IDENTIFYING AN ACHILLES' HEEL: THE VULNERABILITIES OF THE AUSTRALIAN ARMY'S LOGISTICS INFORMATION SYSTEMS IN CYBERSPACE

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

JULIE PEARCE, MAJOR, AUSTRALIAN ARMY
MMgtStud, The University of New South Wales, Canberra, ACT, 2011
MDefStud, The University of New South Wales, Canberra, ACT, 2005
BSc, The University of New South Wales, Canberra, ACT, 2001

Fort Leavenworth, Kansas
2018

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 15-06-2018	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* AUG 2017 – JUN 2018

4. TITLE AND SUBTITLE Identifying an Achilles' Heel: The Vulnerabilities of the Australian Army's Logistics Information Systems in Cyberspace	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Julie Pearce	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Logistics Information Systems have enabled the Australian Army's supply chains, maintenance, transportation and distribution systems to become lean, responsive and efficient. However, these systems are reliant on a permissive cyberspace environment. Not only are the Australian Army's logistics information systems reliant on cyberspace to support forces in the physical domains but they routinely share information with third-party contractors, civilian and commercial vendors to generate the required effects. These interactions between information systems increase the vulnerability of military logistics information systems operating within cyberspace.

Cyberspace has provided adversaries with a different method of targeting logistics, one that can be achieved by state and non-state actors with relatively low costs. Academic literature identifies opportunities and threats presented by the cyberspace domain but does not articulate the vulnerabilities of Logistics Information Systems operating in cyberspace. There is relatively little academic literature identifying what measures should be taken to protect Logistics Information Systems in cyberspace. Australian Army logistics doctrine focuses almost exclusively on the benefits gained through integrated networks without detailed risk mitigation focused on maintaining the confidentiality, integrity, and access to military Logistics Information Systems while developing resilience and redundancy to mitigate against network compromise.

15. SUBJECT TERMS
Australian Army Logistics, Cyberspace, Logistics, Australian Army

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	125	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Julie A. Pearce

Thesis Title: Identifying An Achilles' Heel: The Vulnerabilities Of The Australian Army's Logistics Information Systems In Cyberspace

Approved by:

____, Thesis Committee Chair
George E. Hodge, M.S.

____, Member
O. Shawn Cupp, Ph.D.

____, Member
Robert C. LaPerez, M.A.

Accepted this 15th day of June 2018 by:

____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

IDENTIFYING AN ACHILLES' HEEL: THE VULNERABILITIES OF THE AUSTRALIAN ARMY'S LOGISTICS INFORMATION SYSTEMS IN CYBERSPACE, by Julie Pearce, 125 pages.

Logistics Information Systems have enabled the Australian Army's supply chains, maintenance, transportation and distribution systems to become lean, responsive and efficient. However, these systems are reliant on a permissive cyberspace environment. Not only are the Australian Army's logistics information systems reliant on cyberspace to support forces in the physical domains but they routinely share information with third-party contractors, civilian and commercial vendors to generate the required effects. These interactions between information systems increase the vulnerability of military logistics information systems operating within cyberspace.

Cyberspace has provided adversaries with a different method of targeting logistics, one that can be achieved by state and non-state actors with relatively low costs. Academic literature identifies opportunities and threats presented by the cyberspace domain but does not articulate the vulnerabilities of Logistics Information Systems operating in cyberspace. There is relatively little academic literature identifying what measures should be taken to protect Logistics Information Systems in cyberspace. Australian Army logistics doctrine focuses almost exclusively on the benefits gained through integrated networks without detailed risk mitigation focused on maintaining the confidentiality, integrity, and access to military Logistics Information Systems while developing resilience and redundancy to mitigate against network compromise.

ACKNOWLEDGMENTS

I would like to acknowledge my MMAS committee for the hours of reading, preparation, and conversations that enabled my successful completion of this thesis. As a logistician, it was a daunting prospect to write about cyberspace. It was my committee that provided me invaluable advice, guidance, and confidence to research and complete this thesis. I would like to additionally thank my Staff Group Advisor and fellow CGSC officers from my Staff Group 4C, who provided me with much-valued support while undertaking this MMAS and CGSOC in general.

To my husband Trent, who followed me halfway around the world, completed more than his fair share of household chores, kept me supplied with coffee and Tim Tams, and had to endure hours of conversation regarding cyber and logistics. I will forever be grateful. To my daughters, Jasmine and Annalise, thank you for the cuddles, kisses, and reassurance that you still love me even when I have to study.

TABLE OF CONTENTS

ACRONYMS

ACSC	Australian Cyber Security Center
ADF	Australian Defence Force
APT	Advanced Persistent Threat
ASD	Australian Signals Directorate
CO	Cyber Operations
CSOC	Cyber Security Operations Center
CERT	Computer Emergency Response Team
DCO	Defensive Cyber Operations
DDoS	Distributed Denial of Service
DoD	Department of Defence/Defense
DODIN	Department of Defense Information Networks
DPN	Defence Protected Network
DSN	Defence Secure Network
IP	Internet Protocol
IWD	Information Warfare Division
LogIS	Logistics Information Systems
OCO	Offensive Cyber Operations
NATO	North Atlantic Treaty Organization
NIPR	Non-secure Internet Protocol Router Network
UN	United Nations
URL	Uniform Resource Locator

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

> The line that connects an army with its base of supplies is the heel of Achilles—its most vital and vulnerable point.
>
> — John S. Mosby, *War Reminiscences*

Introduction

An electronically interconnected world has made logistics systems and supply chains more efficient. The ability to share information quickly and accurately has revolutionized logistics practices in supply, transport, and maintenance. Like most military forces, the Australian Army has leveraged these technological advancements to enhance and streamline its logistics practices. However, the benefits gained through connectivity come with significant risks and vulnerabilities.

Australian Army supply chains and logistics lines of communication are high-value targets, identified as targetable critical vulnerabilities in most non-permissive military operations.[1] Unfortunately, the risks to military logistics operations and associated treatments have focused on kinetic vulnerabilities within the traditional land, sea and air domains; treated through conventional defensive measures. The cyberspace domain of warfare provides adversaries with an alternative. Targeting the strategic and operational logistics systems may enable adversaries to force a culmination point on the battlefield before kinetic activity has even begun.

[1] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Combat Service Support* (Canberra, ACT: Australian Army, 2009), 22, accessed 23 September 2017, https://www.cove.org.au/doctrine/lwd-4-0-combat-service-support/.

Background

Despite the sensationalism and hype that appears to surround the subject area of cyberspace, legitimate threats to Government information systems and networks exist. The Australian Signals Directorate (ASD) responds to cybersecurity incidents on government systems. Between 01 January 2015 and 30 June 2016 ASD responded to 1095[2] incidents considered serious enough to warrant operational responses. Between 01 July 2016 and 30 June 2017 the number was 671[3].

The observation of fewer compromises of Australian government networks does not necessarily represent a reduction in targeting. Adversaries regularly target government networks; however, as government defenses gradually improve, cyber adversaries will look to identify softer targets to gain access to government information networks. These softer targets include Defense contractors and companies involved in the design, manufacture, and maintenance of Defense capabilities. Cyber adversaries are also using increasingly sophisticated tools, meaning some compromise attempts go undetected.

History has identified logistics lines of communication and supply routes as targetable critical vulnerabilities."Almost without exception the enemy flanks and supply line would define the decisive points for attack; an army could not survive without supply

[2] Commonwealth of Australia, *Australian Cyber Security Centre 2016 Threat Report* (Canberra, ACT: Australian Cyber Security Centre, 2016), 10, accessed 23 September 2017, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf.

[3] Commonwealth of Australia*, Australian Cyber Security Centre 2017 Threat Report* (Canberra, ACT: Australian Cyber Security Centre, 2017), 52, accessed 10 November 2017, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf.

and to threaten its base would compel it to fight, no matter how unfavorable the circumstances."[4] The acknowledgment of cyberspace as a warfighting domain has not changed the enduring nature of war. However, it has provided adversaries with a different method of targeting logistics, one that can be achieved by both state and non-state actors with relatively low costs.

Logistics information systems (LogIS) have enabled military supply chains, maintenance, transportation and distribution systems to become lean, responsive and efficient. These systems are reliant on a permissive cyberspace environment, and few training scenarios challenge logisticians to operate in a degraded cyberspace environment. Not only are military logistics information systems reliant on cyberspace to support forces in the physical domains but they routinely share information with third-party contractors, civilian and commercial vendors to generate the required effects. This interaction of information systems between Department of Defense information systems and unclassified information systems increases the vulnerability of military LogIS in cyberspace.

The focus of cyberspace within the logistics community to date has focused on the opportunities that it provides. The Internet of Things (IoT), delivery drones, and even air based warehousing have attracted interest from the logistics community in the recent past. The Australian Army, like other modern militaries, have implemented Radio Frequency Identification (RFID) and numerous computer systems to enhance logistics processes. It is prudent to conduct a detailed risk assessment from a cyberspace

[4] John Shy, "Jomini," in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton, NJ: Princeton University Press, 2010), 154.

perspective to ensure that the vulnerabilities these systems have introduced are mitigated and the residual risk accepted.

LogIS are vulnerable to compromise, and military operations may reach a culmination point before crossing the line of departure. Assuming adversaries can infiltrate military networks, their ability to access information regarding personnel and materiel movements, delete or modify and deny access to LogIS could prove catastrophic to military operations.

Within the remit of unclassified research, the cyber case studies of the Target Corporation, Stuxnet, and Estonia will be analyzed to identify vulnerabilities specific to military logistics information systems and propose solutions from doctrine, training and materiel perspectives to help protect the Australian Army from these identified vulnerabilities.

Significance of Study

Regardless of the technical constraints and vulnerabilities of an information system in cyberspace, the humans that operate and interface with a computer network remain its greatest vulnerability. Over the past seventeen years, the awareness of cyberspace as a domain of warfare has increased within both academic and military spheres of influence. However, the development of cyberspace understanding remains isolated to those with the technical expertise to understand the threats.

This research aims to raise awareness among the Australian Army logistics community regarding the vulnerabilities of logistics information systems in the cyberspace domain. The current state of oblivion amongst logistics planners, operators and users has its foundations on the assumptions of cyberspace superiority. The first steps towards addressing this oblivion include articulating vulnerabilities and identifying doctrine, training and materiel solutions.

Research Question

What are the vulnerabilities facing the Australian Army's logistics information systems within the cyberspace domain?

Secondary Research Question

What doctrine, training and materiel solutions exist that can help mitigate against vulnerabilities to logistics information systems within the cyberspace domain?

Definitions

This thesis is reliant on a common understanding of the cyberspace domain. There is an acknowledged lack of universally accepted terms to define cyberspace. The United Nations (UN), the North Atlantic Treaty Organization (NATO) and Australia's strategic cyber policy do not provide the breadth of definitions required to establish a common understanding for the reader. The definitions of cyberspace and associated terms used by the US Department of Defense have been used to establish common understanding and consistency throughout this research.

Cyberspace. A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[5]

Cybersecurity. Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.[6]

Offensive Cyberspace Operations (OCO). Cyberspace operations intended to project power by the application of force in or through cyberspace.[7]

Defensive Cyberspace Operations (DCO). Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.[8]

Department of Defense Information Networks (DODIN). Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks.[9]

[5] Chairman Joint Chiefs of Staff (CJCS), Joint Publication (JP) 3-12 (R), *Cyberspace Operations* (Washington, DC: Government Printing Office, 2013), GL-4, accessed 23 September 2017, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[6] Department of Defense (DoD), Department of Defense Instruction (DoDI) *Cybersecurity* (Washington, DC: Government Printing Office, 2014), 55, accessed 5 November 2017, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf.

[7] CJCS, JP 3-12 (R), GL-4.

[8] Ibid.

[9] CJCS, JP 3-12 (R), GL-4.

Logistics Information Systems (LogIS). Automated systems used to communicate with other units on vertical and horizontal flow of logistics and maintenance information and status.[10]

Assumptions

This thesis assumes that modern adversaries (state, non-state actors, or a combination of both) have the technological capability or access and infiltrate military logistics networks, and conduct OCO. Once access has been gained adversaries will target network confidentiality, integrity, and availability. The publicized cyberspace attacks against Estonia in 2007, the cyberspace attacks prevalent in the 2008 Russo-Georgian War, the Stuxnet attack revealed in 2010, the breach of Target information systems in 2013 and the ongoing cyber attacks on Ukraine, support this assumption.

Limitations

The primary limitations of this thesis are time to complete research, availability of information, and the accessibility of information in the unclassified realm. The time available to research this topic was limited to eight months. This time limitation has restricted the author's ability to analyze, and synthesize the information available, and apply it to the research area in the time available. The time available has impacted on the scope of the research conducted.

[10] Headquarters, Department of the Army (HQDA), Army Regulation (AR) 750-1, *Army Materiel Maintenance Policy* (Washington, DC: Government Printing Office, 2013), 203.

While logistics, supply chains, and transportation links are referred to in cyberspace literature as systems vulnerable to cyber-attacks, there are limited academic studies dedicated to how and why these systems are vulnerable and what to do to protect against these threats. Needless to say even less is written specifically on the vulnerabilities of military logistics systems in the cyberspace domain, and there are no case studies available at the unclassified level detailing attacks on logistics information systems in cyberspace. Therefore, this thesis analyses three case studies of cyberspace interference on information systems and will infer the impact of these types of attack on logistics information systems specifically.

This thesis is limited to information available at the unclassified level. For this reason, there is a reliance on unclassified US DOD doctrine and definitions, due to its availability and maturity from a cyberspace perspective. The use of US DOD doctrine also acknowledges the belief that US DOD research, doctrine and operating procedures are leading the western world in this area of warfare. As Australia's primary security ally it is reasonable to assume that US DOD cyberspace doctrine will influence Australian Defence Force cyberspace doctrine in the future, and therefore it should not detract from the analysis produced.

Delimitations

The study will assess the vulnerabilities of Australian Army's LogIS within the cyberspace domain, and propose doctrine, training and materiel solutions for logisticians to help reduce capability gaps. Cyberspace case studies will assist to identify vulnerabilities that can be exploited to achieve a detrimental effect on military LogIS. From this perspective, the research and analysis will not focus on the specific capabilities, tactics, techniques or procedures of a particular adversary or nation-state. The vulnerabilities of LogIS in cyberspace are enduring, regardless of the adversary that yields the capability to exploit them.

This research focuses on cyberspace threats and mitigations at the strategic and operational level of war. Exploitation of these vulnerabilities and capability gaps at the tactical level from a detailed technical perspective are beyond the scope of research, and outside of the expertise of the author.

The focus of research is on identifying the vulnerabilities of Australian Army LogIS in the cyberspace domain. Although parallels may be evident for the Australian Navy and Air Force, this is not the focal point for assessment or analysis. Likewise, this paper is not concerned with Offensive Cyberspace Operations conducted against a potential adversaries' LogIS. Although it is logical that their systems are vulnerable in similar ways to ours, this is deserving of independent research in its own right.

