contracts are employed as programs for blockchain, they share some benefit from blockchain's key features including "decentralization, persistency, anonymity and auditability" [103]. Smart contracts can be used to cut out the 'middle-man' in transactions, as they serve to enforce the terms of the agreement for execution to occur. Using blockchain smart contract-based technologies, such as Ethereum, enables the execution of smart contracts for non-monetary transactions. Platforms such as Ethereum thus open up smart contracts to applications beyond cryptocurrencies, enabling blockchain storage of "general-purpose data expressible as a key-value tuple" [102]. Smart contracts are applicable to many scenarios, ranging from the smart property, e-voting, financial payments, insurance and identity management [104]. From a military supply chain management perspective, data stores recorded in blockchains via smart contracts may include the state of products within the supply chain, such as information about a specific load of fuel. Thus, smart contacts can be used to validate product flows throughout the supply chain, ensure the quality and integrity of the chain, and finally monitor the status of items within the chain.

The utilization of smart contracts within supply chains has the potential to enable a data-driven management approach within those systems. Maintaining the legitimacy and transparency of supply chain products and processes is one sector in which smart contracts can be applied, especially within the context of armed forces. For example, a smart contract could be utilized to ensure that certain military supplies are sourced from legitimate organizations, to reduce the risk of tampering. Within this sphere, smart contracts can add a layer of assurance to defense supply chain processes, and thus contribute to their overall security. However, such technologies are still in their infancy and have not been applied in circumstances that would validate their usefulness in this space.

5.6.1. Threats against Smart Contracts

Ethereum is one of the most notable smart contract frameworks, however, it is not immune to vulnerabilities, with one attack involving the temporary loss of sixty million dollars [105]. Therefore, while smart contracts may contribute to the securitization of the military supply chain, they are not invulnerable to cyber threats. Privacy is also a threat to the security of smart contracts, as while pseudonymous public keys are used to identify transactions, transaction data, such as balances, remain publicly visible [106]. While private blockchains offer a potential solution to this issue, they are often less secure due to their tendency to be centralized within a single organization [103].

Additional security risks have been identified with specific smart contract implementations. For example, the lack of permissions on the Ethereum network has been identified as a potential avenue for adversaries. Some of the problems experienced by smart contracts come from misunderstandings of contract semantics and the relationships between contracts and other network participants. Potential sources of security breaches as a consequence of these semantic issues include transaction-ordering dependence, where near simultaneous transactions are not ordered and executed correctly within the blockchain; timestamp dependence, where system times are modified to manipulate contracts that operate based on timestamp variables; the mishandling of exceptions within or between smart contracts; and re-entrancy, where calls are used to manipulate the state of contracts and invoke unintended outcomes, such as multiple currency withdrawals [107]. Failure to mitigate against these issues may invoke significant financial loss or compromise of information.

5.6.2. Assessment of Smart Contract Solutions

Evaluations of the suitability to implement smart contracts into a system are often considered within evaluations for its parent technology, being blockchain [98]. Smart contracts, while relying on blockchain technologies, are a specific subset with their own features, advantages, disadvantages and challenges. Mik attempts to argue the effect that smart contracts can have on organizations, but this comes from a contract law based perspective [108]. A holistic assessment of the effects of all blockchain implementations on a system or supply chain may not yield the same results as an evaluation of smart contracts alone. Subsequently, there is a need for evaluation within this sub-area.

While some studies have a greater focus on the applicability of smart contracts to businesses, these are often concentrated on specific cases; such pharmaceuticals, food safety and smart grids; rather than on building a model that can be used to assess the impact of smart contracts across all scenarios [109]. Lessons from these implementations can contribute to an understanding of the system features that complement smart contract application, however, they do not constitute a holistic framework. Emerging frameworks do appear to be forthcoming, with new semantic models.

5.7. Artificial Intelligence-Enabled Applications

Artificial Intelligence (AI) generally refers to systems that exhibit characteristics that replicate human behavior, working in autonomous, asynchronous and goal-oriented environments [110]. Artificial Intelligence within the supply chain context often serves to solve the industrial problems inherent within these systems, such as to do with operation synchronization, collaboration and distribution. Chaotic time series refers to deterministic systems with significant levels of complexity, with the prediction of these series applying to supply chain management practices [111].

Applications of chaos theory, being the study of how simple conditions can lead to complicated and perceived unpredictable behavior, have the potential to improve the tools developed to the effective management of supply chain systems. Machine learning refers to computer programming intending to optimize performance to solve a particular problem [112]. Artificial neural networks, which refer to input-output mapping based on biology, have been applied to supply chain management and incurred more effective utilization of AI agents and total supply chain order fulfillment in test environments [113].

5.7.1. Threats against Artificial Intelligence

There are, however, vulnerabilities to machine learning applications within supply chain processes regarding verification and inspection of neural networks. Verification and Validation (V&V) represent the primary tools used to ensure accuracy and reliability in artificial neural networks [114]. Obtaining complex AI systems also presents issues of trust when users cannot have a complete understanding of the application [115]. Considering the specific demands of defense supply chains, the application of machine learning and artificial intelligence must pass these V&V tests, because the outcomes of misinformation can have severe human and operational consequences. Therefore, AI systems must be truly fit for purpose in military environments, which raises questions regarding the assessment criteria to determine how to fulfill these demands.

