Assessment of Cyber Security Implications of New Technology Integrations into Military Supply Chains

Theresa May Sobb
School of Engineering and
Information Technology
University of New South Wales
Australian Capital Territory,
Australia
ORCID: 0000-0001-9373-2179

Benjamin Turnbull
UNSW Canberra Cyber
University of New South Wales
Australian Capital Territory,
Australia
ORCID: 0000-0003-0440-5032

Abstract— **Military supply chains play a critical role in the acquisition and movement of goods for defence purposes. The disruption of these supply chain processes can have potentially devastating affects to the operational capability of military forces. The introduction and integration of new technologies into defence supply chains can serve to increase their effectiveness. However, the benefits posed by these technologies may be outweighed by significant consequences to the cyber security of the entire defence supply chain. Supply chains are complex Systems of Systems, and the introduction of an insecure technology into such a complex ecosystem may induce cascading system-wide failure, and have catastrophic consequences to military mission assurance. Subsequently, there is a need for an evaluative process to determine the extent to which a new technology will affect the cyber security of military supply chains. This work proposes a new model, the Military Supply Chain Cyber Implications Model (M-SCCIM), that serves to aid military decision makers in understanding the potential cyber security impact of introducing new technologies to supply chains. M-SCCIM is a multiphase model that enables understanding of cyber security and supply chain implications through the lenses of theoretical examinations, pilot applications and system wide implementations.**

Keywords—supply chain, cyber-security, framework, military, cyber, Systems-of-systems

I. Introduction

The cyberspace landscape is constantly evolving, with developments and exploits being revealed on a regular basis. Systems are increasingly complex and interconnected, resulting in new risks in integration, management and potentially exposing new vulnerabilities to critical infrastructure [1, 2]. Cyber-attacks are increasing in number and complexity each year and impacting individuals, businesses and governments [3]. Risk assessments are heavily relied upon to understand the threats posed by technological integration; however, they do not constitute a holistic solution to understanding the range of consequences caused by the introduction of a new technology into unencapsulated military supply chains.

Supply chains are a fundamental component of business and defence processes that serve as a key enabler for the management of resources and the linking of materials from sources, to transformers, to users [4]. Within a military context, the management of supply chains can have significant tactical, operational or strategic consequences; and therefore, their security needs to be of the upmost importance to defence organisations. Defence supply chains are abstract, complex Systems of Systems that serve to support critical military objectives and capabilities. Subsequently, vulnerabilities in military supply chains can have consequences that can both affect national security and threaten human lives.

This paper addresses the need for a generic model that is technology agnostic, can be used as a framework for whatever new technologies are under consideration, and serves to augment risk assessment and cyber security processes. This model is not designed to solve all issues associated with integrating new technologies into supply chains, but to outline considerations and processes. It introduces the Military Supply Chain Cyber Implications Model, a process model for identifying risks and considerations for integrating new technologies into military supply chains, from a cyber-security perspective.

The remainder of this paper is structured as follows; Section 2 provides an overview of background and related work as pertinent to this research, incorporating an overview of military supply chains, their considerations and requirements, existing frameworks that are related to this research, and an overview of emerging technologies that are in the process of integration into military supply chains. Section 3 introduces the Military Supply Chain Cyber Implications Model (M-SCCIM), a framework for assisting with understanding the systemic cyber-security concerns when integrating new technologies into military supply chains. Section 4 analyses the current state, the future work and next phases of work for this model and concludes this paper.

II. Background and Related Work

A. Supply Chains

Supply chains are a fundamental component of business and organisational processes, serving to enable the

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

DOI 10.1109/SPW50608.2020.00038

management of resources and the linking of materials from sources, to transformers, to users [4]. Specifically, supply chains refer to "the network of organisations that are involved, through upstream and downstream linkages, in the different processes and activities that produce value in the form of products and services delivered to the ultimate consumer" [5]. Supply chains are inherently abstract; they exist as part of complex systems containing blurred boundaries, where every subsystem is unique. However, the aims of supply chains can generally be described as one of three phases; procurement, production and distribution [6]. Supply chains and logistics are not synonymous, as the supply chain considers logistical "point-of-origin to point-of-consumption" as only part of its integration of "all key business operation[s]" [4].