Summary

Logisticians have achieved effectiveness and efficiencies through reliance on networks and LogIS. The ability to share information simultaneously provides an excellent opportunity for automation and further improvement in logistics practices. However, while research and development need to focus on harnessing these evolving technologies, it must also be cognizant of the risks present in cyberspace. Failure to do so may force a culmination point jeopardizing the operational reach and maneuverability of the combat force.

A literature review is conducted in chapter 2 to identify the vulnerabilities facing the Australian Army's LogIS within the cyberspace domain. Academic literature will be used to gain an understanding of cyberspace, Australia’s current cyberspace policy, military operations in cyberspace, military logistics operations and logistics operations in cyberspace. The literature review articulates the common operating environment to enable a case study methodology to answer the primary and secondary research questions.

CHAPTER 2

LITERATURE REVIEW

> Australia and Australians are targets for malicious actors—including serious and organised criminal syndicates and foreign adversaries—who are all using cyberspace to further their aims and attack our interests. The scale and reach of malicious cyber activity affecting Australian public and private sector organisations and individuals is unprecedented. The rate of compromise is increasing and the methods used by malicious actors are rapidly evolving.
>
> —Prime Minister Malcolm Turnbull, *Australia's Cyber Security Strategy*

Introduction

The purpose of this literature review is to evaluate existing literature relevant to the thesis and identify gaps. The amount of academic literature available on military Logistics Information Systems (LogIS) operating within cyberspace is limited. Given that the audience for this thesis is logisticians, it is essential that the literature review provides the context of both cyberspace and military logistics. This review includes a summary of the frameworks contained within these subject areas to provide a common understanding of the environment, before identifying vulnerabilities and proposing solutions. The literature review is designed to answer the following questions:

1. What is Cyberspace?
2. What is Australia's Cyberspace strategy?
3. How are military operations conducted in Cyberspace?
4. What are Military Logistics Operations?
5. How does cyberspace impact Logistics Operations?

Cyberspace

Cyberspace has been acknowledged as a warfighting domain since 2009,[11] distinct from land, sea, air and space domains which dominated previous military concepts. In an increasingly interconnected world, cyberspace can impact on the other physical domains in ways not previously conceptualized. It is important to come to a common understanding of the domain to comprehend the impact of cyberspace on military logistics. It is equally important to identify what threats exist in the domain, and the common methods used by adversaries to gain access to networks to exploit them. Finally, it is important to summarize the broad methods of protecting networks against these vulnerabilities in the cyberspace domain.

The US, along with most other nations, is becoming increasingly reliant on the cyberspace domain for enabling many national security requirements.[12] This reliance is viewed by adversaries as an opportunity for targeting and exploitation, resulting in a focus on cybersecurity. "Increased international interest in cyber warfare is also based on

[11] Committee On Armed Services House of Representatives, *Cyberspace as a Warfighting Domain: Policy, Management and Technical Challenges to Mission Assurance*, Hearing Before the Terrorism, Unconventional Threats and Capabilities Subcommittee of the Committee On Armed Services House of Representatives 111th Congress, 5 May 2009, accessed 29 March 2018, https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg57218/pdf/CHRG-111hhrg57218.pdf.

[12] U.S. President, *The National Security Strategy of the United States of America* (NSS) (Washington, DC: Government Printing Office, 27 May 2010), accessed 16 October 2017, http://nssarchive.us/national-security-strategy-2010.

the recognition that information networks in cyberspace are becoming operational centers of gravity in armed conflict."[13]

"Cyberspace is first and foremost an information environment."[14] However, this oversimplifies the concept. The domain and the activities conducted within the domain must be defined to ensure a common baseline of understanding. Unfortunately, the definitions are numerous. In fact, the NATO Cyber Cooperative Defence Centre of Excellence notes: "there are no common definitions for Cyber terms – they are understood to mean different things by different nations/organizations, despite prevalence in mainstream media and in national and international organizational statements."[15]

Martin Libicki asserts that Cyberspace is a replicable construct that is built rather than born. It can exist in multiple locations simultaneously; in cyberspace, no single *there* exists. Cyberspace has three layers; physical hardware; a syntactic level where data and information are constructed and controlled; and semantic layer that contains the information meaningful to the end user whether it be human or machine.[16] Daniel Kuehl provides a broader definition, that Cyberspace is an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and

[13] Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (Lincoln, NE: Potomac Books, 2015), 222.

[14] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford, NY: Oxford University Press, 2014), 13.

[15] North Atlantic Treaty Organization, "NATO Cooperative Cyber Defence Centre of Excellence," NATO Cooperative Cyber Defence Centre of Excellence, 26 May 2014, accessed 2 November 2017, https://www.ccdcoe.org/cyber-definitions.

[16] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 5.

exploit information via interconnected and Internetted information systems and their associated infrastructures[17].

Australia's Cyber Security Strategy does not define cyberspace or cybersecurity. With the UN, NATO, and Australia unable to provide detailed definitions across a range of cyberspace terms, the definitions used by the United States of America Department of Defense will be adopted throughout this paper, as detailed in chapter 1. Therefore cyberspace is defined as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[18]

From numerous definitions, there are common factors identified which help the reader to understand Cyberspace. Firstly, Cyberspace contains a physical layer, which is the physical nodes, network infrastructure, software and hardware required to access cyberspace. These physical components reside in the land, air, sea and space domains and are vulnerable to disruption by lethal or kinetic effects. This layer includes the hardware which makes cyberspace possible. Some examples include routers, servers and individual computers, the physical assets which make networks and connections in cyberspace possible.[19]

[17] Franklin Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security*, (Washington, DC: Potomac Books, 2009), 4.

[18] CJCS, JP 3-12 (R), GL-4.

[19] Ibid., I–3.

Secondly, cyberspace consists of a logical network layer or the syntactic layer as proposed by Libicki. This layer includes elements of the network that are related to one another that is abstract from the physical network. These elements are independent as opposed to being tied to an individual or node. Examples include websites hosted on multiple domains that use a single Uniform Resource Locator (URL). Networks such as the Nonsecure Internet Protocol Router Network (NIPRNET) for the US military and the Defence Protected Network (DPN) for the Australian military reside in the logical layer.[20]

Lastly, cyberspace contains a cyber-persona layer, a further abstraction of the logical network layer. The layer relies on the logical network to create a digital representation or persona in cyberspace. The layer represents all the human interactions with the network. Cyber-personas can identify an actual person, including e-mail and IP address(es). However, a single person may have multiple cyber-personas, and a single cyber persona may have multiple users. This complication is one of the reasons that attributing responsibility for actions that occur in cyberspace can be so difficult.[21]

Intrusion Vectors

Singer and Friedman propose that "there are only three things you can do to a computer: steal its data, misuse credentials, and hijack resources."[22]These ideas have prevailed for a significant amount of time with Willis Ware outlining similar concepts in

[20] CJCS, JP 3-12 (R), I-3.

[21] Ibid., I–4.

[22] Singer and Friedman, *Cybersecurity and Cyberwar*, 39.

1967.[23] However, in a network-centric world, these three things can cause significant damage. The objectives of securing information environments include confidentiality, integrity, and availability[24]. It is logical that these, in turn, can be targeted to erode the trust that users have in the information system. Confidentiality attacks include gaining access to a network and extracting information and monitoring activities. Examples range from theft to espionage. Integrity attacks involve entering a network to modify data as opposed to extracting information. Availability attacks aim to prevent access to the network; this can be achieved through a Distributed Denial of Service (DDoS) in cyberspace, or through a kinetic effect which takes the network offline.

While the motives of cyberspace operations may be able to be grouped into three categories, the methods used to gain network access and facilitate these attacks are numerous and are continually becoming more sophisticated. Some of the more common methods include phishing attacks, and malware, distributed denial of service, and zero-day exploits.

Phishing Attacks

E-mails that contain a malicious link or file attachment containing malware constitute a phishing attack. Spearphishing is a sub-category where a phishing attack targets specific users of a network. Users of the network might easily identify a phishing attack from a Nigerian prince requesting bank details as a phishing attack. However,

[23] Willis H. Ware, “Security and Privacy in Computer Systems” (Report, RAND, Santa Monica, CA, April 1967), iii-4.

[24] Singer and Friedman, *Cybersecurity and Cyberwar*, 35.

these types of attack are becoming increasingly more sophisticated, and adversaries are exploiting data available on social media sites to assist them in making their attacks more plausible. These social engineering techniques help adversaries to exploit individuals personal and professional circumstances to deceive targets into opening malicious attachments and e-mails.[25]

Malware

Craig Stallard proposes that the most prevalent types of malware used in cyber-attacks include viruses, worms, and Trojan horses. A virus is a program that infects computers by attaching itself to a host program, replicating itself and transferring to another host. While a virus requires contact between the program and the host, a worm contains self-propagating code that enables it to move throughout the network. Worms can target selected programs as they move throughout a network, often targeting zero-day vulnerabilities. Trojan horses are programs concealed in software that appears benign and will remain dormant until triggered by pre-determined protocols (an external command, set of conditions or a time limit). Trojan horses are data-collection tools, including keyloggers that enable the monitoring of passwords and activities, as well as rootkits that allow the conduct of unauthorized logins and activities on a host system.[26]

[25] Commonwealth of Australia, *Australian Cyber Security Centre 2016 Threat Report*, 20.

[26] Craig Stallard, "At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force" (Monograph, School of Advanced Air and Space Studies, Maxwell Air Force Base, AL, 2011), 42.

Distributed Denial of Service

This method of attack does not gain access to the target network. Instead, it prevents authorized users from accessing the network altogether. Attackers accomplish the effect by flooding bandwidth or servers with e-mails or website-access requests. The volume of traffic, usually measured in millions of hits per second, overwhelms the servers causing them to crash. This form of attack is heavily reliant on bots which use software that accesses an individual computer, usually through malware, then surreptitiously sends out e-mails or pings targeted information systems. The owner of the individual computer is normally oblivious to the cyber activity. The malware can impregnate computers and form a network allowing a distributed and coordinated attack on the target network.[27]

Zero Day Exploits

These are vulnerabilities previously unknown to software or hardware developers so that there has been no time to develop or distribute patches.[28] All software has flaws. Vulnerabilities are the flaws that create a security weakness in the design, implementation, or operation of a system or application. Typically, there are 20 bugs per 1,000 lines of code before testing and one or two orders of magnitude less after

[27] Stallard, "At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force," 43.

[28] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (1 February 2011): 24.

testing.Adversaries can exploit these vulnerabilities through the malicious code to achieve their objectives in cyberspace.[29]

When discussing threats to networks in cyberspace, it is essential to highlight the role that humans play. Historically, password insecurity and the inherent trusting nature of people, who are often time poor and have different knowledge and familiarity with threats in cyberspace enable adversaries to access to networks. "Clever attackers take advantage of our innate trust to convince us to click links, open attachments, or give out our passwords to strangers over the phone Since 99 percent of our phone calls and e-mails are not malicious, it is hard to be constantly vigilant."[30]

Network Access

According to the Australian Cyber Security Centre 2016 threat report, a 'typical' compromise of a network in cyberspace constitutes four phases, gaining an initial foothold, establishing a presence, persistence, and execution of intent. Figure 1 provides a graphical representation of these phases. It is imperative to understand how access to a network is exploited using the intrusion vectors summarized above to determine how LogIS are vulnerable in cyberspace,

[29] Martin C. Libicki, Lillian Ablon, and Tim Webb, *The Defender's Dilemma: Charting a Course Toward Cybersecurity* (Santa Monica, CA: RAND Corporation, 2015), 42.

[30] Singer and Friedman, *Cybersecurity and Cyberwar*, 65.

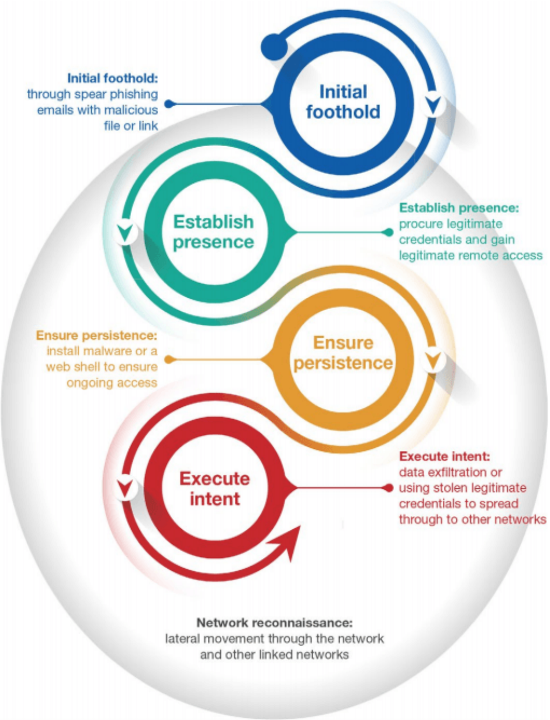

Initial foothold
Initial foothold: through spear phishing emails with malicious file or link
Establish presence
Establish presence: procure legitimate credentials and gain legitimate remote access
Ensure persistence
Ensure persistence: install malware or a web shell to ensure ongoing access
Execute intent
Execute intent: data exfiltration or using stolen legitimate credentials to spread through to other networks
Network reconnaissance: lateral movement through the network and other linked networks

Figure 1. ACSC 'Typical' Compromise

Source: Commonwealth of Australia, *Australian Cyber Security Centre 2016 Threat Report* (Canberra, ACT: Australian Cyber Security Centre, October 2016), 34, accessed 23 September 2017, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf.

Initial Foothold

An adversary gains access to the network by establishing an initial foothold. Phishing attacks, including spear phishing, honey traps, and watering holes are all intrusion vectors utilized to establish the foothold. All of these types of attack lure users of networks into executing malware which creates an entry into the network. Once the foothold is secure, the attacker takes steps to establish their presence.[31]

Establish Presence

Once an initial foothold is secured, adversaries establish their presence by monitoring and searching for administration credentials with the intention of spreading to other connected networks, which may be the main target for the attack. While monitoring the network, the attacker attempts to gain legitimate user credentials with the aim of obtaining remote administrator access. After obtaining legitimate credentials, the adversary can transition from access that is dependent on malware to the use of a Virtual Private Network (VPN), Virtual Desktop Infrastructure (VDI), or other corporate remote-access solutions combined with software native to the organization.[32]

Ensure Persistence

Once access to the network is secured, attackers install malware or a web shell to ensure ongoing access. This malware prevents their legitimate access from being revoked. Web Shells generate no network traffic and therefore enable the attacker to remain below the detection threshold.[33]

[31] Commonwealth of Australia, *Australian Cyber Security Centre 2016 Threat Report*, 34.

[32] Ibid.

[33] Ibid.

Execute Intent

It is only during this phase of the cyber-attack that the adversary is now able to execute the intent for their operation. As previously stated the intention for any attack falls into three categories, confidentiality, integrity and availability. Adversaries are likely to conduct data exfiltration or data modification activities during this phase of the compromise.[34]

Advanced Persistent Threats (APT)

APTs are well coordinated, informed and resourced. This term does not describe the technique used to gain access but describes the style of attack. These attacks aim to break into a network, avoid detection, and collect information over an extended period. "the initial target is frequently not the main prize. An effective way into a network is via trusted outsiders, who often have lower levels of defense, or by targeting people in the network who have some access permissions to open the gates wider."[35] Organized entities ranging from state actors to cybercriminals who have access to both the technology and the funding to execute a long-term reconnaissance of a network are capable of APT operations.