5.7.2. Assessment of Artificial Intelligence Solutions

Research into AI within the supply chain is highly focused on how it has been implemented into specific scenarios, rather than an assessment of the suitability of applying AI in the general case. For example, artificial intelligence has been applied within the supply chain management space to aid organizations. The application of AI agents within a cooperative supply chain environment can aid in the management of disturbances that occur within the supply chain processes [116]. For example, the case study 'The Beer Game', involving retailers, wholesalers, distributors and manufacturers, provided artificial intelligence agents a scenario to effectively respond to changes within the business environment. Machine learning techniques, such as artificial neural networks, have been successfully implemented in studies, with outcomes including enhanced forecasting accuracy and automatic reconfiguring of supply chains [117].

A suitability assessment model for agent-based distributed intelligent systems has been developed and implemented in a Battlefield Information System scenario [118]. This demonstrates its potential applicability to military systems. The study does not specifically mention supply chains, but could potentially be adapted to investigate them, considering that some of the environmental properties of the solution align with that of supply chains including; uncertainty, dynamicity, dependability and distributed environment. Buckland and Florian propose framework for considering "the role that artificial intelligence might... play in information systems" [119]. Their approach specifically identifies "users' expertise, task complexity of information system use, artificial intelligence and information service mission" as elements of this framework, and how the multidimensionality of some of these elements affects their assessment [119]. This approach is designed to be broad-reaching for different information systems and scenarios, and therefore its conclusions may apply to a military supply chain assessment approach when considering AI technologies specifically.

5.8. Summary of Threats and Assessment Models

Adoption assessments are often particularly specific to a technology, making their widespread applicability difficult. In this section, several currents and emerging technologies were described with their significance to military supply chains. The approaches then used to determine their applicability were then evaluated to identify whether there are common impact modeling threads across these technologies.

There are several independent research areas that seek to formally model and define each of these areas, with multiple models in development. Integration of these new models, with each other and other predefined models in related areas of discourse, is a future research challenge in this space.

Of note, the status of wireless communications, Cloud computing, the Internet of Things, the Industrial Internet of Things, Industry 4.0, track and trace processes, cyber-physical systems, blockchain technologies, and Artificial Intelligence all contribute to supply chain 4.0 exploitability, and thus must all be addressed to enhance supply chain security. A common trend throughout the approaches described within this section is a lack of cross applicability of the frameworks across different and new technologies and common absence of military focus.

5.8.1. Assessment of Key Considerations

Several key lessons are drawn from the examination of approaches that can be applied to assessments of technology implementations to defense supply chains. Each technology-specific approach discussed was varied from the others, indicating the importance of considering this factor when determining how technology will impact defense supply chains. As an extension of this, the implementation context, such as the environment, purpose, and objectives of using the technology, must be identified. Risk furthermore must also be considered to ensure that the potential consequences of implementation are understood. These ideas all contribute to the development of understanding regarding technology's potential that exists within the defense supply chain. Table 1 highlights the states of each of these in regards to each of these areas.

Technology-specific security concerns must be considered as part of any impact assessment. While an examination of technology-specific approaches provides insight into common considerations for implementation assessments, the diversity of technologies available voids any of these approaches as a complete solution for new technologies in general. One of the primary challenges with taking a technology-specific approach is revealed through obsolescence. The technologies discussed have relevance within specific contexts, and subsequently, the frameworks used for their assessments may lack the longevity needed for future assessments, even for newer iterations of those same established technologies. Nevertheless, characteristics, features and traits of specific technologies must be considered as a component of the assessment, as they still have consequences within employed solutions.

The specific features of the implementation context must be considered. This goes beyond simply identifying a military supply chain ecosystem and must extend to the nature of each environment. Examination of technology-specific approaches demonstrates how specific military environment features, such as potential operation in infrastructure-limited areas, affects the feasibility of implementation. Furthermore, the nature of the specific supply chain environment must also be considered, such as the nature of digital supply chains and physical supply chains. Military supply chain environments rarely exist as encapsulated systems, and thus complexity traits must also be considered as part of the implementation context. Consideration of risk is a critical component of assessing the impact of technology to defense supply chains 4.0 but should be considered within a larger, holistic approach. Risk assessments have value in understanding the potential consequences of actions, but they need to be taken into account within the context of other key factors that contribute to decision making. The justification of risk is thus another valuable component of impact assessment.

In some cases, external factors will dictate that implementation must occur, and new technologies must be integrated. These may be the result of partners, business decisions, or a need to upgrade legacy platforms. In such cases, formal models provide a greater insight into the technological platforms themselves, processes and mechanisms for analysis and consideration. There are significant benefits to formally modeling processes, systems and their components, and integration is one of these.

Table 1. Technology-Specific Approaches.