Effective supply chain management involves the organisation of network and business connections and relationships across all stages of the chain [4]. Complexity within supply chains brings forth issues of uncertainty that propagate throughout the entire network, potentially disrupting business operations [7].

It is the authors assertions that supply chains are considered Systems-of-Systems (SoS), as opposed to complicated systems, as they are dependent on many varied factors that are unable to be effectively modelled or defined [8]. This includes personal relationships, business relationships, the use of multiple levels of subcontracting, weather, international logistics and other external factors that may cause delays or changes to the supply and movement of goods.

Globalisation enables the accruement and delivery of product components from multiple organisations concurrently on an international scale, involving businesses such as primary producers, manufacturers and transport companies. This trend is evident in the supply chains for both commercial business and government departments, providing them with a competitive advantage over other organisations that cannot access global resources [9].

The interconnection of systems within military supply chains brings forth potential vulnerabilities. 'Cascading failure' within flows of service infrastructure can occur when a failure in one element of an interconnected, interdependent series of systems invokes a domino effect of further failures within the larger complex system [10]. [11] defines the idea of 'ecosystem accidents'; which involves the "interaction of systems that were thought to be independent but are not because of the larger ecology"; as critical to understanding how the nature of system complexity can influence their effective operation.

B. The Unique Nature of Military Supply Chains

Military supply chains are unique from civilian supply chains and operate with a distinct end-state to consider. The outcomes resulting through a supply chain 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, products delivered through defence supply chains can influence the tactical and operational capability of a force. Subsequently, the management and operation of military supply chains can have direct impacts to human life. Military supply chain requirements include readiness for war, supply chain flexibility, item diversity and unstable demands; which demonstrate a divergence from standard civilian outcomes. Subsequently, attacks on military supply chains often target these unique requirements in order to have a measurable effect on armed force operations.

Unlike many commercial supply chains, military supply chains are less focused on profit maximisation and more focused on security, which can bring forth conflicts of interests in joint civilian and defence ventures [12]. Within a defence environment, the management of separate capability platforms; such as ships or aeroplanes; cannot be considered independent, as they are inherently interconnected through other systems within the military ecology, such as resupply systems, finance and operational readiness. Considering these ideas and the complexity of supply chains, there is thus an inherent risk that the interdependence of multiple capabilities and systems within the ecology of a military can also bring forth cyber security challenges.

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 own supply chain; which can pose a threat within operational contexts [13, 14] .

There is often a misalignment of goals between military supply chains and commercial supply chains; being operational outcomes and profit respectively [15]. Thus, this disconnect between defence organisations and their contractors and outsourcers can provide further opportunities for vulnerability. As aforementioned, the consequences of a security breach within a military context can have significant consequences to 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 Defence Force cyber security breach in 2016, in which attackers achieved their objectives by targeting a third-party contractor [16, 17].

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 remodelled into their final form [18]. The globalised economy and transnational supply chains mean that even the simplest of products can have components from different countries and vendors. Even the F-35 Strike Fighter aircraft, utilised by countries including the United Kingdom, the United States of America, and Australia; contains parts manufactured in multiple countries [19, 20]. In this case, security concerns about potential compromise of the aircraft through these supplier components have been repeatedly raised; highlighted by speculations that "weapon system[s] may become dependent on parts made by a potential future adversary" [19, 20]. However these apprehensions have been met with assurances from Britain's Ministry of Defence who stated that the F-35's supply chain contains "no risk" [19, 20]. This debate highlights uncertainty within the community in relation to the upkeep of supply chain integrity, particularly of classified military systems.

C. *The Cyber Security of Supply Chains*

Attack vectors experiencing growth in the cyber domain include social engineering and spear phishing, exploitation of underlying libraries and protocols malicious advertising and distributed denial of service [21]. Through secondary targeting, an attacker may compromise a military system through one of their partners within the supply chain who has a less developed and hardened network security.