[34] Commonwealth of Australia, *Australian Cyber Security Centre 2016 Threat Report*, 34.

[35] James Torrence, "Spear Phishing: Dangers & Need for Education," *Small Wars Journal*, 5 February 2017, accessed 10 October 2017, http://smallwarsjournal.com/print/62068.

Protection and Risk Mitigation

Risk mitigation strategies and protection mechanisms broadly fall into three categories, network architecture, system hygiene (patching and software updates), and user practices. The ASD has published eight steps to mitigate cybersecurity incidents. These steps include application whitelisting, patching applications, disabling untrusted Microsoft office macros, user application hardening, restricting administrative privileges, patching operating systems, multi-factor authentication and daily backup of important data.[36]

Resiliency is part of the solution to the threats faced by information systems operating in cyberspace. "Resilience is what allows a system to endure security threats instead of critically failing. A key to resilience is accepting the inevitability of threats and even limited failures in your defenses."[37] Resiliency must include redundancy, both electronic and physical. From this perspective, electronic redundancy refers to the duplication of data, or back up files stored in multiple locations. Physical redundancy for military logistics refers to additional warehouse stocks that provide sustainment support if the adversary compromises the electronic lines of communication.

Specifically for sustainment considerations, US cyberspace doctrine suggests that military forces must "identify required forces and capabilities, critical cyberspace assets, assess risk, ensure redundancy (including non-cyberspace alternatives), and actively

[36] Commonwealth of Australia, *Essential Eight Explained* (Canberra, ACT: Australian Signals Directorate, February 2017), 2, accessed 5 December 2017, https://www.asd.gov.au/publications/protect/Essential_Eight_Explained.pdf.

[37] Singer and Friedman, *Cybersecurity and Cyberwar*, 36.

exercise continuity of operations plans to respond to outages or adversary actions that degrade or compromise cyberspace access or reliability."[38] These practical steps to build cyberspace resiliency do not appear in logistics or sustainment doctrine in the US Army or the Australian Army.

Australian Cyberspace Policy

Australian Cyberspace strategy is in its infancy when compared to its primary security ally, the United States of America (USA) or China, as the dominant regional power in South East Asia. Australia's policies towards cyberspace will be depicted firstly from a historical perspective before analyzing current guidance provided in the 2016 Defence White Paper and Cyber Security Strategy respectively. This paper then discusses Government structures, and roles and responsibilities before identifying the role of the ADF in particular.

Cybersecurity first emerged as a national security issue in the 2000 Defence White Paper which led to the production of the E-security initiative launched in May 2001 by Prime Minister John Howard. This policy was later reviewed in 2008 by Prime Minister Kevin Rudd. Tangible action at the political level to address policy within cyberspace was not apparent until 2009 Defence White Paper by the Rudd government. The Cyber Security Strategy released in November 2009, established for the first time Australia's strategic priorities for securing Australia's National Information Infrastructure. It established the Cyber Security Operations Center (CSOC) within the ASD and the Computer Emergency Response Team (CERT Australia). The 2013

[38] CJCS, JP 3-12 (R), viii.

Defence White Paper released by Prime Minister Julia Gillard built upon these foundations and established the Australian Cyber Security Centre (ACSC) as part of the National Security Strategy. While these early policy documents indicate a growing awareness of cyberspace, they conceptualize the problem, rather than provide clear direction.

The 2016 Defence White Paper, still fell short of providing clear direction for the ADF. The term cyber is used 55 times throughout the 186-page document; yet, it failed to provide definitions, frame the problem, or provide direction and vision for the future. The depth and breadth of vulnerabilities in the cyberspace domain was not acknowledged, with emphasis placed on cyber attacks being "direct threat[s] to the ADF's warfighting ability."[39] This definition was limited in its usefulness because it provided a narrow definition of cyber attack and focused on the ADF in particular. It was ambiguous regarding the role of the ADF to respond to a cyber attack compromising national infrastructure, or government networks.

The Turnbull government developed national policy within the cyberspace domain through the update of the National Cyber Security Strategy in 2016. The strategy establishes five themes of action over a four-year period, a national cyber partnership, strong cyber defenses, global responsibility and influence, growth and innovation and a

[39] Commonwealth of Australia, *Department of Defence White Paper 2016* (Canberra, ACT: Department of Defence, 2016), 51, accessed 2 November 2017, http://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.

cyber-smart nation[40]. The national strategy appears to focus on the opportunities that cyberspace can provide Australia as a nation and is narrow in its depiction of cyberspace as part of the information revolution. The focus is primarily on expanding industrial sectors, new markets and expanding cybersecurity businesses while mitigating online risks at a user level.[41]

The strategy aimed to streamline the Government cybersecurity structure to bring together distinct functions of both the policy and operational elements. Three coordinated strategic level pillars were announced to achieve this. The Department of the Prime Minister and Cabinet will be the central point for policy issues to ensure a simplified Government interface for stakeholders. The Department is designed to oversee the cybersecurity policy and implementation of the strategy. The second pillar is the ACSC Coordinator charged with guiding whole-of-nation cybersecurity priorities and coordinating the Government's cybersecurity capabilities at the organizational level. The ASD leads the ACSC, recognizing the proportion of work conducted by the Department of Defence (DoD) in defending Australia against malicious cyber activity. The Department of Foreign Affairs and Trade forms the final pillar, where a Cyber Ambassador is appointed to lead Australia's international cyber effort.[42]

[40] Commonwealth of Australia, *Australia's Cyber Security Strategy* (Canberra, ACT: Department of the Prime Minister and Cabinet, 2016), 6, accessed 23 September 2017, https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf.

[41] Ibid., 4–11.

[42] Ibid., 23.

The Australian Cyber Security Centre (ACSC) opened in 2014 and is an impressive collaborative initiative. The ACSC brings together the Australian Government's operational cybersecurity capabilities in one location to share threat information. ACSC is the central organization for the cybersecurity efforts of the ASD, the Defence Intelligence Organisation (DIO), the Australian Intelligence Organisation (ASIO), CERT Australia, the Australian Criminal Intelligence Commission (ACIC), and the Australian Federal Police (AFP).[43] The ACSC produces an annual threat report aiming to inform the Australian public on current threats persisting in cyberspace. The ACSC also provides advice on how organizations can defend themselves and conducts an assessment of the maturity of cyberspace practices.[44]

[43] Commonwealth of Australia, *Australian Cyber Security Centre 2016 Threat Report*, 3.

[44] Commonwealth of Australia, *Australia's Cyber Security Strategy*, 31.

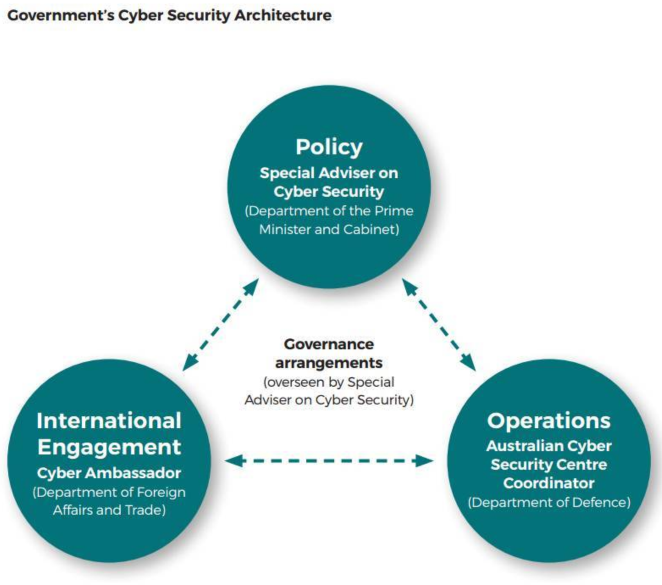

Government's Cyber Security Architecture
Policy
Special Adviser on Cyber Security
(Department of the Prime Minister and Cabinet)
Governance arrangements
(overseen by Special Adviser on Cyber Security)
International Engagement
Cyber Ambassador
(Department of Foreign Affairs and Trade)
Operations
Australian Cyber Security Centre Coordinator
(Department of Defence)

Figure 2. Australian Government's Cyber Security Architecture

Source: Commonwealth of Australia, *Australia's Cyber Security Strategy* (Canberra, ACT: Department of the Prime Minister and Cabinet, 2016), 24, accessed 23 September 2017, https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf.

In June 2017 the Australian Defence Force announced the establishment of the Information Warfare Division (IWD), reporting to the Chief of the Defence Force through the Joint Capability Group. Major General Marcus Thompson commands IWD and is responsible for four branches Information Warfare Capability, C4 (command control, coordination and communications) and Battle Management Capability, Capability Support Direction, and the Joint Cyber Unit.[45] Greg Austin, a professor at the Australian Centre for Cyber Security applauds the establishment while simultaneously

[45] Greg Austin, "'Cyber Revolution' in Australian Defence Force Demands Rethink of Staff, Training and Policy," *The Conversation*, 1, accessed 23 September 2017, http://theconversation.com/cyber-revolution-in-australian-defence-force-demands-rethink-of-staff-training-and-policy-80317.

offering the following critique, “The Australian Defence Force is on the cusp of a revolution as it prepares to reorganize for cyber-enabled warfare. The military cyber shake-up coming many years late brings big problems and some windfall gains.”[46] While responsibility for OCO appears to remain with ASD, it is likely that the new Information Warfare Division will focus on DODIN and DCO.

Military Operations in Cyberspace

At the time of publication, the Australian Army does not have Cyberspace or Cybersecurity doctrine published at the unclassified level. With the announcement of the IWD, it is logical to assume that Australia will use US CYBERCOM structure and doctrine as a guide to inform national strategic and operational level doctrine. Not only is it advantageous to leverage off intellectual rigor and lessons learned previously by a close ally, but it will also assist Australian and US military forces operating together in the future if definitions and concepts are the same or similar. Therefore, the framework that US CYBERCOM has adopted to distinguish between different CO has been summarized below to provide a conceptual framework for how Australian cyberspace operations are likely to be conducted in the future.

The primary source of information regarding US military operations in Cyberspace is Joint Publication 3-12 (R) *Cyberspace Operations*. To this end, the US military has determined that CO, as defined in chapter 1, are categorized as OCO, DCO and DODIN operations based on the intention of the military operation. The discussion of

[46] Greg Austin, “A Cyber Revolution on Russell Hill,” Australian Strategic Policy Institute, *The Strategist*, 16 May 2017, accessed 6 November 2017, https://www.aspistrategist.org.au/cyber-revolution-russell-hill/.

military operations in Cyberspace is limited to DODIN operations and DCO due to the scope of the thesis.

Expanding upon the definition provided in chapter 1, DODIN operations achieve the objective of providing freedom of maneuver in cyberspace. It includes the remit of designing, building, configuring, securing, operating, maintaining and sustaining the information environment upon which the US DOD is reliant.[47] Major General Williams proposes that it is useful to think of DODIN operations as being network focused and threat agnostic. This description is useful as it explains the difference between DCO and DODIN operations from a military perspective.

DODIN operations set the baseline of security for DOD networks. These operations approach security from an Information Technology (IT) viewpoint and focus on the operational configuration of the network. Examples of DODIN operations include correcting known IT vulnerabilities, encrypting data and determining encryption standards across the network, as well as establishing and enforcing user and administrator training and compliance. DODIN security measures are not aimed at a specific threat but are benchmarks established to deter a wide range of threat vectors and actors as well as mitigating against known vulnerabilities.[48]

Separate to the definition provided in chapter 1, DCO aims to outmaneuver adversaries in cyberspace by providing the ability to discover, detect, analyze and mitigate threats to the DOD. This remit includes networks used in support of US DOD

[47] CJCS, JP 3-12 (R), II–2.

[48] Brett Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* (2nd Quarter 2014): 15.

operations and is not limited to the Non-classified Internet Protocol (IP) Router Network (NIPR Network) or networks exclusively used by the US DOD. DCO are mission focused and threat-specific, executed against specific threats with known malicious capability and intent to affect DOD key cyberspace terrain.[49]

DCO operations include Internal Defence Measures (IDM) and Response Actions (RA). IDM is DCO conducted within the DODIN. It encompasses hunting for advanced internal threats, internal responses to these threats and responding to unauthorized activities. RA is authorized defensive actions conducted external to the DODIN conducted to defeat ongoing or imminent threats and therefore defend DOD cyberspace capabilities or other designated systems.[50]

Military Logistics Operations

The Australian Army defines logistics as "the science of planning and carrying out the movement and maintenance of forces."[51] The concept details sub-functions within logistics, for this study the relevant subfunctions are the design and development, acquisition, storage, movement, distribution, maintenance, evacuation and disposition of materiel. Doctrine also provides a definition of lines of communication, "All the land, water, and air routes that connect an operating military force with one or more bases of

[49] Williams, "The Joint Force Commander's Guide to Cyberspace Operations," 15.

[50] CJCS, JP 3-12 (R), II–3.

[51] Commonwealth of Australia*, Land Warfare Doctrine 4-0 Logistics* (Canberra, ACT: Australian Army, 2018), 9, accessed 08 April 2018, https://www.army.gov.au/sites/g/files/net1846/f/lwd_4-0_logistics_full.pdf.

operations, and along which supplies and reinforcements move.”[52] It is plausible to extend this definition to incorporate cyberspace operations to include activities which facilitate the connection of military forces with one another, and the networks that communicate digital demands.

Logistics must be tightly integrated across the tactical, operational and strategic levels of war to create a continuum that extends across organizational and functional boundaries to provide combat elements with materiel in the right condition, and services of the required quality, on time and at the right place. The continuum comprises a complex network of logistic processes, systems, installations, and organization, all of which must provide support to enhance combat power.[53]

In discussing the contemporary operating environment for logistics, Land Warfare Doctrine (LWD) *Logistics* 4-0 identifies challenges to logistics as “resourcing and budgetary pressures, organizational change and reforms, operational tempo and complexity of equipment.”[54] It also acknowledges that conflicting priorities, complex interoperability and communication requirements combined with relationships between Services, government agencies, host nation, foreign militaries and civil contractors make the operating environment more complex.[55] The Australian Army published the latest

[52] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Combat Service Support*, 97.

[53] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Logistics*, 13.

[54] Ibid., 15.

[55] Ibid.

release of LWD 4-0 in 2018; it is significant that it does not identify cyberspace as a threat or challenge in the current or future operating environment for logisticians.

Increased connectivity is written predominantly from a positive perspective, identifying that successful execution relies on "unwavering reliance placed on connectivity throughout the land force operating in future environments . . .R]apid information flow around the battlespace will be considered a norm, as it is now."[56] These assertions assume cyberspace superiority, as opposed to an assumption of a cyberspace degraded operational environment. This doctrine envisions future resupply convoys being autonomous, or semi-autonomous while relying on automated supply chains in a highly complex enterprise network.[57]

LWD 4-0 does acknowledge network threats, "[o]ngoing data and network threats will exist in the logistics continuum, in both military and civil environments."[58] However, it fails to identify what these network threats look like currently, or in the future and provides no assessment of the likelihood or impact of such an attack eventuating. As such, the mitigating measures identified in LWD4-0 are broad and difficult to implement.