Technology	Approach	Considers Supply Chains	Considers Military	Assessment Framework
Communications Enabled Track & Trace	Feasibility of cryptography-based solutions	-	-	-
	US Department of Defense RFID Track and Trace Implementation	X	X	-
Internet of Things & Industry 4.0	N-DEMATEL and AHP assessment	X	-	X
	Design principles for cyber risk impact assessment	X	-	X
Cyber-Physical and SCADA Systems	Modeling evaluation in the context of CPS challenges	X	X	-
	Modeling evaluation in the context of power systems	X	-	-
Blockchain	Blockchain suitability evaluation framework	X	-	X
	Blockchain use case feasibility study	X	-	X
Smart Contracts	Smart contracts: terminology, technical limitations and real-world complexity	-	-	-
	Use-case of blockchains in the pharma supply-chain	X	-	-
	Blockchain-based smart grid proposal	-	-	-
	Supply chain traceability system for food safety	X	-	-
Artificial Intelligence	Management of Supply Chain Disturbances	X	-	-
	'The Beer Game'test	X	-	-
	Machine learning technique applications	X	-	-
	Suitability assessment model for agent-based systems	-	X	X
	A framework on expertise, task complexity and AI	-	-	X

5.8.2. Assessment Evaluation

Ultimately, while all models identified were related to a specific technology, or met some of the assessment criteria, no model was able to meet all of the topical criteria identified. This lack of crossover is highlighted in Table 1, where no approach met the three criteria of supply chain consideration, military consideration, and existence as an assessment framework. Several key trends were identified throughout the approaches and highlighted the need for a general approach to still consider the specific features of technologies, their implementation environments and risks, as part of a larger framework model. Therefore, while no technology-specific approach can be used to assess how implementing new technology will affect military supply chains, the amalgamated lessons from examinations of several approaches indicate key areas of assessment consideration for future work in this research area.

6. Conclusions and Future Work

One of the future cyber security battlegrounds for military and defense systems is supply chain 4.0 systems. With the changing landscape of technology and the role of the military, the interconnectivity within commercial and global systems, and the increasing reliance upon this connectivity, the importance of understanding defense supply chain vulnerability is demonstrated. Although defense and military networks are increasingly interconnected with commercial systems, they are also unique in their requirements and processes. There are several emerging technologies and drivers that will change the global supply chain over the next decade. Some of these technologies are potentially beneficial, while some introduce threats or vulnerabilities. Often, these new developments encompass both. Such technologies include the continued power of ubiquitous computing, adoption of cloud-based applications and the evolution of cyber-physical systems and platforms. It also involves technologies such as blockchain and smart contracts.

Changes to the manufacturing process itself, in the form of 3D and additive printing, Industry 4.0 and the Internet of Things, will also change the effectiveness and processes for the supply chain management. These too may induce cyber security concerns, and the scale of impact is yet to be fully evaluated. What is certain is that as technologies are developed and implemented, they will be applied to supply chains. It is not possible, nor necessarily preferable, to ignore new developments due to their potential risks. Instead, decisions on their applicability, use, and limitations will need to be made, in addition to research on what their risks truly are in an operational context. As demonstrated in the literature, the range of emerging and current technologies that have the potential to impact how military supply chains operate is extensive. Each technology represents its own field of research, in which more nuanced assessments can be made. The use cases present are generally focused on encapsulated systems, revealing the need for an overall generic understanding of how new technologies may affect military supply chains before they are implemented, from a cyber security perspective. Whilst these specific case studies do not constitute frameworks that can be used to understand the suitability of applying new technology to military supply chains; three key factors were recognized as considerations for future work. These were; examination of technology-specific features, deliberation of their contextual implementation environments, and assessment and justification of cyber risk. Consequently, consideration of these factors can aid in helping researchers understand what factors enable the successful integration of these technologies and inform how they affect the cyber security of their respective systems.

Military studies tend to focus on either case evaluations of practical implementations, such as the United States of America's Department of Defense's application of RFID Track and Trace technology to their supply chains; or focus on the applicability of a singular technology to military or general supply chains, such as the blockchain decision tree for supply chains. The holistic frameworks considered generally lack a focus on military supply chains, which have features unique to commercial chains. Therefore, while the approaches can be considered, they do not constitute a complete solution to addressing the impacts of new technologies on military supply chains. Changes to global supply chains are necessary to improve efficiency, grow interconnectivity, and implement more rapid and effective processes and architecture. However, the unique needs of military systems must be taken into account when adopting or adapting technology for these use-cases.

Military supply chains have different aims and objectives than commercial supply chains, with consequences to military supply chain management potentially affecting national security and human lives. The importance of these chains for the sustainment of military operations cannot be underestimated, and in a world where the cyber domain is becoming a new platform for warfare, understanding how different technologies may affect the security of the military supply chain is essential. Subsequently, militaries should have tools that enable them to accurately assess the cyber security impact that new technologies may have on their supply chains 4.0 so that they are better able to mitigate against cyber security threats and build cyber resiliency. Thus, this work has highlighted areas that would benefit from future research, to assist in the creation and maintenance of secure, adaptable processes for understanding the effect of new technologies on military supply chains.