Potential techniques to mitigate the threats posed by system integration within complex supply chain systems includes the implementation of Enterprise Architecture (EA) approaches [22]. 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.

Ultimately, 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.

D. *Related Frameworks and Processes*

There exist several fields of study that are relevant to portions of this work; risk analysis, cyber security attack frameworks and other management models. However, there is an unaddressed research opportunity at the intersection of supply chain management, new technology integration, cybersecurity, and military and defence systems.

Risk analysis frameworks serve to aid organisations in determining their potential vulnerabilities and assess how those vulnerabilities may affect the organisation and its systems. Cyber Supply Chain Risk Management (CSCRM) is defined as "the organisational 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" [23].

Risk matrixes can also be used to evaluate the status of potential risks and their impacts within a system [24]. In traditional risk assessment matrixes, severity and frequency are used to categorise risks, and fuzzy logic can be used to extend the possibilities beyond set classifications [24]. While risk matrixes may form part of an assessment on how a technology may affect the defence supply chain, there are still non-risk related factors that need to be considered.

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 [25]. This has been implemented into the United States Navy and Airforce since 2009; however it lacks a supply chain specific focus.

The Six Sigma DMAIC model involves defining objectives of improvement to a process, then measuring, analysing, improving and finally controlling the process [26]. In a 2006 analysis of the suitability of applying the Six Sigma methodology to the UK defence supply chain, it was determined that while the methodology could be utilised, there were limiting factors that reduced the likelihood of its implementation, including stock holding policies and activity levels [27].

The Lockheed Martin Cyber Kill Chain is a phase-based method that defines the different stages of a cyberspace-based attack [28]. Each level of the Cyber Kill Chain can be used to understand how a new technology may introduce vulnerabilities to the military supply chain in which it is being implemented, although it is not intended to understand considerations of implementing systems, but to forensically understand adversarial attacks and to provide minimisation of attack surface.

The Supply-Chain Operations Reference model (SCOR) is a "cross-industry framework for evaluating and improving enterprise-wide supply-chain performance and management" [29]. SCOR uses standard descriptions of process elements, benchmarking metrics, management practises and software product mapping in order to "communicate, compare and develop new or improved supply-chain practises" [29]. Additionally, one of the model's critical success factors relies on the idea that a "company's operations strategy must be consistent with and support the business strategy", which may not be applicable to all militaries, where their overall strategies do not have business or consumer driven outcomes [29].

E. *Emerging Technologies*

There is a need for a technologically agnostic framework that incorporates considerations from any new technology. That said, there is a number of new technologies currently being researched, considered and actively implemented in supply chains globally. This work discusses two of these, noting that there are others; smart contracts, and the Internet of Things. Each of these is briefly introduced.

Smart contracts refer to "pieces of software that represent a business arrangement and execute themselves automatically under pre-determined circumstances" [30, 31]. In implementation, smart contracts are developed on blockchain technologies, and enable programmability and customisation of transaction criteria [32]. As smart contracts are employed as programs for blockchain, they share some benefit from blockchain's key features including decentralization, persistency, anonymity and auditability. Smart contracts can be applied to a wide range of scenarios, ranging from smart property, e-voting, financial payments, insurance and identity management [33]. 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 quality and integrity of the chain, and finally monitor the status of items within the chain.

Some of the problems experienced by smart contracts come from misunderstandings of contract semantics and the relationships between contracts and other network participants [34]. 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 [34]. Failure to mitigate against these issues may invoke significant financial loss or compromise of information. Additional security risks have been identified within the sphere of smart contracts based on the implementation, such as lack of permissions on the Ethereum network.

Internet of Things (IoT) integration is a growing trend within commercial supply chains and can be expected to enter into military supply chains also. Therefore, the vulnerabilities present within IoT devices have the potential to compromise defence 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 minimisation [35]. 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[36].

III. The Military Supply Chain Cyber Implication Model

After extensive consideration of the current literature regarding existing models for assessing the impact of technologies to defence supply chains, and the nature of military supply chains in general, the Military Supply Chain Cyber Implication Model (M-SCCIM) has been created. M-SCCIM serves to delineate the key considerations for assessing how a new technology will impact a military supply chain. It is outlined in Figure 1.