The identified mitigation is "[e]nsuring that individuals are routinely informed and aware of information management techniques in threat environments and appropriate

[56] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Logistics*, 16.

[57] Ibid.

[58] Ibid.

information security are measures in place."[59] LWD 4-0 does not articulate who is responsible for implementing these mitigation strategies. Based solelyon this broad mitigation, the document declares that "the risk is reduced within the logistics continuum."[60] The 2018 review of LWD 4-0 is a missed opportunity to achieve the identified mitigation strategy of raising awareness and informing users of LogIS of the threats faced by logisticians in the cyberspace domain.

The Australian Army identifies principles of logistics which are used to guide logistics activities to achieve an effective logistic system. These principles include responsiveness, simplicity, economy, flexibility, balance, foresight, sustainability, survivability, and integration.[61] Relevant to this study are the principles of responsiveness, economy, balance, and survivability. The definitions of these principles are provided below, and will be used in chapter 5 to identify the impact that cyberspace operations can have on logistics operations:

Responsiveness

Responsiveness is the ability of the logistic system to provide the right support at the right time and place, and in the right condition, to meet the commander's needs. Responsiveness is the keystone principle in the sense that all else becomes irrelevant if the logistics system cannot support the operation.[62]

[59] Ibid.

[60] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Logistics*, 16.

[61] Ibid., 11.

[62] Ibid., 10.

Economy

In military operations logistic resources will be scarce, and economy of both resources and effort must be a logistic goal. Economy is achieved from a logistics perspective when effective support is provided using the fewest resources at the least cost and within acceptable levels of risk.[63]

Balance

The logistic system must balance the need for economy with the requirement for redundancy and reserve capacity. It must balance the need to anticipate the requirement to adapt and respond. It must also balance the need for efficiency with the need for effective support in a battlespace characterized by friction, uncertainty, fluidity, and disorder.[64]

Survivability

Survivability is the capacity of the logistic system to prevail in the face of potential or actual destruction. The ability of the logistics assets to continue to operate in support of the commander's plan is integral to the success of that plan. Logistic installations, units, and information systems are high-value targets that must be safeguarded by both active and passive measures. Survivability requires planning for the dispersion and protection of critical nodes of the logistics infrastructure. A degree of decentralization and redundancy is critical to the safety of the logistic system. The

[63] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Logistics*, 10.

[64] Ibid.

allocation of reserves, development of alternatives and phasing of logistic support also contribute to survivability.[65]

The doctrinal definition of a culmination point reveals the importance of logistics operations to the Australian Army. "The point in time and location where a force will no longer be stronger than the enemy and risks losing the initiative."[66] The notes accompanying this definition detail that this may be due to reduced combat power, attrition, logistics, dwindling national will or other factors. This reference provides further evidence that the Australian Army identifies Logistics operations as a critical vulnerability, as it has the power to force a culmination point before military forces achieving the desired military objective or endstate.

Logistics Operations in Cyberspace

Logistics has benefited significantly from technological advances in cyberspace. Globalization and improvement in communications systems have led the military to adopt lean logistics practices. The commercial practices of Just in Time (JIT) logistics have prevailed over Just in Case (JIC) logistics. This transformation has made logistics supply chains more efficient.[67] Less redundancy, reduced wastage and reduced stockholdings have made the lines of communication more flexible, more maneuverable

[65] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Logistics*, 11.

[66] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Combat Service Support*, 96.

[67] Sirius Bontea, "The Cyber Threat to Military Just-In-Time Logistics: Risk Mitigation and the Return to Forward Basing" (Monograph, School of Advanced Military Studies, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2017), 10.

with comparable responsiveness. Logistics practices such as forward basing and redundancy have become less relevant by LogIS.

General McDrew, the current commander of US Transportation Command, gave an address at the Logistics Officer Association Symposium in 2017, where he proposed that emerging technology, volatile geopolitics, and shifting demographics will be the changes that will define the modern military. Significantly, he has identified cybersecurity as one of his priorities for his command. He identifies the threat and the impact to logistics systems below:

> An adversary doesn't have to stop us. All they have to do is slow us down. All they have to do is make us doubt the accuracy of our own data. Once we've lost the veracity, how do you get it back? We will check double-check and triple-check every piece of data. By the time we figure it out it may be too late. Our adversaries may have already won. They will not have used one bomb or one bullet. Instead, they will use ones and zeros. That is the reality of our time; it does not matter if we have the most lethal military in the world if we can't get it where it needs to go when it needs to get there. It just doesn't matter.[68]

Military logistics supply chains have become completely reliant on information systems operating in cyberspace to manage inventory, receipt, issue, and distribute materiel and equipment. LogIS are particularly vulnerable as the data is shared with commercial contractors, and often the data travels through the unsecured commercial internet. "Furthermore, unsecure networks and systems of our commercial transportation service providers, coupled with critical infrastructure vulnerabilities around the globe,

[68] Darren McDrew, "Transcom Commander Discusses the Strategic Environment" (Speech, presented at the Logistics Officer Association Symposium, National Hall, MD, November 15, 2017), accessed 16 November 2017, https://cdn.dvidshub.net/media/video/1711/DOD_105079033/DOD_105079033-1920x1080-6221k.mp4.

almost wholly reside outside our control and pose significant risk to mission assurance."[69]

The Germany-based multinational software company, Systems, Applications & Products in Data Processing (SAP), produces Enterprise Resource Planning (ERP) software for sectors including manufacturing, government, energy, telecommunications, finance, as well as defense.[70] Global Combat Support System-Army runs exclusively on this software. Multinational interoperability has become a focus for the US military and her allies. It is therefore not surprising to note that 14 NATO countries including the USA, Canada, Germany, Netherlands, Sweden, Denmark, and Norway have all adopted LogIS based on the SAP platform[71]. Australia is in the process of moving from a number of LogIS to a singular platform based on SAP ERP software.

SAP is a multi-billion-dollar company with 345,000 customers in 190 countries, including 87 percent of the Forbes Global 2000. While SAP software provides robust security capabilities across the aforementioned industries and builds critical software

[69] House of the Armed Services Committee, *The Current State of U.S. Transportation Command*, House of the Armed Services Committee 115th Congress, 30 March 2017, Testimony of General Darren W. McDrew, USAF, accessed 16 November 2017, http://docs.house.gov/meetings/AS/AS03/20170330/105767/HHRG-115-AS03-Wstate-McDewUSAFD-20170330.pdf.

[70] SAP, "Military, Defense, and Security | Industry Software," accessed 5 December 2017, https://www.sap.com/industries/defense-security.html.

[71] SAP, "SAP Paves Way for NATO's Next-Generation Command and Control Systems," SAP News Center, 26 July 2005, accessed 5 December 2017, https://news.sap.com/sap-paves-way-for-natos-next-generation-command-and-control-systems/.

patches for their users on a monthly basis, it is not invulnerable to cyber-attacks.[72] While interoperability is a significant force multiplier, particularly in forming multinational coalitions, it also makes SAP a high-value target for a potential adversary.

SAP ERP software is a large step forward for Australian LogIS. The current state of the ADFs ERP environment consisting of a multitude of systems operating in silo environments. The Logistics information system is MILIS, the Human Resource information system is PmKeys (transitioned to Defence One in 2017), and the financial information system is Roman.[73] This structure led to a number of network silos within the LogIS network. Figure 3 provides a graphical representation of the current network relationships.

[72] Mathieu Geli, Darya Maenkova, and Alexander Polyakov, *SAP Cyber Security in Figures (Global Threat Report 2016)*, 2016, accessed 5 December 2017, https://erpscan.com/wp-content/uploads/publications/Sap-Cyber-Threat-Report.pdf.

[73] KPMG, “Defense ERP Overview by Country,” April 2016, accessed 5 December 2017, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/04/defense-erp-overview-by-country.pdf.

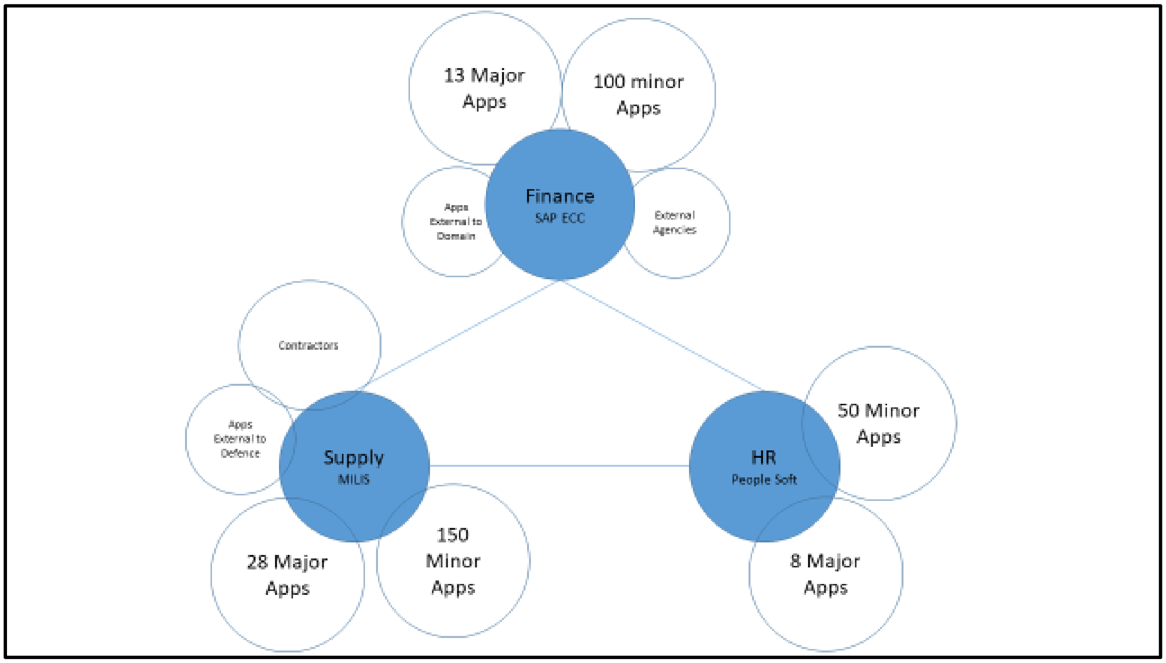


Figure 3. Australian Army Current LogIS

Source: Created by author.

This network can be contrasted with the future ADF ERP environment once SAP is integrated. Figure 4 depicts the future ERP environment, particularly notable is increased automation between applications and networks, and a considerable reduction in applications and programs. The reduction in the number of information systems will facilitate security through network architecture and system hygiene. SAP will replace a number of legacy systems which have been unable to be easily modified or patched, thus reducing the risk across the ADF DPN.

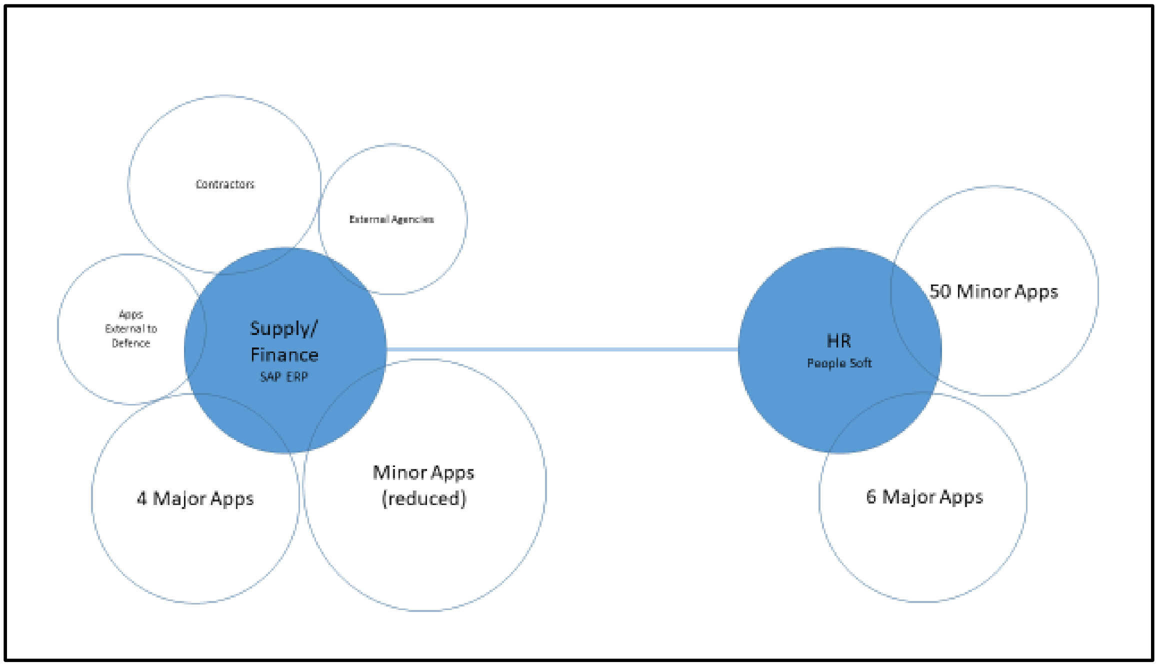


Figure 4. Australian Army Future LogIS

Source: Created by author.

Military LogIS have arguably made logistic supply chain processes more efficient and more effective, in a permissive cyberspace environment. The key issue is now to understand the vulnerabilities that are inherent in these military LogIS and look at risk mitigation strategies to provide militaries with the redundancy and resilience to continue to provide logistics support in a non-permissive or degraded cyberspace environment. Failure to identify, understand and mitigate these risks can lead to an early culmination point before the land battle begins.

Summary

> The ability to use cyberweapons as a force multiplier for conventional military operations is another significant characteristic of cyber warfare. Cyber weapons are well suited for attacks on logistical networks, reinforcements, and command-and-control facilities 'to induce operational paralysis.
>
> — Brian Mazanec, *The Evolution of Cyber War*

Contemporary academic literature identifies opportunities and threats presented by the cyberspace domain. However, literature does not articulate the vulnerabilities of LogIS operating in cyberspace. There is relatively little academic literature aimed at logisticians explaining what measures should be taken to protect LogIS.

Compared to the US Army, and other regional powers Australia, its Defence force and Army specifically are late in formalizing its strategy and military doctrine towards cyberspace. DCO and DODIN security operations should be the focus for logisticians and LogIS operating in cyberspace. These operations should focus on maintaining the confidentiality, integrity, and availability of military LogIS while developing resilience and redundancy to mitigate against network compromise. "There is still much more to do to address our current and future cyber capabilities. People, processes, and technology are all key areas where we can enhance our cyber resiliency."[74]

[74] House of the Armed Services Committee. *The Current State of U.S. Transportation Command*, 18.