Author Contributions: Conceptualization, T.S., B.T. and N.M.; methodology, T.S.; validation, T.S., B.T. and N.M.; formal analysis, T.S., B.T. and N.M.; investigation,T.S., B.T. and N.M.; resources, T.S., B.T. and N.M.; data curation, T.S., B.T. and N.M.; writing—original draft preparation, writing—review and editing, T.S., B.T. and N.M.; visualization, T.S., B.T. and N.M.; supervision, B.T.; project administration, T.S., B.T. and N.M.; funding acquisition, Not Applicable. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The views expressed are the authors' and not necessarily those of the Royal Australian Air Force or the Australian Department of Defence. The Commonwealth of Australia will not be legally responsible in contract, tort or otherwise for any statement made in this publication.

Conflicts of Interest: The authors declare no potential conflict of interests.

References

1. Sharma, A.; Jain, D.K. *A Roadmap to Industry 4.0: Smart Production, Sharp Business and Sustainable Development*; Springer: Cham, Switzerland, 2020; pp. 23–38.
2. Mentzer, J.T. Defining supply chain management. *J. Bus. Logist.* **2001**, *22*, 1–25. [CrossRef]
3. Frederico, G.F.; Garza-Reyes, J.A.; Anosike, A.; Kumar, V. Supply Chain 4.0: Concepts, Maturity and Research Agenda. *Supply Chain Manag. Int. J.* **2019**, *25*, 262–282. [CrossRef]
4. Waters, D.; Rinsler, S. *Global Logistics: New Directions in Supply Chain Management*; Kogan Page Publishers: London, UK, 2014; pp. 100–127 .
5. Ivanov, D.; Dolgui, A.; Sokolov, B. The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *Int. J. Prod. Res.* **2019**, *57*, 829–846. [CrossRef]
6. Garrido-Hidalgo, C.; Olivares, T.; Ramirez, F.J.; Roda-Sanchez, L. An end-to-end Internet of Things solution for Reverse Supply Chain Management in Industry 4.0. *Comput. Ind.* **2019**, *112*, 103127. [CrossRef]
7. Moustafa, N.; Adi, E.; Turnbull, B.; Hu, J. A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems. *IEEE Access* **2018**, *6*, 32910–32924. [CrossRef]
8. Salamai, A.; Hussain, O.K.; Saberi, M.; Chang, E.; Hussain, F.K. Highlighting the Importance of Considering the Impacts of Both External and Internal Risk Factors on Operational Parameters to Improve Supply Chain Risk Management. *IEEE Access* **2019**, *7*, 49297–49315. [CrossRef]
9. Ho, W.; Zheng, T.; Yildiz, H.; Talluri, S. Supply chain risk management: A literature review. *Int. J. Prod. Res.* **1997**, *53*, 62–67. [CrossRef]
10. Turnbull, B. Cyber-resilient supply chains: Mission assurance in the future operating environment. *Aust. Army J.* **2018**, *14*, 41.
11. Keshk, M.; Sitnikova, E.; Moustafa, N.; Hu, J.; Khalil, I. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems. *IEEE Trans. Sustain. Comput.* **2019**. [CrossRef]
12. Marsden, T.; Moustafa, N.; Sitnikova, E.; Creech, G. Probability risk identification based intrusion detection system for SCADA systems. In *International Conference on Mobile Networks and Management*; Springer: Berlin/Heidelberg, Germany 2017; pp. 353–363.
13. Martin, C.; Towill, D.R. Supply chain migration from lean and functional to agile and customised. *Supply Chain Manag. Int. J.* **2000**, *5*, 206–213. [CrossRef]