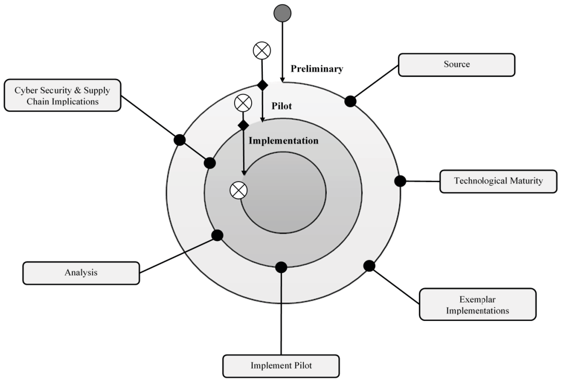

Fig. 1. Figure 1 – Military Supply Chain Cyber Implications Model (M-SCCIM)

M-SCCIM is a conceptual model, which is designed to aid decision makers in understanding the cyber security implications of a new technology being introduced into a defence supply chain. Thus, this model has not been implemented in a decision support system scenario.

The model consists of three phases, with corresponding considerations for each phase. These phases are the Preliminary Phase, the Pilot Phase, and the Implementation Phase. Each of these is discussed separately.

A. The Preliminary Phase

The first phase of the M-SCCIM is the Preliminary Phase, which involves considering source*,* technological maturity*,* exemplar implementations*,* and cyber security and supply chain implications. At the completion of the Preliminary Phase, a decision must be made as to whether a pilot implementation is worth exploring, or if the investigation should cease due to the nature of the considerations identified.

Considerations of source relate to identifying where the technology's boundary of reach stems and the level of control that the affected military party has over that technological change. Boundary of reach incurs the consideration of how far the proposed technology will permeate throughout the supply chain system. An internal source involves the introduction of the technology within the boundaries of the military subsystem of the overall supply chain. The level of control consideration involves identifying to what degree the affected military party has influence or authority over the technology and its implementation. This hinges on the internal or external source identification and comprises of assessing where these control measures may lie.

The consideration of technological maturity aims to understand the current status of the technology within its development. This involves examining four factors; community, patches and versions, stability, and hype cycles, such as those used by Gartner [37]. Community refers to the existence of an active group of users of the technology, often within an online sphere. The consideration of patches and versions relates to assessing how often and to what extent that the technology is updated. These actions are important, because they serve to minimise the threats posed by outdated software and the vulnerabilities it contains. While updates and new version releases can aid in mitigating against cyber threats, too many iterations of these cycles suggests a lack of technological steadiness. This is assessed in the stability component of technological maturity. Stability involves assessing how well-tested and complete different versions and updates to a system or technology are. The hype cycle "characterizes the typical progression of an *emerging technology…"* [38]. It provides a guide to how a technology will evolve and develop throughout its life, which is critical to assessing its impact within an organisation [37]. Consideration of the hype cycle is important because the capabilities of new technologies can sometimes be overstated due to excitement about their development.

As part of the Preliminary Phase of M-SCCIM, exemplar implementations of the technology in focus must be considered. This involves assessing the existence of implementations, the nature of their implementation environments, and the learning opportunities drawn from those implementations. Examples can be drawn from any environment for the purpose of analysis. If there are none, then an assessment needs to be made as to the reason why. The environment consideration involves studying the implementation contexts to determine whether there are any similarities or differences between that and the military supply chain environment in question. The benefits of considering exemplar implementations are demonstrated through evaluative case study research. Assessment of case studies applies to multiple disciplines, and can aid in teaching crisis management and highlight gaps in theory [39, 40]. Therefore, examining exemplar implementations provides decision makers with the opportunity to consider the history of technological application, and to take lessons from these scenarios that can be applied to new ones.

Cyber security and supply chain implications of implementing a technology are considered within both the Preliminary Phase and Pilot Phase of M-SCCIM. They involve consideration of both technologically agnostic implications and foundational prerequisite implications.