CHAPTER 3

RESEARCH METHODOLOGY

Purpose

This chapter outlines the process applied to researching this thesis. This chapter will define the methodology incorporated into the research, why this methodology is appropriate for the research questions and subject area, data collection methods, and methods of data analysis. The primary research question, what are the vulnerabilities facing the Australian Army's LogIS within the cyberspace domain will limit the scope of data analyzed.

Methodology

This thesis will use qualitative research methods to identify vulnerabilities faced by the Australian Army in cyberspace. Qualitative research is appropriate because the problem needs further exploration.[75] While there is quantitative and qualitative research available analyzing cyberspace attacks, threats and vulnerabilities there has been limited extrapolation of this research to include the impact of cyber-attacks on LogIS. To integrate rigor into the qualitative research, the study has focused on reducing bias and achieving fourth generation evaluation parallel criteria as proposed by Guba and Lincoln

[75] John W. Creswell, *Qualitative Inquiry and Research Design: Choosing among Five Approaches,* 2nd ed. (Thousand Oaks, CA: SAGE Publications, Inc., 2006), 39-40.

in their work, *Fourth Generation Evaluation*. These criteria are credibility, transferability, dependability, and confirmability.[76]

Within the parameters of qualitative research, this thesis will be conducted using the multiple case study framework as proposed by John Creswell in his book *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.* He posits that case study research "involves the study of an issue, explored through one or more cases within a bounded system."[77] The collective or multiple case study method "involves studying multiple cases simultaneously or sequentially in an attempt to generate a still broader appreciation of a particular issue."[78] Case research has consistently been one of the most powerful research methods.[79] Case study analysis allows answers to the questions of what, why and how while gaining an appreciation of the complexity of the entire phenomenon.[80]

Case study methodology lends itself to this particular thesis, as it enables the researcher to examine previous vulnerabilities within the financial, industrial and commercial networks. Data is then extrapolated to propose that similar vulnerabilities exist within the Australian Army Logistics Information system networks. Furthermore,

[76] Egon G. Guba and Yvonna S. Lincoln, *Fourth Generation Evaluation* (Newbury Park, CA: Sage Publications, 1989), 228-251.

[77] Creswell, *Qualitative Inquiry and Research Design*, 73.

[78] Ibid., 98.

[79] Chris Voss, Nikos Tsikriktsis, and Mark Frohlich, "Case Research in Operations Management," *International Journal of Operations & Production Management* 22, no. 2 (1 February 2002): 195.

[80] Ibid., 197.

identification of measures taken to repair and defend those networks can be used to identify prevention measures that can be adopted by the Australian Army to make its LogIS more robust. Thus the methodology can adequately answer both the primary and secondary research questions.

Case Study methods are “bounded or described within certain parameters, such as a specific place and time.”[81] Chapter 1 identifies the parameters for research as limitations and delimitations. Case Studies are constrained to cyberspace attacks that occurred in the last decade, focusing on the motivation of network infiltration as discussed in chapter 2 as opposed to network infiltration methods. These motivations including violating data confidentiality, and data integrity or denying availability of networks, systems, and data. These parameters ensure that the case study selection is relevant to the subject area and that the subsequent conclusions made are plausible within the scope of research undertaken.

Credibility is considered to be one of the key criteria in the conduct of a qualitative study to achieve internal validity, “to ensure that their study measures or tests what is intended.”[82] It includes the adoption of appropriate, well-recognized research methods, debriefing sessions between researcher and superiors, and the examination of previous research to frame findings. The case study methodology used to conduct qualitative research for this thesis is an academically recognized methodology for conducting research. A committee of academic professionals across the Tactics, Logistics

[81] Creswell, *Qualitative Inquiry and Research Design*, 98.

[82] Andrew Shenton, “Strategies for Ensuring Trustworthiness in Qualitative Research Projects,” *Education for Information* 22, no. 2 (2004): 64.

and Cyberspace areas of expertise have reviewed the research for this thesis. This committee has reviewed the primary and secondary research questions, the research methodology and the literature review in chapter 2 to determine the credibility and quality of the research.

"How one determines the extent to which the findings of a particular inquiry have applicability in other contexts"[83] is called transferability. Establishment of transferability is essential to answer the research questions. This thesis is reliant on demonstrating that the analysis and vulnerabilities of financial, industrial, and commercial information systems in cyberspace apply to Australian Army LogIS. The selection of case studies and the case study assessment criteria contribute to the achievement of transferability. The provision of background data before the assessment and analysis of selected case studies is essential to establish the context of the study and detailed description of the occurrence in question to comparisons to be made.[84]

"The way in which a study is conducted should be consistent across time, researchers, and analysis techniques."[85] Dependability is evident in research if another researcher can follow the same decision trail used by the initial researcher. This chapter outlines both the methodology and framework for conducting analysis, as well as the

[83] Eileen Thomas and Joan Kathy Magilvy, "Qualitative Rigor or Research Validity in Qualitative Research," *Journal for Specialists in Pediatric Nursing* 16, no. 2 (1 April 2011): 151.

[84] Shenton, *Strategies for Ensuring Trustworthiness in Qualitative Research Projects*, 73.

[85] Susan L. Morrow, "Quality and Trustworthiness in Qualitative Research in Counseling Psychology," *Journal of Counseling Psychology* 52, no. 2 (April 2005): 252.

method of collecting and capturing results of the case study methodology. The in-depth methodological description enables a different researcher to repeat the study.

Confirmability "is the qualitative investigator's comparable concern to objectivity."[86] It includes the steps taken by the researcher to mitigate bias and remain objective. Triangulation is a technique used to increase the fidelity of interpretation of data, it "usually depends on the convergence of data gathered by different methods."[87] This thesis achieves triangulation through the number of case studies, the types of networks analyzed and the different motivations of the adversary in gaining access to networks. This chapter also discusses the limitations and shortcomings of the research methodology selected and measures taken to mitigate these shortfalls. Credibility, transferability, and dependability as established in the research, as has been outlined in this chapter all contribute to the establishment of confirmability.

Analytical Framework

The four key factors the ACSC use to guide the assessment of a cybersecurity incident are used to analyze the case studies. These factors are sensitivity, impact, success, and attribution.[88] These assessment criteria developed by an independent

[86] Shenton, *Strategies for Ensuring Trustworthiness in Qualitative Research Projects*, 72.

[87] Sharon Kolb, "Grounded Theory and the Constant Comparative Method: Valid Research Strategies for Educators," *Journal of Emerging Trends in Educational Research and Policy Studies* 3 (1 January 2012): 85.

[88] Commonwealth of Australia, *Australian Cyber Security Centre 2017 Threat Report*, 24.

Australian government agency further enhance the rigor of the research reduces bias and enhances the dependability of the research.

Sensitivity is determined by who the target or victim is, the data their network holds, and why they may be of interest to a malicious cyber adversary. Impact identifies the tradecraft employed during the attack, what the activity enables on the network, and what security controls might prevent or limit, potential damage. Success refers to whether there are any indications that the malicious activity has been successful and the extent of any potential compromise. Finally, ACSC attempts to determine which adversary is attributed to the activity, what is their intent and makes an assessment of their level of cyberspace capability. [89] These factors enabled the determination of the impact of a comparable cyber attack against the Australian Army's LogIS.

The case studies analyzed were selected to represent the three motivations for accessing a network. The cyberspace attack on the Target Corporation was selected to analyze the intention of breaching confidentiality and stealing data contained in the information system for further exploitation. The initial foothold to enable network access came through a contractor's system, which was an additional reason to include this case study in the research. Stuxnet was included, not only for its complexity and relevancy to the targeting of military infrastructure but because the attack intended to impact the integrity of the data contained within a stand-alone system. Attacks denying the availability of financial and government online services in Estonia in 2007 demonstrated the willingness of adversaries to attack information systems in cyberspace by denying the

[89] Commonwealth of Australia, *Australian Cyber Security Centre 2017 Threat Report*, 24.

availability of networks to achieve political outcomes. These case studies provide purposeful maximal sampling which will portray different perspectives on the problem.[90]

A within-case analysis for each case study is included to provide context and a detailed analysis of the cyberspace attack, this is followed by a cross-case analysis of sensitivity, impact, success, and attribution, as discussed previously. A final category of prevention has been added to identify any processes, training or materiel solutions that have since been implemented to prevent against similar cyberspace threats in the future. The table below facilitates the depiction of the analysis. The tabulated data facilitates the formation of assertions and conclusions for each case study. Extrapolation of information is then possible to facilitate a discussion on comparable attacks in cyberspace against the Australian Army's LogIS.

[90] Creswell, *Qualitative Inquiry and Research Design*, 75.

Table 1. Multiple Case Study Method

Criteria of analysis by category		Definition of Answer
Sensitivity	Target of attack	Who was the target for the attack?
	Motivation of attack	What was the motive behind the attack?
	Data held by the network	What data resided on the network?
	Value of the Network	Why was the network valuable to the adversary?
Impact	Intrusion vector	How did the adversary gain access to the network?
	Actions taken after Intrusion	What actions did the adversary take once access to the network had been established?
	Consequence of Breach	What impact did access to the network by the adversary cause to the target of the attack?
	Security Controls in place	What security measures did the network have to prevent access to the network, and to identify adversarial activity? How effective were these measures?
Success	Duration of Access before detection	How long did the adversary have access to the network before the intrusion was identified?
Attribution	Identity of Attacker	Who was responsible for the attack?
	Intention of Attacker	Why did the attacker choose this target?
	Assessment of Cyberspace Capability	What cyberspace capabilities does it demonstrate?
Prevention	Processes	What Processes have been implemented to prevent reoccurrence?
	Materiel	What Materiel (hardware and software) solutions exist to prevent reoccurrence or to limit the consequences of future breaches?
	Training	What training has been implemented to prevent future cyberspace attacks on the network?

Source: Created by author.

Strengths and Weaknesses

The qualitative case study approach provides strength to this topic from the perspectives of flexibility, data collection from a range of sources, and historical evidence about a social context. Creswell's research does indicate that while there are significant advantages to a qualitative, multi-case study approach, there are also weaknesses relating to the validity, reliability, and over generalization.[91] These weaknesses have been mitigated by the focus on credibility, transferability, dependability, and confirmability as proposed by Guba and Lincoln.

The topic of cyberspace vulnerabilities to military LogIS is narrow in scope. Therefore case studies were selected based on the desired effect on the information held by the information system (confidentiality, integrity, and availability) rather than focusing on specific vector method of an attack through cyberspace. This approach analyzes multiple case studies that are valid and applicable to a hypothetical attack on the Australian Army's LogIS through cyberspace.

Case study selection included consideration of the location of the attack, the adversary responsible for the attack, motivation for the attack, and the period since the attack, to ensure that the data, and the subsequent assessments, are reliable and consistent across contemporary environments. To prevent over-generalizations specific non-subjective criteria were developed to maintain research integrity by preventing the author's bias from interfering with analysis, enabling critical scrutiny.

[91] Creswell, *Qualitative Inquiry and Research Design*, 75-76.

Summary

Using a qualitative approach, through a multi-case study methodology, the researcher aims to provide relevant, and valid analysis on a topic that is under-represented in academic literature. A hypothetical cyber-attack on Australian Army's LogIS is then conducted using the results from the three case studies. The three case-studies cover the different motivations of attack through cyberspace, consisting of confidentiality, integrity, and availability. The research will determine the vulnerabilities of the Australian Army LogIS to a cyber attack, identify potential impacts on Australia's Army operations, and propose prevention methods which will help to bridge current capability gaps and prevent against current vulnerabilities. This methodology enables the study to answer the primary and secondary research questions.

CHAPTER 4

ANALYSIS

> The supreme excellence is not to win a hundred victories. The supreme excellence is to subdue the armies of your enemies without even having to fight them.
>
> —Sun Tzu, *The Art of War*

Introduction

Within the realm of unclassified research, the cyber case studies of the Target Corporation, Stuxnet, and Estonia will be analyzed to identify vulnerabilities specific to military Logistics Information Systems (LogIS) and propose solutions from doctrine, training and materiel perspectives to help protect the Australian Army from these identified vulnerabilities. This case study methodology is used to answer the primary research question, what are the vulnerabilities facing the Australian Army's LogIS within the cyberspace domain?

The four key factors the Australian Cyber Security Centre (ACSC) use to guide the assessment of a cybersecurity incident are used to analyze the case studies. These factors are sensitivity, impact, success, and attribution. A final category of prevention has been added to identify any processes, training or materiel solutions that have since been implemented to prevent against similar cyberspace threats in the future.

Target Corporation Breach, 2013

In November 2013 one of the largest retail companies in the United States was the victim of a successful cyber-attack. The Target Corporation's (Target) networks were compromised by cyber thieves who stole the financial credit and debit card information of 40 million customers[92] and the personal information of an additional 70 million customers.[93] The McAfee Director of Threat Intelligence Operations described the malware as "absolutely unsophisticated and uninteresting."[94] However, the malware did not need to be sophisticated, as long as it was successful.

Sensitivity

The Target Corporation was the objective of the cyber-attack, specifically the financial information collected in the form of unencrypted, plaintext data collected by the corporation as it passed through infected Point of Sale (POS) machines.[95] Online black-market sites then sold the stolen data ranging in price from $6 a piece for a pre-paid gift card to almost $200 for an American Express Platinum card.[96] It appears that there was no ulterior motive other than financial gain for the adversary. This breach is estimated to

[92] Target Corporate, "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," 19 December 2013, accessed 18 January 2018, http://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car.

[93] Target Corporate, "Payment Card Issue FAQ," accessed 18 January 2018, http://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ.aspx.

[94] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," Bloomberg, 13 March 2014, accessed 18 January 2018, https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

[95] Committee On Commerce Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach,* 26 March 2014, 2, accessed 15 January 2018, https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf.

[96] Riley et al., "Missed Alarms and 40 Million Stolen Credit Card Numbers," 5.

have cost the Target Corporation $148 million in actual expenses.[97] Additionally, this breach has cost financial institutions approximately $200 million in reissuing cards without including the cost of the fraudulent activity[98]. It is estimated that one to three million cards sold on the black market for an estimated price of $53.7 million[99]. The financial impact including lost revenue, brand degradation and the loss of consumer trust is unmeasurable. However, Target's profit in the fourth quarter of 2013 dropped 46 percent compared with the year before.[100]

Impact

The cybercriminals in this case study likely undertook reconnaissance initiatives, which identified Target POS systems as vulnerable to the cyber-attack. Electronic reconnaissance would have provided the adversary with a large amount of detail on Target's vendor relationships including a vendor portal and a list of Heating Ventilation and Air Conditioning (HVAC) and refrigeration companies. It is plausible that information regarding Target's use of Microsoft virtualization software, centralized name

[97] Rachel Abrams, "Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop," *The New York Times*, 5 August 2014, accessed 28 January 2018, https://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html.

[98] NBC News, "Target Data Breach Cost for Banks Tops $200M," 18 February 2014, accessed 28 January 2018, https://www.nbcnews.com/business/business-news/target-data-breach-cost-banks-tops-200m-n33156.