14. Boyson, S. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation* **2014**, *34*, 342–353. [CrossRef]
15. Xiao, Q.; Boulet, C.; Gibbons, T. RFID security issues in military supply chains. In Proceedings of the Second International Conference on Availability, Reliability and Security (ARES'07), Vienna, Austria, 10–13 April 2007; pp. 599–605.
16. Hendricks, K.B.; Singhal, V.R. Association Between Supply Chain Glitches and Operating Performance. *Manag. Sci.* **2005**, *51*, 695–711. [CrossRef]
17. Liya, J.; Tiening, W.; Ronghui, W. Risk evaluation of military supply chains based on case and fuzzy reasoning. In Proceedings of the 2010 International Conference on Logistics Systems and Intelligent Management (ICLSIM), Harbin, China, 9–10 January 2010; Volume 1, pp. 102–104.
18. Mei, M.M.; Andry, J.F. The Alignment of Business Process in Event Organizer and Enterprise Architecture Using TOGAF. *JUTI J. Ilm. Teknol. Inf.* **2019**, *17*, 21–29. [CrossRef]
19. Zarour, K.; Benmerzoug, D.; Guermouche, N.; Drira, K. A BPMN extension for business process outsourcing to the cloud. In *World Conference on Information Systems and Technologies*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 833–843.
20. Leon Rangel, A. Extending the BPMN Model for IOT Design. Ph.D. Thesis, Auckland University of Technology, Auckland, New Zealand, 2020.
21. Scrapper, C.; Droge, G.N.; Xydes, A.L.; de la Croix, J.P.; Rahmani, A.; Vander Hook, J.; Lim, G. Mission Modeling Planning, and Execution Module (M2PEM) Systems and Methods. US Patent Appl. 16/403,838, 7 November 2019.
22. Kumar, V.R.S.; Khamis, A.; Fiorini, S.; Carbonera, J.L.; Alarcos, A.O.; Habib, M.; Goncalves, P.; Li, H.; Olszewska, J.I. Ontologies for industry 4.0. *Knowl. Eng. Rev.* **2019**, *34*, e17. [CrossRef]
23. Waters, G.; Blackburn, A.J. *Australian Defence Logistics: The Need to Enable and Equip Logistics Transformation*; Kokoda Foundation Limited Publisher, Number. 19: Balmain, Australia, 2014.
24. Wang, F.; Ge, B.; Zhang, L.; Chen, Y.; Xin, Y.; Li, X. A system framework of security management in enterprise systems. *Syst. Res. Behav. Sci.* **2013**, *30*, 287–299. [CrossRef]
25. Flauzac, O.; González, C.; Hachani, A.; Nolot, F. SDN based architecture for IoT and improvement of the security. In Proceedings of the 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangiu, Korea, 24–27 March 2015; pp. 688–693.
26. Poudel, S. Internet of things: Underlying technologies, interoperability, and threats to privacy and security. *Berkeley Tech. LJ* **2016**, *31*, 997.
27. Seliem, M.; Elgazzar, K.; Khalil, K. Towards Privacy Preserving IoT Environments: A Survey. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1032761. [CrossRef]
28. Shon, T.; Cho, J.; Han, K.; Choi, H. Toward Advanced Mobile Cloud Computing for the Internet of Things: Current Issues and Future Direction. *Mob. Netw. Appl.* **2014**, *19*, 404–413. [CrossRef]
29. Pathan, A.S.K.; Lee, H.W.; Hong, C.S. Security in wireless sensor networks: Issues and challenges. In Proceedings of the 2006 8th International Conference Advanced Communication Technology, Phoenix Park, Korea, 20–22 February 2006; Volume 2, pp. 6–1048.
30. Aazam, M.; Huh, E.N. Fog computing and smart gateway based communication for cloud of things. In Proceedings of the 2014 International Conference on Future Internet of Things and Cloud, Barcelona, Spain, 27–29 August 2014; pp. 464–470.
31. Singh, J.; Pasquier, T.; Bacon, J.; Ko, H.; Eyers, D. Twenty Security Considerations for Cloud-Supported Internet of Things. *IEEE Internet Things J.* **2016**, *3*, 269–284. [CrossRef]
32. Mendes, R.; Vilela, J.P. Privacy-Preserving Data Mining: Methods, Metrics, and Applications. *IEEE Access* **2017**, *5*, 10562–10582. [CrossRef]
33. Saleh, M.; Khatib, I. Throughput analysis of WEP security in ad hoc sensor networks. In Proceedings of the Second International Conference on Innovations in Information Technology (IIT'05), Dubai, UAE, 26–28 September 2005; pp. 26–28.
34. Awasthi, A.; Grzybowska, K. Barriers of the supply chain integration process. In *Logistics Operations, Supply Chain Management and Sustainability*; Springer: Cham, Switzerland, 2014; pp. 15–30.
35. Chourabi, H. Understanding smart cities: An integrative framework. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2012; pp. 2289–2297.