Technologically agnostic implications focus on examining how the new technology may affect the cyber security of the supply chain system. This includes considerations of legal and policy, security, criticality, agility and maintainability.

The legal and policy implications of implementing the chosen technology are one component of the technologically agnostic assessment. Legal and policy limitations for technologies may stem from multiple sources, including government legislation, administration requirements and organisational information protection requirements [41, 42]. Specific limitations will rely on the nature of the technology, with applicable fields of consideration including data privacy, information exchanges and data accuracy, among others.

The implications of security must also be considered as part of M-SCCIM, with the factors of transparency, privacy, and mechanisms of security being addressed. Transparency refers to the conditions in which data is revealed within the system, such as who can access data and in what circumstances. Transparency, thus, involves considering the opaqueness of data, involving the display of required data at the highest level necessary in consideration of the request context and permissions of each system. Privacy refers to "the control and release of personal data", and the level of privacy within a system can be an outcome of the transparency conditions present [43]. The mechanisms used to achieve security within the system must also be considered, as they serve to minimise inappropriate interaction with the system and its data. Examples of such mechanisms may include firewalls, authentication requirements, network traffic capture and encryption, among others [44].

The criticality consideration involves assessing the components of the system that are crucial to the operation of the system. This encompasses resilience, availability, reliability and dependency. When examining these factors, the following definitions should be taken into account; resilience refers to determining the ability of the system to recover from an incident, availability encompasses how information can be accessed "when and where desired" [Peterson, Brown & Maw, as cited in 45], reliability involves determining the consistent performance of the system, and dependency concerns the relationship between essential components of the system. Assessments of reliability can be made qualitatively, or quantitatively, such as via either the calculation of the mean time between service incidents or the mean time between failures [46]. The agility consideration addresses how the system responds to changes within its environment. It involves assessing the adaptability and flexibility of the technology within its proposed implementation environment. Flexibility refers to the ability of the technology to operate under a range of conditions, while adaptability involves the ability to modify the system as necessary to meet different conditions. Flexibility and adaptability are imperative for military organisations, as changes to mission requirements, adversaries and environmental pressures may force the modification of goods and upgrades to newer products [King and Sivaloganathan, Rajan et al., as cited in 47].

The maintainability consideration involves determining how the technology is managed, supported and improved. The idea of reliability-centred maintenance is currently present in maintenance assessment literature [48, 49]. Maintenance considerations often include cost-effectiveness and accuracy [48]. Maintainability of a system can affect reliability, but the two concepts are not mutually exclusive and therefore maintenance is not considered as an essential component of criticality considerations.

The foundational prerequisites considerations focus on the key requirements of the technology in order for it to function effectively. There are two subcategories to this consideration, being information technology and information processes.

Information technology involves examining the hardware and software involved in the development and implementation of the technology. This can include considering the components of the technology itself, and the linkage requirements for application within a larger existing system. Hardware and software should be considered as implementations of the technology's blueprint.

Information processes involves considering the collection, processing, transmission and storage of data and information within the system. These may have direct follow-on impacts to the information technology considerations. Collection involves identifying how data is obtained and inputted into the system. Processing encompasses the transformation of data. Transmission involves the movement of data, and storage comprises of how and where data is kept. Collection considerations for input may include the source of data, its validation and how it is procedurally obtained. Processing considerations may include potential processing limitations, expected outputs, resource management and the requirements of sub-processes involved. When addressing transmission, elements such as transmitting devices, receivers, destination parameters, channels of communication and interference should all be contemplated. Finally, considerations of storage may include operating system requirements, file system structure, location and ownership of storage devices, and backup procedures.

In the Preliminary Phase of M-SCCIM, the cyber security and supply chain implications are considered from a theoretical perspective. This occurs through utilising all available resources in order to understand the potential implications that the new technology may have to the cyber security of the defence supply chain.