[99] Brian Krebs, "The Target Breach, By the Numbers," *Krebs on Security*, 6 May 2014, accessed 28 January 2018, https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

[100] Ibid.

resolution and Microsoft System Configuration Manager (SCCM) was derived from a case study published on the Microsoft website. "The case study describes the Target technical infrastructure, including POS system information, in significant detail."[101]

This reconnaissance led them to identify a refrigeration vendor Fazio Mechanical. Two months before the credit card breach the adversary conducted a spear phishing attack to install malware on Fazio's computer network. The Malware was a derivative of the ZeuS banking Trojan which is a password-stealing bot program. At this stage, the adversary was able to steal the electronic credentials to Target's online vendor portal.[102]

The adversaries were now able to access Target's systems through the stolen credentials through their vendor portal. They were then able to find vulnerabilities in the vendor portal to move laterally through the network. Aorato asserts that it is likely that adversaries overcame Target's network segregation by exploiting a vulnerability in the web application itself. The web application was designed to upload legitimate documents such as invoices, but the application did not have security checks installed to prevent an executable program from being uploaded.[103] The adversary was then able to leverage the information available through the online case study to understand network segregation

[101] Teri Radichel, "Case Study: Critical Controls That Could Have Prevented Target Breach," (Report, SANS Institute, North Bethesda, MD, August 2014), 2, accessed 18 January 2018, https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

[102] Ibid.

[103] Aorato Labs, "The Untold Story of the Target Attack: Step by Step," (Aorato Labs, Herzliya, Tel Aviv, August 2014), 8, accessed 15 January 2018, https://aroundcyber.files.wordpress.com/2014/09/aorato-target-report.pdf.

and vulnerabilities which could be exploited to download Random Access Memory (RAM) scraping malware to POS terminals.[104] To do this, the attackers ran Operating System commands to find the servers within the Target network that hold credit cards and credit card holder's information.

The Active Directory within a network holds all the data on all members of the Domain, including users, computers, and services. There are no privileges or tools required to query the Active Directory. The adversaries used the retrieved service names to infer the purpose of each service. For example, MSSQLSvc/billing server identifies the server which holds billing data for the network. Having identified the servers to be targeted, the adversaries required Domain Admin privileges. The adversaries used a well-known attack called Pass-the-Hash to impersonate a valid user.[105] Cyber-investigative journalist, Brian Krebs identifies that "the internal administrators would use their [Active Directory] log in to access the system from inside."[106]

When users login to a computer, Windows creates an NT hash and records it in the computer's memory. This NT hash facilitates Single-Sign-On (SSO), where users only enter their password during the login process and do not have to enter a password for each application. NT Hash remain in the memory until the server is booted. The adversaries gained access to the NT hashes of the Target Domain Administrator and

[104] Committee On Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach*, 9.

[105] Aorato Labs, "The Untold Story of the Target Attack: Step by Step," 10.

[106] Brian Krebs, "Email Attack on Vendor Set Up Breach at Target," *Krebs on Security*, 12 February 2014, accessed 28 January 2018, https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.

created a legitimate Domain Admin account. The adversaries again hid in plain sight by creating a username which mimicked the username of a legitimate IT application.[107]

At this point in the attack, the adversaries were forced to modify their original plan. The Target network was indeed complying with PCI requirements which meant that Target did not store sensitive authentication data after authorization on a server. Instead, the attackers installed the Kaptoxa malware on all of the POS machines. This malware scanned the memory of the POS machine, and when identifying a credit card, it saved the encrypted Personal Identification Number (PIN) and credit card data to a local file. In order to exfiltrate the credit data obtained by the malware, a remote file share was created using Domain Admin credentials and Windows commands. The files were then sent to the attackers' controlled account using the Windows internal File Transfer Protocol (FTP) client.[108]

Success

At the time of the attack, it was the biggest data breach on record. In 2018, it still ranks as the sixth largest data breach of the 21st century.[109] This ranking is reliant on the number of people affected by the data breach, as opposed to the value of the data itself. Figure 5 provides a timeline of the Target data breach. This timeline is significant in

[107] Aorato Labs, "The Untold Story of the Target Attack: Step by Step", 11.

[108] Ibid., 14.

[109] Taylor Armerding, "The 17 Biggest Data Breaches of the 21st Century," *CSO Online*, 26 January 2018, accessed 28 January 2018, https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

understanding the success of the attack, but more importantly the failure of Target's security systems.

In September 2013, Fazio had its digital security credentials stolen, but the attackers were unable to breach the Target network until November. Installation of the POS and exfiltration malware did not occur until 30, November 2013 and importantly both Symantec antivirus software and First FireEye malware intrusion detection system triggered alerts. "However, Target's security team neither reacted to the alarms nor allowed the FireEye software to automatically delete the malware in question."[110] Department of Justice notified the Target Corporation on 12, December 2013 that after monitoring suspicious credit card charges and payments, Target appeared to be the common factor. It took until 15 December 2013 for Target to remove the malware, and confirm the breach. Adversaries had access to the Target network for a whole month, with exfiltration of data and PII occurring for two weeks.[111]

[110] Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach*, 3.

[111] Ibid., 12.

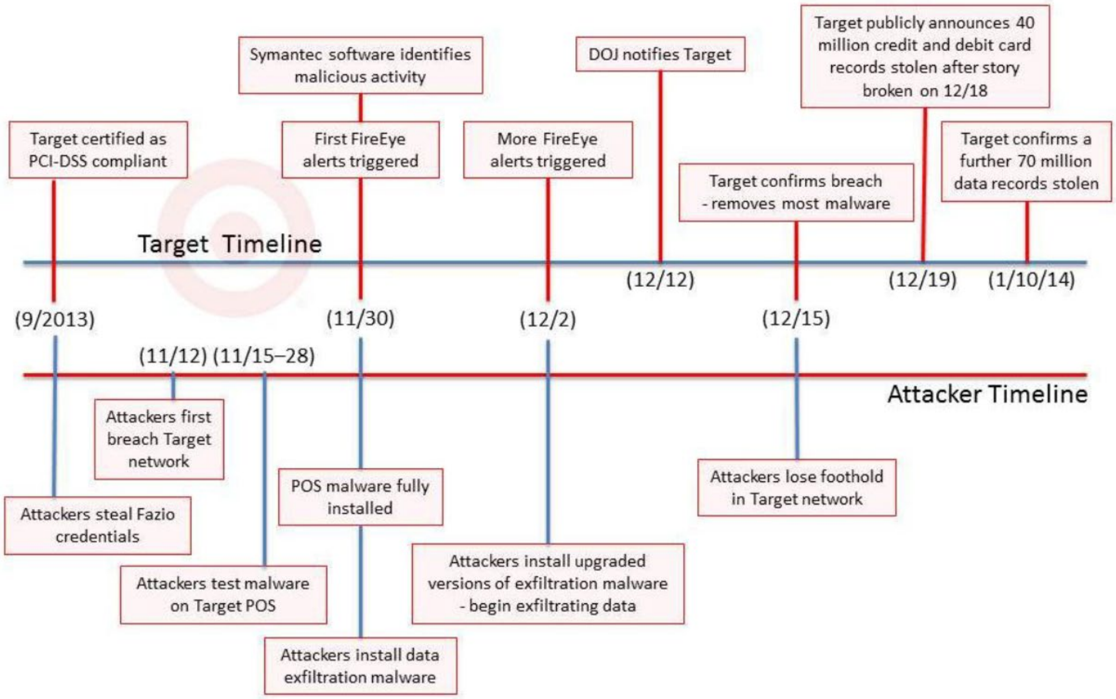

Target publicly announces 40 million credit and debit card records stolen after story broken on 12/18
Symantec software identifies malicious activity
DOJ notifies Target
Target certified as PCI-DSS compliant
First FireEye alerts triggered
More FireEye alerts triggered
Target confirms breach - removes most malware
Target confirms a further 70 million data records stolen
Target Timeline
(12/12)
(12/19)
(1/10/14)
(9/2013)
(11/30)
(12/2)
(12/15)
(11/12)
(11/15–28)
Attacker Timeline
Attackers first breach Target network
Attackers steal Fazio credentials
POS malware fully installed
Attackers lose foothold in Target network
Attackers test malware on Target POS
Attackers install upgraded versions of exfiltration malware - begin exfiltrating data
Attackers install data exfiltration malware

Figure 5. A Timeline of the Target Data Breach

Source: Committee On Commerce Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach,* 26 March 2014, 3, accessed 15 January 2018, https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf.

Attribution

There is very little definitive data available regarding the identity of the adversaries, although theories of attribution point to a cybercriminal network based in Ukraine or the Russian region. Federal law enforcement obtained actual stolen data, which the hackers had left on the dump servers used during the data exfiltration. One password within the malware was Crysis1089. There is a theory that this is a reference to the October 1989 protests that preceded Ukranian independence and the dissolution of the

Soviet Union. Another name embedded within the code is Rescator, though to be a Ukranian cybercriminal who operates numerous sites selling stolen credit card information.[112]

Neither of these pieces of information have led to conclusive evidence as to the identity of the adversary, or any motive beyond cybertheft and associated profits. It is feasible that a non-state actor could fund a similar cyber attack using the cyber skills demonstrated by the criminal underworld. Conversely, as this attack was not sophisticated, it is within the cyber capabilities demonstrated by numerous state actors.

Prevention

Target Chairman, President, and Chief Executive Officer Gregg Steinhafel stated that "Target was certified as meeting the standard for the payment card industry (PCI) in September 2013. Nonetheless, we suffered a data breach." [113]This statement is misleading, Target's security systems complied with PCI, but the corporation failed to act on alerts that would have prevented or mitigated the impact of this attack. There are a number of security recommendations as a result of the study and analysis of the Target data breach including hardening access controls, monitoring of networks and systems, risk mitigation and defense in depth all would have enhanced Target's response to the network incursion and mitigated the data breach.

Networks should monitor profile access patterns enabling a system to identify abnormal and rogue access patterns. Multi-Factor Authentication (MFA) would harden

[112] Riley et al., "Missed Alarms and 40 Million Stolen Credit Card Numbers," 3.

[113] Ibid., 2.

network access controls, although this does not eliminate the risk of credential stealing. Network segregation limits allowed protocol usage and users' excessive privileges. While Network segregation delays an Advanced Persistent Threat (APT), it does not guarantee that an APT will be unsuccessful in securing a foothold in a network. These measures do buy time for the network to identify malware or an APT before it has achieved its objective.[114]

Monitoring networks is an impossibly broad prevention measure, as it appears to be all-encompassing. However, there are specific areas of network monitoring that could inhibit or delay an APT from gaining a foothold in a network. Monitoring users' lists for the addition of new users, especially Domain Administrators is particularly useful in identifying an APT. Security and monitoring of networks should focus on the Active directory as it is involved in nearly all stages of the attack. Anti-Malware and Anti-Virus systems should be valued and installed, but they also need to be monitored by an adequate number of personnel with the required skill sets to be able to distinguish between a legitimate IT process, and malware designed to appear as a legitimate IT process.[115]

The Target "breach makes it clear that PCI compliance, legal and industry mandates do not provide adequate security for sensitive data due to limitations in scope and an ever-changing threat landscape."[116] Instead, a risk management approach to

[114] Aorato Labs, "The Untold Story of the Target Attack: Step by Step", 36.

[115] Ibid., 17.

[116] Radichel, "Case Study: Critical Controls That Could Have Prevented Target Breach," 24.

network security would have analyzed the threats and vulnerabilities of the system as a whole. An inherent understanding of how data, both encrypted and unencrypted flowed throughout the system would have identified areas where data was residing unencrypted, and vulnerable to malware.[117] Risk mitigation includes an assessment of both the value of specific parts of the network combined with the vulnerability of those systems to cyber attacks. "Even though the POS system was one of the most valuable systems, the internet-facing vendor system had a higher risk level. Additional controls on that internet-facing environment may have prevented the attack."[118]

"A security system is only as strong as its weakest link."[119] Target had invested heavily in its network security, as can be seen by the FireEye system. However, because network security was not viewed holistically through a risk management approach, unidentified weaknesses became the Achilles heel of the network. Encryption, whitelisting and security assessments on vendors and third-party service providers would have provided defense in depth, making network incursion and data exfiltration more difficult for the adversary to accomplish in the time available.

"Even though encryption was used, the card data was available in memory at some points on the POS systems. This card data was accessible because hackers were able to infiltrate the network through other vulnerable systems to ultimately access the

[117] Radichel, "Case Study: Critical Controls That Could Have Prevented Target Breach," 9.

[118] Ibid., 10.

[119] Ibid., 7.

POS machines."[120] In this case study, both hardware and software encryption is a factor. At the time of the incident Target still used swipe card readers at its POS, and had not yet transitioned to chip card technology. Updated hardware combined with point to point encryption software would likely have denied or at a minimum delayed access to credit card data.[121] Additional layers of network security such as application whitelisting, where only authorized software is authorized to run on the POS system would have provided another layer of complexity in launching this attack.

Following the data breach, there has been a large amount of academic critique of the security of Target's networks. Less assessment is available on the network security adopted by Fazio. Fazio used a free version of Malwarebytes Antivirus on its network and that this free version does not possess automatic scanning features. This version of the software was inadequate for the business that was using it, leaving Target vulnerable through a third party service provider.[122] From this case study, it is important that contracts which provide third party service providers with access to any part of the network comply with training and minimum software requirements as part of their contractual obligation. Multi-Factor Authentication (MFA) would also have prevented the theft of vendor credentials because the adversary would require access to the physical token. For third-party service providers who require infrequent access to the network,

[120] Radichel, "Case Study: Critical Controls That Could Have Prevented Target Breach," 10.

[121] Ibid., 12.

[122] Krebs, "Email Attack on Vendor Set Up Breach at Target."

emphasis on segregation of the Target network reinforced by defense in depth would have inhibited the attack.[123]

Implications for LogIS

The cybercriminals in the attack on Target disguised malicious components of malware as legitimate. In this way they were often able to hide in plain sight, making the intrusion more difficult for network monitoring to identify the actions of the APT as malicious.[124] This point is especially salient for military LogIS as they have interfaces with unclassified networks to communicate with trusted service providers and third-party providers. This interface makes LogIS vulnerable to the security of networks outside of the Australian Army's control. These interfaces make LogIS a 'weak link' that adversaries might use to establish a foothold and gain access to the Defence Protected Network as a whole for espionage purposes.

"The use of an uploaded file to subvert a web application has been documented to be a popular penetration method among the attackers."[125] This method of intrusion is not isolated to the Target attack and has been pivotal in previous attacks such as the attack against security vendor Bit9.[126] LogIS will rely on the upload of documents

[123] Radichel, "Case Study: Critical Controls That Could Have Prevented Target Breach," 18.

[124] Aorato Labs, "The Untold Story of the Target Attack: Step by Step", 9.

[125] Ibid.

[126] Ibid.

including inventories and invoices. However, this requirement is a vulnerability of LogIS and monitoring for exploitation potential is essential.

Personnel operating computer networks are arguably the weakest link in network security. This statement also includes network security personnel who can monitor systems, identify abnormal traffic or behavior and respond accordingly. The human reaction was lacking in response to indications of a cyber-attack in this case study. For network monitoring to be effective, it needs to be made a priority and resourced relative to the risk.