36. Mcfadden, F.E.; Arnold, R.D. Supply chain risk mitigation for IT electronics. In Proceedings of the 2010 IEEE International Conference on Technologies for Homeland Security HST, Waltham, MA, USA, 8–10 November 2010; pp. 49–55.
37. Metcalfe, B. Metcalfe's law after 40 years of ethernet. *Computer* **2013**, *46*, 26–31. [CrossRef]
38. Ali, A.; Mahfouz, A.; Arisha, A. Analysing supply chain resilience: Integrating the constructs in a concept mapping framework via a systematic literature review. *Supply Chain Manag. Int. J.* **2017**, *22*, 16–39. [CrossRef]
39. Gunter, C.A. Open APIs for embedded security. In Proceedings of the European Conference on Object-Oriented Programming, Darmstadt, Germany, 21–25 July 2003; pp. 225–247.
40. Chen, P.; Desmet, L.; Huygens, C. A study on advanced persistent threats. In Proceedings of the IFIP International Conference on Communications and Multimedia Security, Aveiro, Portugal, 25–26 September 2014; pp. 63–72.
41. Choo, K.K.R. The cyber threat landscape: Challenges and future research directions. *Comput. Secur.* **2011**, *30*, 719–731. [CrossRef]
42. Molnar, D.; Wagner, D. Privacy and security in library RFID: Issues, practices, and architectures. In Proceedings of the 11th ACM conference on Computer and Communications Security, Washington, DC, USA, 25–29 October 2004; pp. 210–219.
43. Byres, E.; Lowe, J. The myths and facts behind cyber security risks for industrial control systems. *Proc. VDE Kongr.* **2004**, *116*, 213–218.
44. Vukalović, J.; Delija, D. Advanced Persistent Threats-detection and defense. In Proceedings of the 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 25–29 May 2015; pp. 1324–1330.
45. O'hara, G. Cyber-Espionage: A growing threat to the American economy. *CommLaw Conspec.* **2010**, *19*, 241.
46. Mohurle, S.; Patil, M. A brief study of wannacry threat: Ransomware attack 2017. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*. [CrossRef]
47. Markowski, A.S.; Mannan, M.S. Fuzzy risk matrix. *J. Hazard. Mater.* **2008**, *159*, 152–157. [CrossRef]
48. Pettit, T.J.; Fiksel, J.; Croxton, K.L. Ensuring supply chain resilience: development of a conceptual framework. *J. Bus. Logist.* **2010**, *31*, 1–21. [CrossRef]
49. Toma, S.G. What is Six Sigma? *Manag. J.* **2008**, *8*, 152–155.
50. Chappell, A.; Peck, H. Risk management in military supply chains: Is there a role for six sigma? *Int. J. Logist. Res. Appl.* **2006**, *9*, 253–267. [CrossRef]
51. Hahn, A.; Thomas, R.K.; Lozano, I.; Cardenas, A. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *11*, 39–50. [CrossRef]
52. Zhong, B.; Li, Y. An ontological and semantic approach for the construction risk inferring and application. *J. Intell. Robot. Syst.* **2015**, *79*, 449–463. [CrossRef]
53. Coletti, A.; De Nicola, A.; Vicoli, G.; Villani, M.L. Semantic Modeling of Cascading Risks in Interoperable Socio-technical Systems. In *Enterprise Interoperability VIII*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 119–129.
54. Lamine, E.; Thabet, R.; Sienou, A.; Bork, D.; Fontanili, F.; Pingaud, H. BPRIM: An integrated framework for business process management and risk management. *Comput. Ind.* **2020**, *117*, 103199. [CrossRef]
55. Maksimović, M.; Vujović, V.; Davidović, N.; Milošević, V.; Perišić, B. Raspberry Pi as Internet of things hardware: Performances and constraints. *Des. Issues* **2014**, *3*, 6.
56. Li, Q.C.; Niu, H.; Papathanassiou, A.T.; Wu, G. 5G Network Capacity: Key Elements and Technologies. *IEEE Veh. Technol. Mag.* **2014**, *9*, 71–78. [CrossRef]
57. Jakobs, K.; Pils, C.; Wallbaum, M. Using the Internet in transport logistics-The example of a track & trace system. In Proceedings of the International Conference on Networking, Colmar, France, 9–13 July 2001; pp. 194–203.
58. He, W.; Tan, E.L.; Lee, E.W.; Li, T. A solution for integrated track and trace in supply chain based on RFID & GPS. In Proceedings of the 2009 IEEE Conference on Emerging Technologies & Factory Automation, Bangalore, India, 22–25 September 2009; pp. 1–6.
59. Juels, A. RFID security and privacy: A research survey. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 381–394. [CrossRef]