B. The Pilot Phase

In the event that decision makers continue onto the Pilot Phase, a pilot environment to implement the technology is constructed and analysed, followed by consideration of further cyber security and supply chain implications from the pilot's results. At the conclusion of this phase, a decision must be reached regarding whether to continue with a complete implementation of the technology into the defence supply chain or whether the investigation should cease.

The Pilot Phase informs whether the Preliminary Phase assessments were accurate, and whether there are any additional implications of considerations that need to be assessed. Benefits of conducting pilot testing and trials include increased understanding of risks and issues, potential advantages and disadvantages, evaluation of tools and assessment of viability for a potential system-wide implementation [50].

The first component of the Pilot Phase of M-SCCIM involves the implementation of the chosen technology into a pilot environment. The aim of this pilot should be to replicate the intended implementation system as closely as possible in a separated environment. The subsequent components of the Pilot Phase; analysis and cyber security and supply chain implications; cannot be achieved without first the pilot being applied within this test environment.

The analysis component of M-SCCIM occurs only in the Pilot Phase. This phase involves considering the nature of the pilot's implementation, including its outcomes. Thus, the analysis step focuses on the results of the pilot implementation. Considerations may include challenges to implementation, timeline factors, suitability and accuracy of assessments made in the Preliminary Phase.

During the Pilot Phase, the cyber security and supply chain implications of integrating the new technology into the defence supply chain are again considered. In this phase, these assessments are informed by the analysis results, with these results being discussed in terms of their implications. The same implication categories used in the Preliminary Phase may be used in the Pilot Phase in order to organise the nature of implications. This serves to enrich understanding of the technology's implications based on its pilot implementation.

At the conclusion of the Preliminary and Pilot Phases of M-SCCIM, a decision needs to be made regarding whether the technology should continue to be assessed by the model. This involves an evaluation of each previous consideration addressed within the model, and a determination as to whether the technology in question remains suitable for implementation into the defence supply chain. The decision points within M-SCCIM offer two options; either the technology is considered within the model's next phase or the assessment process ends due to the technology's lack of suitability for implementation into the defence supply chain.

C. The Implementation Phase

The last phase, Implementation, involves the application of the technology completely into the supply chain. This serves as the final phase of the model, because any further cyber security implications assessment will be conducted as part of service maintenance and improvement. This is outside the scope of the M-SCCIM, considering that the model focuses on building an initial understanding of how a new technology will affect a defence supply chain *before* it is implemented fully.

IV. Conclusion and Future Work

This work has articulated the need for a model framework to accurately and comprehensively understand the holistic risks of new technology integrations into military supply chains, from a cyber security perspective. It has then proposed a model for review, the M-SCCIM. M-SCCIM is not designed to replace existing risk management approaches, but to augment them with a process specifically designed for the unique characteristics of military supply chains, and the unique aspects of cyber-security. M-SCCIM contains three distinct phases; the Preliminary Phase, Pilot Phase and Implementation Phase; with these each containing considerations or actions. The Preliminary and Pilot Phases serve to increase the information available to decision makers about a technology's cyber security consequences, while the Implementation Phase constitutes the finishing state of the model for a system-wide implementation. Each phase requires a decision at its conclusion to determine whether the technology should be further considered. The structure and contents of M-SCCIM was determined by outcomes of the literature review, observations of systems engineering and project management frameworks, and further cyber security research.

The M-SCCIM is currently being significantly tested and validated with two specific implementations; the first being the integration of smart alarm systems into specific supply chain sites, and the second being the use of smart contracts to organise a subset of logistics movements between collaborators. The outcomes of this will inform potential modifications to the model to ensure all aspects and project risks are captured and clearly articulated.

As global supply chains increase in complexity, and become increasingly technologically integrated at all levels, there is a potential for adversaries to target them in order to achieve combat or operational superiority. Ultimately, M-SCCIM serves to generate understanding as to how a new technology will affect the cyber security of defence supply chains.

References

[1] D. Mikulecky. "The Complexity of Nature." Virginia Commonwealth University.

http://www.people.vcu.edu/~mikuleck/cmpxnat.html (accessed 19 June, 2019).