Cyber hygiene practices were poorly understood by network operators who used their active directory login to access the system from inside. This vulnerability was exploited by the adversaries using pass the hash techniques. Conducting an assessment of the convenience of single sign-on procedures against the ability of an adversary to exploit this to gain a foothold within the network is essential.

Stuxnet, 2010

The Stuxnet worm was discovered in 2010 and is the first known instance of a cyber-attack resulting in physical damage. The worm was a complex and sophisticated attack unofficially attributed to state actors, the United States of America and Israel. It aimed to disrupt and delay Iranian nuclear enrichment by targeting specific Siemens Supervisory Control and Data Acquisitions (SCADA) systems as a subset of Industrial Control Systems (ICS). The Stuxnet worm may have destroyed 1,000 centrifuges at Natanz, about 11 percent of centrifuges installed at this time.

Sensitivity

No one has ever claimed responsibility for Stuxnet and Iran has been hesitant to fully disclose the impact of Stuxnet on its nuclear enrichment program. Therefore, available information comes from analysis of the worm after its discovery. Analysis of the malware revealed that “Stuxnet was designed to target a very specific set of programmable logic controllers (PLCs) that are only designed by two countries in the world: Finland and Iran.”[127]

Stuxnet aims to identify those hosts which have the Siemens Step 7 software installed. When Symantec analyzed the percentage of infected hosts by country, it revealed that 67.60 percent of infected hosts were in Iran. Other infected countries included 8.10 percent in South Korea, 4.98 percent in America, 2.18 percent in the United Kingdom, 2.18 percent in Indonesia, 1.56 percent in Taiwan, 1.25 percent in India and all other countries amalgamated to 12.15 percent[128]. The disproportionate number of infected hosts in Iran provides further evidence that Iran was the target of the attack.

In addition to the above, the Stuxnet worm is very specific about the types of SCADA systems it targets. Stuxnet only targets facilities with a particular physical layout, known as a cascade. Publicly available photos of Iranian President Ahmadinejad visiting Natanz on April 8, 2008, inadvertently show a centrifuge cascade. This structure

[127] Irving Lachow, “The Stuxnet Enigma: Implications for the Future of Cybersecurity,” *Georgetown Journal of International Affairs* (Fall 2011): 120.

[128] Nicolas Falliere, Liam O Murchu, and Eric Chien, “W32.Stuxnet Dossier” (Report, Symantec, Cupertino, CA, February 2011), 6, accessed 4 February 2018, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

matches the Stuxnet code exactly.[129] One section of code targets systems where 984 machines are linked together. In 2009, the IAEA inspected 984 machines[130], providing additional weight to the argument that the primary target was Iran's nuclear enrichment facility in Natanz, although some experts believe that the Bushehr plant was also a target.[131]

Accepting that Iran's Natanz uranium enrichment facility was the intended target of the attack, most researchers agree that the cyber-attack was politically motivated. United Nations Security Council Resolutions between 2006 and 2008 demanded that Iran suspend uranium enrichment and reprocessing, and submit to additional safeguards. International Atomic Energy Agency (IAEA) were unable to rule out a weapons program.[132] Iran maintains that its nuclear program is entirely peaceful. However, in 2002 Iran was forced to admit it had constructed facilities for fuel enrichment and heavy water production[133]. The worm aimed to delay this process by damaging the centrifuges used by Iran to enrich uranium. There is cause for speculation that this was to enable

[129] Paul Mueller and Babak Yadegari, "The Stuxnet Worm" (Report, University of Arizona Computer Science Department, Tuscon, AZ, 2012), 1, accessed 26 January 2018, https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf.

[130] William J. Broad, John Markoff, and David E. Sanger, "Stuxnet Worm Used Against Iran Was Tested in Israel," *The New York Times*, 15 January 2011, accessed 4 February 2018, https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[131] Lachow, "The Stuxnet Enigma," 122.

[132] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (July 2013): 379.

[133] Mueller and Yadegari, "The Stuxnet Worm."

America to pursue diplomatic and economic means to deter Iran from producing nuclear weapons.[134]

Impact

Stuxnet was unprecedented in its technical complexity and sophistication. It made use of four zero-day vulnerabilities and used rootkits to hide from users and anti-malware software on Windows and the SCADA targets. It employed two stolen digital certificates, and the size of the worm was 500 kilobytes as opposed to the usual 10 to 15 kilobytes.[135] "The creators were able to implant the worm on computers that were almost certainly not connected to the Internet, and they were able to mask its presence even while it was modifying the signals that the industrial control systems were sending." [136]

One of the important aspects of Stuxnet as a cyber-attack is that the SCADA systems operating in Natanz were 'air-gapped.' Computers that were infected had no public internet connection. Analysts of the code have determined that an intermediary device, most probably a USB stick was used to gain an initial foothold and establish control.[137] Stuxnet exploits a zero-day vulnerability to scan the contents of the USB. It then downloads a large, partially encrypted file onto the computer, and works to exploit

[134] Broad, Markoff, and Sanger, "Stuxnet Worm Used Against Iran Was Tested in Israel."

[135] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired Magazine*, no. 11 (2011): 8.

[136] Isaac R. III Porche, Jerry Sollinger, and Shawn McKay, "A Cyberworm That Knows No Boundaries" (Report, RAND, Santa Monica, CA, 2011), ix, accessed 23 September 2017, https://www.rand.org/pubs/occasional_papers/OP342.html.

[137] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 24.

further zero-day vulnerabilities to spread to other computers on the network. Stuxnet used stolen valid signed digital certificates from RealTek Semiconductor, a hardware maker in Taiwan and JMicron Technology, a circuit maker in Taiwan.[138] These certificates help the worm to avoid detection from anti-virus an anti-malware software, by deceiving operating systems that the Stuxnet worm is a legitimate program

Stuxnet actively searches for computers running Siemens WinCC. It spreads by using windows shared folders to propagate itself over local networks and through a print spooler zero-day vulnerability, enabling Stuxnet to infect remote machines[139]. The Stuxnet worm employed Siemens' default passwords to access the Windows Operating system that runs the WinCC and Siemens SIMATIC Step7 programs. These are Programmable Logic Controller (PLC) programs that manage industrial plants. Stuxnet was designed to penetrate through firewalls and into machines that would not have connections to the internet.

Once Stuxnet infected a SIMATIC machine it verified the configuration of the PLC in the network. The configuration specifications matched the Iranian Natanz exactly. It then instructed the PLC to speed up and slow down, at speeds outside the design parameters of the centrifuge. While this process was occurring, Stuxnet provided feedback to the SIMATIC operator that the centrifuges were spinning normally.[140]

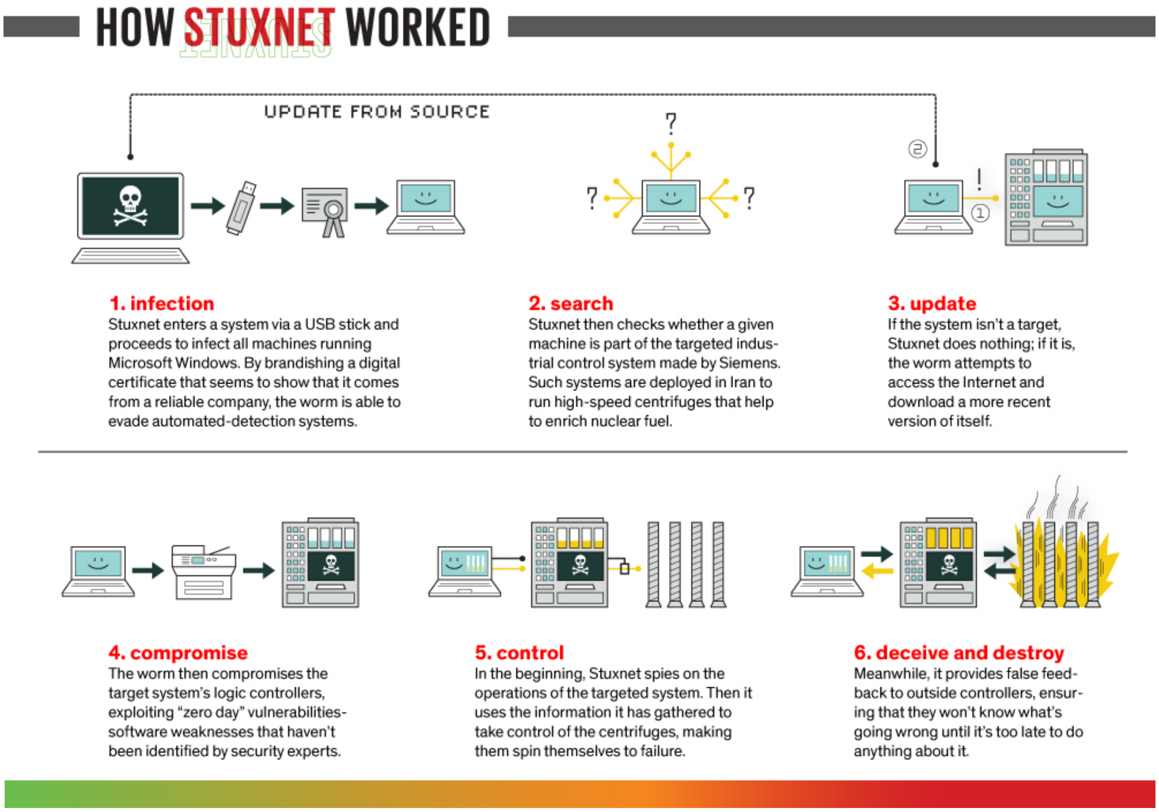
[138] Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," 4.

[139] Mueller and Yadegari, "The Stuxnet Worm," 5.

[140] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 384.

"The attacker cause[d] the defenders to spend valuable time trying to determine the reason for the decrease in their equipment's production. The infiltration create[d] uncertainty in the minds of the defenders about their ability to pull off the complex task of enrichment."[141] Figure 6 provides a depiction of the steps taken by Stuxnet to gain network access, exploit the network and achieve physical destruction.

[141] Lachow, "The Stuxnet Enigma," 121.



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Figure 6. How Stuxnet Worked

Source: David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum: Technology, Engineering, and Science News*, 2, 26 February 2013, accessed 25 January 2018, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Stuxnet was designed to remain concealed for a long duration. It installed rootkits on the infected Windows computers to hide its files. A relatively small antivirus firm in Belarus, VirusBlokAda discovered Stuxnet. One of their Iranian clients consulted with them as their machine was continually rebooting itself. This consultation led to the investigation of malware, later named 'Stuxnet' based on a filename in the code. VirusBlokAda reported the zero-day vulnerability they had identified to Microsoft, and they went public before Microsoft released the security patch.[142] "Despite its relative sophistication, Stuxnet was quickly and effectively disarmed."[143] Symantec initiated an investigation and revoked stolen digital certificates, and released security patches. Collaboration amongst the cybersecurity network has led to the Stuxnet kill chain being reverse engineered, although some elements of the Stuxnet worm remain a mystery.[144]

Success

As it is likely that Stuxnet was a state-sponsored attack against a secret Iranian facility, neither the attacker nor the defender have published a detailed timeline of the attack. What information is known has been determined by analyzing the Stuxnet code, Stuxnet was discovered and observed predominantly in 2010. However, reports indicate that versions of Stuxnet had been operating on Iranian computers as far back as 2009 without detection,[145] some researchers argue that versions of Stuxnet could have been in place since 2006.[146]

[142] Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History."

[143] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 27.

[144] Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History."

[145] Ibid.

[146] Michael J. Assante and Robert M. Lee, "The Industrial Control System Cyber Kill Chain" (Report, SANS Institute, North Bethesda, MD, October 2015), 17, accessed 4 February 2018, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

Publicly Iran has downplayed the significance and impact that Stuxnet has had on Iran's nuclear enrichment program. However, the IAEA is required to inspect any decommissioned, damaged or otherwise unusable centrifuges at the Natanz enrichment plant. This data provided researchers with an indication of the physical impact of Stuxnet. When conducting normal operations, Iran replaced up to 10 percent of its centrifuges a year, usually due to material defects and other issues. This percentage equates to 800 centrifuges decommissioned during a year. When IAEA reviewed footage from the cascade rooms monitoring Iran's enrichment program they estimated that 1,000 to 2,000 centrifuges were swapped out over a few months.[147]

These assessments indicate the physical impact that Stuxnet had on the centrifuges at Natanz; there is no data to analyze the psychological impact of Stuxnet in the confidence of data held within the Iranian uranium enrichment community. David Sanger reported in the New York Times that the initial attacks caused confusion at Natanz. However, as the attacks persisted this reportedly led to mistrust in the digital control systems with the IAEA reporting that "the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw."[148]The impact of Stuxnet was much more than the physical degradation of centrifuges. The mistrust and lack of confidence in the control systems resulted in

[147] Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," 1.

[148] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, 1 June 2012, 6, accessed 4 February 2018, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

personnel fired from the project, this contributed to the success that Stuxnet accomplished by achieving a delay in the Iranian uranium enrichment project.[149]

Attribution

"Although the authors of Stuxnet haven't been officially identified, the size and sophistication of the worm have led experts to believe that it could have been created only with the sponsorship of a nation-state."[150] These indicators combined with leaks to the press in both America and Israel, lead most researchers to attribute the attack to these countries. David Sanger asserts in the *New York Times* that Stuxnet was part of a sustained US cyber campaign against the Iranian nuclear program known as Olympic Games.[151]

Collaboration with Israel was essential to the development and execution of Stuxnet. America needed access to Israeli clandestine intelligence networks already operating in Iran and wanted to dissuade Israel from launching kinetic air strikes. Theories postulate that rehearsals for the attack occurred at Israel's Dimona nuclear facility.[152] However, attribution has been unable to be confirmed, and critics assert that "one must consider the possibility that the creators of the Stuxnet worm may have planted

[149] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," 6.

[150] Kushner, "The Real Story of Stuxnet," 2.

[151] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," 6.

[152] Ibid.

‘clues’ in an attempt to deliberately mislead analysts who would attempt to attribute the attack.”[153]

The discovery of Stuxnet has taken the concept of cyber-attacks sponsored by nation-states from the realm of possibility to reality, while at the same time providing nation-states with plausible deniability. “States are capitalizing on technology whose development is driven by cyber crime, and perhaps outsourcing cyber attacks to non-attributable third parties.”[154] After Stuxnet, it is unsurprising that Iran announced its cyber unit capable of offensive operations in 2011. Brigadier General Gholamreza Jalali, chief of Iran’s Passive Defense Organization at the time, declared that Iran could fight its enemies in cyberspace.[155]

Stuxnet was the most advanced piece of malware at the time it was launched and was the first to cause physical destruction. America had been concerned about the protection of critical infrastructure in the cyberspace domain as early as May 1998. Stuxnet demonstrated the capability and potential magnitude of future cyber-attacks. Security vendors, researchers and control systems experts could no longer assess a cyber-attack as improbable or unlikely.[156] As such a publicized event, Stuxnet provoked the investment into cyberspace as a warfare domain. Up until this point the digital domain

[153] Lachow, “The Stuxnet Enigma,” 119.

[154] Farwell and Rohozinski, “Stuxnet and the Future of Cyber War,” 24.