60. Goyal, S.; Mezzavilla, M.; Rangan, S.; Panwar, S.; Zorzi, M. User association in 5G mmWave networks. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017; pp. 1–6.
61. Baldini, G.; Oliveri, F.; Braun, M.; Seuschek, H.; Hess, E. Securing disaster supply chains with cryptography enhanced RFID. *Disaster Prev. Manag. Int. J.* **2012**, *21*, 51–70. [CrossRef]
62. Hong, C.H.; Varghese, B. Resource management in fog/edge computing: A survey on architectures, infrastructure, and algorithms. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–37. [CrossRef]
63. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; et al. A view of cloud computing. *Commun. ACM* **2010**, *53*, 50–58. [CrossRef]
64. Al-Khafajiy, M.; Baker, T.; Hussien, A.; Cotgrave, A. UAV and Fog Computing for IoE-Based Systems: A Case Study on Environment Disasters Prediction and Recovery Plans. In *Unmanned Aerial Vehicles in Smart Cities*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 133–152.
65. Kunal, S.; Saha, A.; Amin, R. An overview of cloud-fog computing: Architectures, applications with security challenges. *Secur. Priv.* **2019**, *2*, e72. [CrossRef]
66. Elzamly, A.; Messabia, N.; Doheir, M.; Abu Naser, S.; Elbaz, H.A. Critical Cloud Computing Risks for Banking Organizations: Issues and Challenges. *Religación. Rev. De Cienc. Soc. Y Humanidades* **2019**, *4*, 673–682.
67. Sha, K.; Yang, T.A.; Wei, W.; Davari, S. A survey of edge computing-based designs for iot security. *Digit. Commun. Netw.* **2020**, *6*, 195–202. [CrossRef]
68. Ni, J.; Zhang, K.; Lin, X.; Shen, X.S. Securing fog computing for internet of things applications: Challenges and solutions. *IEEE Commun. Surv. Tutorials* **2017**, *20*, 601–628. [CrossRef]
69. O'donovan, P.; Gallagher, C.; Bruton, K.; O'Sullivan, D.T. A fog computing industrial cyber-physical system for embedded low-latency machine learning Industry 4.0 applications. *Manuf. Lett.* **2018**, *15*, 139–142. [CrossRef]
70. Al-khafajiy, M.; Baker, T.; Asim, M.; Guo, Z.; Ranjan, R.; Longo, A.; Puthal, D.; Taylor, M. COMITMENT: A Fog Computing Trust Management Approach. *J. Parallel Distrib. Comput.* **2020**, *137*, 1–16. [CrossRef]
71. Tariq, M.I. Agent Based Information Security Framework for Hybrid Cloud Computing. *KSII Trans. Internet Inf. Syst.* **2019**, *13*. [CrossRef]
72. Ashton, K. That 'internet of things' thing. *RFID J.* **2009**, *22*, 97–114.
73. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]
74. Stock, T.; Seliger, G. Opportunities of Sustainable Manufacturing in Industry 4.0. *Procedia CIRP* **2016**, *40*, 536–541. [CrossRef]
75. Borgia, E. The Internet of Things vision: Key features, applications and open issues. *Comput. Commun.* **2014**, *54*, 1–31. [CrossRef]
76. Chhetri, S.R.; Rashid, N.; Faezi, S.; Faruque, M.A. Security trends and advances in manufacturing systems in the era of industry 4.0. In Proceedings of the 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Santa Clara, CA, USA, 13–16 November 2017; pp. 1039–1046.
77. Tortonesi, M. Leveraging Internet of Things within the military network environment-Challenges and solutions. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 111–116.
78. Hemanidhi, A.; Chimmanee, S.; Kimpan, C. Cyber risk evaluation framework based on risk environment of military operation. In Proceedings of the 2015 Asian Conference on Defence Technology (ACDT), Hua Hin, Thailand, 23–25 April 2015; pp. 42–47.
79. Lanka, D.; Veenadhari, C.L.; Suryanarayana, D. Application of fog computing in military operations. *Int. J. Comput. Appl.* **2017**, *164*, 10–15. [CrossRef]
80. Mishra, S.; Jain, S. Ontologies as a semantic model in IoT. *Int. J. Comput. Appl.* **2020**, *42*, 233–243. [CrossRef]
81. Zeltmann, S.E.; Gupta, N.; Tsoutsos, N.G.; Maniatakos, M.; Rajendran, J.; Karri, R. Manufacturing and Security Challenges in 3D Printing. *JOM* **2016**, *68*, 1872–1881. [CrossRef]
82. Abdel-Basset, M.; Manogaran, G.; Mohamed, M. Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems. *Future Gener. Comput. Syst.* **2018**, *86*, 614–628. [CrossRef]
83. Singh, R.K.; Acharya, P. Identification and Evaluation of Supply Chain Flexibilities in Indian FMCG Sector Using DEMATEL. *Glob. J. Flex. Syst. Manag.* **2014**, *15*, 91–100. [CrossRef]