[2] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, and P. Toivanen, *Three Practical Attacks Against ZigBee Security: Attack Scenario Definitions, Practical Experiments, Countermeasures, and Lessons Learned*. 2014.

[3] K.-K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Computers & Security,* vol. 30, no. 8, pp. 719-731, 2011.

[4] D. M. Lambert, M. C. Cooper, and J. D. Pagh, "Supply chain management: implementation issues and research opportunities," *The international journal of logistics management,* vol. 9, no. 2, pp. 1-20, 1998.

[5] J. T. Mentzer *et al.*, "Defining supply chain management," *Journal of Business logistics,* vol. 22, no. 2, pp. 1-25, 2001.

[6] D. J. Thomas and P. M. Griffin, "Coordinated supply chain management," *European journal of operational research,* vol. 94, no. 1, pp. 1-15, 1996.

[7] T. Davis, "Effective supply chain management," *Sloan management review,* vol. 34, pp. 35-35, 1993.

[8] P. Cilliers, *Complexity and postmodernism: Understanding complex systems*. Routledge, 2002.

[9] J. T. Robert and R. M. Monczka, "Pursuing Competitive Advantage through Integrated Global Sourcing," *The Academy of Management Executive (1993-2005),* vol. 16, no. 2, pp. 66-80, 2002. [Online]. Available: http://www.jstor.org/stable/4165843.

[10] R. G. Little, "Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures," *Journal of Urban Technology,* vol. 9, no. 1, pp. 109-123, 2002.

[11] C. Perrow, *Normal Accidents: Living with High Risk Technologies*. Princeton University Press, 1999.

[12] J. Liya, W. Tiening, and W. Ronghui, "Risk evaluation of military supply chains based on case and fuzzy reasoning," in *2010 International Conference on Logistics Systems and Intelligent Management (ICLSIM)*, 2010, vol. 1: IEEE, pp. 102-104.

[13] N. Bartol, "Information and Communication Technology (ICT) Supply Chain Security – Emerging Solutions," Utilities Telecom Council, PowerPoint Presentation, 2014.

[14] (2005). *Task Force on High Performance Microchip Supply*.

[15] M. Warren and W. Hutchinson, "Cyber attacks against supply chain management systems: a short note," *International Journal of Physical Distribution & Logistics Management,* vol. 30, no. 7/8, pp. 710-716, 2000.

[16] J. Jay, "Hackers make hay as poor security compromises Australia’s defence secrets," in *Teiss*, ed. teiss.co.uk: Teiss, 2017.

[17] L. Martin, "Sloppy password fail exposes military's top secrets," in *Daily Mercury*, ed. dailymercury.com.au: Daily Mercury, 2017.

[18] OECD, "Trade Policy Implications of Global Value Chains," OECD, 2018. [Online]. Available: http://www.oecd.org/trade/topics/global-value-chains-and-trade/

[19] J. Shiffman and A. Shalal-Esa, "Exclusive: U.S. waived laws to keep F-35 on track with China-made parts," in *Reuters*, ed. reuters.com: Reuters, 2014.

[20] Telegraph Reporters, "Chinese-owned company makes parts for British F-35 fighter jets, MoD reveals," in *The Telegraph*, ed. telegraph.co.uk: The Telegraph, 2019.

[21] (2016). *ACSC Threat Report*. [Online] Available: https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

[22] F. Wang, B. Ge, L. Zhang, Y. Chen, Y. Xin, and X. Li, "A system framework of security management in enterprise systems," *Systems Research and Behavioral Science,* vol. 30, no. 3, pp. 287-299, 2013.

[23] S. Boyson, "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems," *Technovation,* vol. 34, no. 7, pp. 342-353, 2014.

[24] A. S. Markowski and M. S. Mannan, "Fuzzy risk matrix," *Journal of hazardous materials,* vol. 159, no. 1, pp. 152-157, 2008.

[25] J. Watters and P. Kertzner, "Crown Jewels Analysis," ed: Mitre Corporation, 2016.

[26] S.-G. Toma, "What is Six Sigma?," *Manager Journal,* vol. 8, no. 1, pp. 152-155, 2008.