84. Baheti, R.; Gill, H. Cyber-physical systems. *Impact Control Technol.* **2011**, *12*, 161–166.
85. Fernandes, R.; Benjamin, P.; Li, B.; Stephenson, A.; Patel, M.; Hwang, J. Use of Topological Vulnerability Analysis for Cyberphysical Systems. In Proceedings of the NAECON 2018—IEEE National Aerospace and Electronics Conference, Dayton, OH, USA, 23–26 July 2018; pp. 78–81. [CrossRef]
86. Frazzon, E.M.; Silva, L.S.; Hurtado, P.A. Synchronizing and Improving Supply Chains through the application of Cyber- Physical Systems. *IFAC-PapersOnLine* **2015**, *48*, 2059–2064. [CrossRef]
87. Lee, K.E.; Lee, E.J.; Park, H.S. Using Markov chains of nucleotide sequences as a possible precursor to predict functional roles of human genome: A case study on inactive chromatin regions. *Genet. Mol. Res.* **2016**, *15*, 4837–4869. [CrossRef]
88. Babu, B.; Ijyas, T.; Muneer, P.; Varghese, J. Security issues in SCADA based industrial control systems. In Proceedings of the 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 26–27 March 2017; pp. 47–51.
89. Fitz, T.; Theiler, M.; Smarsly, K. A metamodel for cyber-physical systems. *Adv. Eng. Inform.* **2019**, *41*, 100930. [CrossRef]
90. Shi, L.; Dai, Q.; Ni, Y. Cyber–physical interactions in power systems: A review of models, methods, and applications. *Electr. Power Syst. Res.* **2018**, *163*, 396–412. [CrossRef]
91. Kshetri, N. Can blockchain strengthen the internet of things? *IT Prof.* **2017**, *19*, 68–72. [CrossRef]
92. Park, J.; Park, J. Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry* **2017**, *9*, 164. [CrossRef]
93. Fernández-Caramés, T.; Blanco-Novoa, O.; Suárez-Albela, M.; Fraga-Lamas, P. A UAV and Blockchain-Based System for Industry 4.0 Inventory and Traceability Applications. *Proceedings* **2018**, *4*, 26. [CrossRef]
94. Pisa, M.; Juden, M. Blockchain and economic development: Hype vs. reality. *Cent. Glob. Dev. Policy Pap.* **2017**, *107*, 150.
95. Alkadi, O.; Moustafa, N.; Turnbull, B. A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions. *IEEE Access* **2020**. [CrossRef]
96. Mikroyannidis, A.; Third, A.; Domingue, J.; Bachler, M.; Quick, K.A. Blockchain Applications in Lifelong Learning and the Role of the Semantic Blockchain. In *Blockchain Technology Applications in Education*; IGI Global: Hershey, PA, USA, 2020; pp. 16–41.
97. Li, Y.; Marier-Bienvenue, T.; Perron-Brault, A.; Wang, X.; Paré, G. Blockchain technology in business organizations: A scoping review. In Proceedings of the 51st Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 3–6 January 2018.
98. Lo, S.K.; Xu, X.; Chiam, Y.K.; Lu, Q. Evaluating suitability of applying blockchain. In Proceedings of the 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS), Fukuoka, Japan, 6–8 November 2017; pp. 158–161.
99. Zīle, K.; Strazdiņa, R. Blockchain Use Cases and Their Feasibility. *Appl. Comput. Syst.* **2018**, *23*, 12–20. [CrossRef]
100. Alkadi, O.; Moustafa, N.; Turnbull, B.; Choo, K.K.R. A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks. *IEEE Internet Things J.* **2020**. [CrossRef]
101. Kim, H.M.; Laskowski, M. Toward an ontology-driven blockchain design for supply-chain provenance. *Intell. Syst. Account. Financ. Manag.* **2018**, *25*, 18–27. [CrossRef]
102. Keshk, M.; Turnbull, B.; Moustafa, N.; Vatsalan, D.; Choo, K.K.R. A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks. *IEEE Trans. Ind. Inform.* **2019**, *16*, 5110–5118. [CrossRef]
103. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data, Boston, MA, USA, 11–14 December 2017; pp. 557–564.
104. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
105. Atzei, N.; Bartoletti, M.; Cimoli, T. A survey of attacks on ethereum smart contracts (sok). In Proceedings of the International Conference on Principles of Security and Trust, Uppsala, Sweden, 22–29 April 2017; pp. 164–186.

106. Ron, D.; Shamir, A. Quantitative analysis of the full bitcoin transaction graph. In Proceedings of the International Conference on Financial Cryptography and Data Security, Okinawa, Japan, 1–5 April 2013; pp. 6–24.
107. Luu, L.; Chu, D.H.; Olickel, H.; Saxena, P.; Hobor, A. Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 254–269.
108. Mik, E. Smart contracts: Terminology, technical limitations and real world complexity. *Law Innov. Technol.* **2017**, *9*, 269–300. [CrossRef]
109. Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777.
110. Tecuci, G. Artificial intelligence. *Wiley Interdiscip. Rev. Comput. Stat.* **2012**, *4*, 168–180. [CrossRef]
111. Ardalani-Farsa, M.; Zolfaghari, S. Residual analysis and combination of embedding theorem and artificial intelligence in chaotic time series forecasting. *Appl. Artif. Intell.* **2011**, *25*, 45–73. [CrossRef]
112. Moustafa, N.; Misra, G.; Slay, J. Generalized outlier gaussian mixture technique based on automated association features for simulating and detecting web application attacks. *IEEE Trans. Sustain. Comput.* **2018**. [CrossRef]
113. Moustaf, N.; Slay, J. Creating novel features to anomaly network detection using DARPA-2009 data set. In Proceedings of the 14th European Conference on Cyber Warfare and Security, Academic Conferences Limited, Reading, UK, 1 July 2015; pp. 204–212.
114. Liu, F.; Yang, M. Verification and validation of artificial neural network models. In Proceedings of the Australasian Joint Conference on Artificial Intelligence, Sydney, Australia, 5–9 December 2005; pp. 1041–1046.
115. Lee, J.D.; See, K.A. Trust in automation: Designing for appropriate reliance. *Hum. Factors* **2004**, *46*, 50–80. [CrossRef]
116. Fox, M.S.; Barbuceanu, M.; Teigen, R. Agent-oriented supply-chain management. *Int. J. Flex. Manuf. Syst.* **2000**, *12*, 165–188. [CrossRef]
117. Piramuthu, S. Machine learning for dynamic multi-product supply chain formation. *Expert Syst. Appl.* **2005**, *29*, 985–990. [CrossRef]
118. Beydoun, G.; Low, G.; Bogg, P. Suitability assessment framework of agent-based software architectures. *Inf. Softw. Technol.* **2013**, *55*, 673–689. [CrossRef]
119. Buckland, M.K.; Florian, D. Expertise, task complexity, and artificial intelligence: A conceptual framework. *J. Am. Soc. Inf. Sci.* **1991**, *42*, 635–643. [CrossRef]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.