[27] A. Chappell and H. Peck, "Risk management in military supply chains: is there a role for Six Sigma?," *International Journal of Logistics Research and Applications,* vol. 9, no. 3, pp. 253-267, 2006.

[28] Lockheed Martin. "Cyber Kill Chain®." https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed.

[29] G. Stewart, "Supply-chain operations reference model (SCOR): the first cross-industry framework for integrated supply-chain management," *Logistics information management,* vol. 10, no. 2, pp. 62-67, 1997.

[30] The Economist Staff, "Not-so-clever contracts," in *The Economist* ed. economist.com: The Economist, 2016.

[31] H. M. Kim and M. Laskowski, "Toward an ontology‐driven blockchain design for supply‐chain provenance," *Intelligent Systems in*

Accounting, Finance and Management, vol. 25, no. 1, pp. 18-27, 2018.

[32] A. M. Antonopoulos and G. Wood, *Mastering ethereum: building smart contracts and dapps*. O'Reilly Media, 2018.

[33] M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," *arXiv preprint arXiv:1710.06372,* 2017.

[34] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016: ACM, pp. 254-269.

[35] !!! INVALID CITATION !!! [34-36].

[36] !!! INVALID CITATION !!! [37-40].

[37] Gartner. "Gartner Hype Cycle." Gartner. https://www.gartner.com/en/research/methodologies/gartner-hype-cycle (accessed 06 August, 2019).

[38] D. E. O'Leary, "Gartner's hype cycle and information system research issues," *International Journal of Accounting Information Systems,* vol. 9, no. 4, pp. 240-252, 2008.

[39] B. Richardson, "Why we need to teach crisis management and to use case studies to do it," *Management Education and Development,* vol. 24, no. 2, pp. 138-148, 1993.

[40] N. Siggelkow, "Persuasion with case studies," *Academy of management journal,* vol. 50, no. 1, pp. 20-24, 2007.

[41] K. W. Smith, "Drone technology: Benefits, risks, and legal considerations," *Seattle J. Envtl. L.,* vol. 5, p. i, 2015.

[42] J. L. Bayuk, J. Healey, P. Rohmeyer, M. H. Sachs, J. Schmidt, and J. Weiss, *Cyber security policy guidebook*. Wiley Online Library, 2012.

[43] C. Landwehr, D. Boneh, J. C. Mitchell, S. M. Bellovin, S. Landau, and M. E. Lesk, "Privacy and cybersecurity: The next 100 years," *Proceedings of the IEEE,* vol. 100, no. Special Centennial Issue, pp. 1659-1673, 2012.

[44] (2017). *Strategies to Mitigate Cyber Security Incident*. [Online] Available: https://www.cyber.gov.au/sites/default/files/2019-03/Mitigation_Strategies_2017.pdf

[45] A. M. Khalfan, "Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors," *International Journal of Information Management,* vol. 24, no. 1, pp. 29-42, 2004.

[46] L. Hunnebeck, *Key element guide ITIL service design*, Second edition. ed. London [England]: London England : TSO, 2012.

[47] A. M. Ross, D. H. Rhodes, and D. E. Hastings, "Defining changeability: Reconciling flexibility, adaptability, scalability, modifiability, and robustness for maintaining system lifecycle value," *Systems Engineering,* vol. 11, no. 3, pp. 246-262, 2008.

[48] G. Niu, B.-S. Yang, and M. Pecht, "Development of an optimized condition-based maintenance system by data fusion and reliability-centered maintenance," *Reliability Engineering & System Safety,* vol. 95, no. 7, pp. 786-796, 2010.

[49] L. Bertling, R. Allan, and R. Eriksson, "A reliability-centered asset maintenance method for assessing the impact of maintenance in power distribution systems," *IEEE Transactions on power systems,* vol. 20, no. 1, pp. 75-82, 2005.

[50] *Tips and Recommendations for Successfully Pilot Testing Your Program*. [Online] Available: https://www.hhs.gov/ash/oah/sites/default/files/pilot-testing-508.pdf