[155] Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran.”

[156] R. M. Lee, “The History of Stuxnet: Key Takeaways for Cyber Decision Makers” (Report, Armed Forces Communications and Electronics Association, Washington, DC, 2012), 11.

had been seen as a combat multiplier, enhancing the ability to communicate and analyze information. Stuxnet identified significant vulnerabilities to information systems including those internal and external to Defense.

Prevention

Given that attribution has not been confirmed, and Iran is not forthcoming with information regarding its inherent security measures or processes it had in place at Natanz it is difficult to make accurate assessments on areas of cyber security which would have prevented the Stuxnet attack from being effective. However, given the intrusion vector was reliant on the people using USBs to infect the network, "policymakers need to assume that even air-gapped networks will be breached, and must have technologies, processes, and training in place to deal with this eventuality."[157] Training for users, including contractors on the cyber hygiene requirements for users of networks, is essential in preventing cyber-attacks.

Stuxnet attacked a specific centrifuge configuration indicating that the reconnaissance conducted by the developer of Stuxnet was thorough. The protection of information regarding network configuration is critical to network security. Media releases and photographs may contain information that is inherently valuable to a technical adversary conducting network reconnaissance, although the data appears benign when approved for release by non-technical personnel.

[157] Lachow, "The Stuxnet Enigma," 124.

Implications for LogIS

LogIS routinely bridge the gap between unclassified networks and the Defence Protected Network (DPN). The ability of Stuxnet to cross the air gap has security implications for Australian Army LogIS. Cyber hygiene training focusing on ways to transfer data safely and to mitigate the risks associated with USBs and CD ROMs, is essential for individual users of LogIS.

Logisticians rely on the accuracy of the data residing in the LogIS that are used to conduct day to day operations. This case study highlights a way in which a cyber-attack can interfere with the integrity of the data contained within a system. A data integrity attack on LogIS would take a lot of time to unravel, and amplify trust deficits which inherently exist between combat operators and logisticians.

The Stuxnet attack utilized an unprecedented number of zero-day vulnerabilities in software and operating systems. For the Australian Army, the use of a Commercial Off The Shelf (COTS) product such as SAP, exposes the LogIS to an increased level of risk. The number of high profile NATO countries which also use the SAP platform for their LogIS amplifies the risk. It is likely that the payoff would be high for an adversary that can identify and exploit a zero-day vulnerability within the SAP software.

Estonia, 2007

In 2007, amid political unrest between Estonians and ethnic Russians Estonia found itself the victim to an unprecedented Distributed Denial of Service (DDoS) cyber-attack. The first strike commenced on 27 April 2007 and focused on denying the availability of important Estonian websites, including political parties, the president and parliament's websites, and the Estonian Police. The attack was then expanded to include newspaper outlets such as Postimees. Hackers also defaced individual websites, and promulgated pro-Russian propaganda, in support of information operations. The attack peaked on

9 May 2007 with targets now including banks and universities. The attacks persisted through until midnight 18 May 2007 when they ceased as abruptly as they started.[158] The attack on Estonia was "the first widespread distributed-denial-of-service (DDoS) attacks to target the government and key services and industries of a nation-state and, as a result, they are frequently referred to as the first cyber war."[159]

Sensitivity

At the time of the attack, Estonia was one of the newest additions to the North Atlantic Treaty Organization (NATO) becoming a full member on 29 March 2004.[160] It is a relatively small country of 45,000 square kilometers with a population of 1.3 million people bordering Russia. It was occupied by Nazi Germany in World War II and liberated by the Soviet Union at the conclusion of the war. The Soviet Union continued to occupy and control Estonia until they peacefully recognized Estonia's independence on

[158] Cyrus Farivar, *The Internet of Elsewhere: The Emergent Effects of a Wired World* (New Brunswick, QC: Rutgers University Press, 2011), 138.

[159] Alison Lawlor Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 69.

[160] North Atlantic Treaty Organization, "Member Countries," accessed 20 February 2018, http://www.nato.int/cps/en/natohq/topics_52044.htm.

6 September 1991, although withdrawal of Russian troops was not complete until 1994.[161]

Estonia possesses strong electronics and telecommunications sectors. At the time of the attack, 40 percent of the population read their newspaper online, 90 percent of bank transactions were completed using the internet, and the country had initiated electronic voting.[162] In 2007, 66 percent of Estonians had access to the internet, one of the highest percentages in the world at the time. This focus on electronic commerce and telecommunications explains the method of attack, but history and political upheaval provide the motivation for the attack.

"After Estonian independence was reestablished in 1991, Estonia was an ethnically, linguistically and culturally divided society."[163] 68 percent of Estonia's population are ethnic Estonians, and 25 percent are ethnic Russians, resettled in Estonia after World War II during the occupation by the Soviet Union.[164] These underlying conditions escalated into instability and unrest, triggered by a political decision to move a bronze statue memorializing the 'Liberators of Tallinn.' The statue commemorated the USSR's war dead, erected in 1947 in Estonia's capital, Tallinn city park. "To the ethnic Russians…the statue symbolizes the bravery of their countrymen and the liberation of the

[161] Russell, *Cyber Blockades*, 71.

[162] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, 21 August 2007, accessed 18 February 2018, https://www.wired.com/2007/08/ff-estonia/.

[163] Russell, *Cyber Blockades*, 73.

[164] Ibid., 71.

Soviet Union. To Estonians, the statue is yet another painful reminder of the vicious history that has long-divided these two groups."[165]

"On April 23, 2007, Russia issued an official protest and warned of 'most serious consequences for relations between Russia and Estonia' if the plans to move the monument proceeded."[166] On April 26, 2007, the Estonian government began relocating the monument. This action immediately triggered protests from ethnic Russians, which increasingly turned violent resulting in one death, dozens injured and hundreds arrested.[167] Coinciding with the protests and civil unrest, the cyber-attack on Estonia also commenced preventing the government from communicating with their people, contributing to the fear and confusion.[168]

Impact

The literature on the Estonian attack asserts that there were three types of attacks employed by attackers to achieve the DDoS attacks. The first wave of attacks was the least sophisticated and began at dusk on April 26. They are assessed as emotionally fueled and organized in concert with the physical riots and violence occurring at the time.[169] These attacks involved 'script kiddies,' an appeal for ethnic Russians to

[165] Farivar, *The Internet of Elsewhere*, 136.

[166] Russell, *Cyber Blockades*, 75.

[167] Farivar, *The Internet of Elsewhere*, 136.

[168] Russell, *Cyber Blockades*, 89.

[169] Dimitar Kostadinov, "Estonia: To Black Out an Entire Country*" InfoSec Institute*, 1 October 2013, 7, accessed 19 February 2018, http://resources.infosecinstitute.com/estonia-to-black-out-an-entire-country-part-one/.

download scripts from the internet which overwhelm web servers using ping attacks. Government websites, including those of the President and Prime Minister and several daily newspapers, were inaccessible due to this attack.[170]

The second attack involved the use of botnets. The attack included the use of over a million computers infected with malware as part of a botnet attack. A handful of people controlled the attack who used master computers to send commands to the legions of bots, often without the knowledge of the individual computer user.[171] The botnet attack sent overwhelming amounts of data to Estonian computer systems in a DDoS attack. This attack flooded the targeted systems and forced them to shut down. These types of attacks peaked on 9 May 2007 with Estonian networks inundated with an average of four million packets of data per second, a two-hundred-fold surge. This type of attack forced Hansabank, the largest bank in Estonia to shut down its online services for a number of hours and then closed all services to customers outside the Baltic states.[172]

The final attack involved hackers, who were able to orchestrate the attack to achieve the desired impact. They were able to "infiltrate individual websites, delete legitimate content, and post their own messages."[173] This attack included posting a fake letter of apology from the Prime Minister, apologizing for the removal of the statue. While the script and botnet attack vectors were effective, they required little human

[170] Russell, *Cyber Blockades*, 75.

[171] Farivar, *The Internet of Elsewhere*, 137.

[172] Kostadinov, *Estonia*.

[173] Davis, "Hackers Take Down the Most Wired Country in Europe."

oversight once the attacks commenced. Hackers posed more of a threat as they were able to adapt to the Estonian defensive measures initiated in response to the attacks.[174]

The Estonian government was able to implement a number of defense measures to mitigate the impact of the cyber-attacks. Before the attacks began, Estonia's Computer Emergency Response Team (CERT) had erected firewalls around government websites and established additional computer servers and alerted key staff. CERT initiated these preparations as experience had taught them "if there are fights on the street, there are going to be fights on the internet."[175]

Once the attacks started, the first response was to limit or prohibit international traffic; this enabled servers to remain operational but limited the services to users within Estonia.[176] Coincidentally there was a meeting of European network operators and 'the vetted' meeting in Tallinn at the time of the attack. 'The vetted' are individuals who are trusted by the largest ISPs. They have the influence to be able to remove computers from ISP networks. Estonia's CERT was able to meet with members of 'the vetted' and gain their support and advice in responding to the DDoS attack.

The government was able to help limit the impact of these attacks and return services to normal in a minimal amount of time by addressing what CERT identified as a fundamental design flaw. Instead of pulling data from a single database source in

[174] Scott A. Cain, "The Net Is Down, Now What Do We Do? Is The Air Force Prepared To Survive A Cyber Attack" (Thesis, School of Advanced Air and Space Studies, Maxwell Air Force Base, AL, June 2009), 39, accessed February 24, 2018, http://www.dtic.mil/docs/citations/ADA540670.

[175] Russell, *Cyber Blockades*, 79.

[176] Cain, "The Net Is Down, Now What Do We Do?" 40.

response to every request, they created back-end databases that stored caches of the website that could better manage floods of requests for the same data.[177] Most websites that were affected by the 'kiddie scripts' were able to be operational again within seventy-two hours.

Success

The DDoS attacks on the Estonian internet infrastructure lasted for twenty-two days, preventing the government from responding to a political crisis and causing a significant impact on daily life.[178] The potential of some of the attacks was catastrophic, but limited in short duration. For example, the telephone exchange was completely unusable for over an hour threatening emergency response services and bank services being inoperable for over an hour. The prolonged duration of other elements of the attack only caused inconvenience to the population. These attacks included the inability to withdraw money, pay for fuel, or use mobile telephones.

The DDoS attacks on Estonia were successful in achieving a psychological impact on the Estonian public and enhancing political unrest which was occurring at the time. However, if they intended to cause a complete shutdown of the cyberinfrastructure in Estonia, then they fell short of achieving that end state. The consequences of the attack could have been worse. "The 2007 attacks did not damage much of Estonian IT infrastructure because they were not sophisticated, and also because the limited size of the country allowed its cyber experts to take speedy defence measures for national

[177] Russell, *Cyber Blockades*, 79.

[178] Ibid., 78.

networks."[179] The identification of the cyber-attack occurred immediately and the government response to mitigate the effects was swift. However, the attacks revealed the vulnerabilities of digital communications networks and forced the world to look at the legal implications of cyber warfare and improve cybersecurity technology and policy.

Attribution

Estonia was quick to accuse the Russian government of coordinating and funding the cyber-attacks, due to the political tensions between the two countries at the time. Instructions for the 'script kiddies' attack were available through Russian-language online forums and server logs showing that attacks originated in Russia and possibly the Kremlin itself. Unfortunately, falsification of server logs, IP addresses, traceroutes and other digital forensic evidence is relatively easy. The Russian government has repeatedly denied its involvement in the attack and the arrest of a nineteen-year-old Estonian citizen, and ethnic Russian named Dmitri Galushkevich who confessed to attacking government computer networks complicates attribution.[180] Russia refused to cooperate in the investigation of the attack, limiting any further arrests.

Estonian foreign minister, Urmas Paet has publicly claimed that the IP addresses involved in the attack were inside Russian government institutions, including the President's administration.[181] Suspicions exist that Russian criminal and business

[179] Vincent Joubert, "Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?" (Research Paper, NATO Defense College, Rome, May 2012), accessed 18 February 2018, https://www.files.ethz.ch/isn/143191/rp_76.pdf.

[180] Farivar, *The Internet of Elsewhere*, 139.

[181] Russell, *Cyber Blockades*, 77.

networks were responsible for distributing and controlling the botnets that infected computers involved in the attack. The duration and intensity of the botnet attack on Estonia indicate that these ‘herds of botnets’ were ‘rented.’ The Russian Business Network (RBN) has been involved in previous rented botnet attacks, making this claim plausible. A Russian publication *‘Hacker’* denies that the Russian government coordinated the attack, and instead asserts that national pride, not financial gain motivated the botnet attack.[182]

Prevention

There are only a few measures that can be taken to prevent a DDoS attack in cyberspace. There are also a few measures that can be taken to mitigate the impact of a DDoS attack, such as those taken by the Estonian CERT in response to the attacks in 2007. One of the key themes is to ensure that there is network redundancy included in the network architecture and design. Locating servers in different data centers, ensuring data centers are located on different networks, and reducing bottlenecks and single points of failure within the network and data centers help to achieve network resiliency.

Load balancers can also be used to distribute traffic across multiple servers within a network. The combination of load balancers and firewalls enable operators to close connections and prevent network traffic from exceeding thresholds. A short-term solution is to have a large amount of bandwidth available to absorb a volumetric attack for a short period, allowing network operators time to respond while ensuring that services are not interrupted. Additionally, a cloud-based anti-DDoS filter can be installed to divert DDoS

[182] Russell, *Cyber Blockades*, 77.

attacks.[183] None of these solutions would have prevented the DDoS attack on Estonia, but they would have reduced the impact and duration of the attack.

Implications for LogIS

LogIS are vulnerable to a DDoS style of attack, whether from a simplistic ‘script kiddies’ attack or a botnet attack. Importantly these attack vectors are difficult to defend against and can be launched with minimal resources at the time of the adversaries choosing. As military supply chains have become focused on achieving commercial best practice of Just In Time (JIT) logistics, there is less flexibility and redundancy to mitigate the impact of a DDoS attack synchronized with kinetic attacks.

Military forces may be unable to limit or prohibit IP addresses from the host nation as its own forces will be operating from the same country as the adversary. Assuming that a DDoS attack would be launched in concert with kinetic effects to achieve multi-domain battle effects, it would inhibit the responsiveness and flexibility of the logistic supply chain and would decrease the operational reach of combat forces thus impacting their sustainability and survivability. While the Estonian attack was relatively short in duration if timed to best effect the adversary can achieve a disproportional effect on the Australian Army’s ability to wage war particularly from the viewpoint of conventional offensive operations.

[183] Paul Ferrillo, “Defending Your Network Against DDoS Attacks,” *Tripwire*, 23 February 2016, accessed 24 February 2018, https://www.tripwire.com/state-of-security/security-awareness/defending-your-network-against-ddos-attacks/.

Australian Army LogIS

A cyber-attack on Australian Army LogIS has not occurred. However, this case study will apply the information extrapolated from the case studies above to discuss the sensitivity, impact, success, attribution and prevention aspects of a hypothetical cyber-attack on Australian Army LogIS. The hypothetical case study outlined below will discuss the ways confidentiality, integrity or availability cyberattacks could impact Australian Army LogIS using malware, zero-day exploits and DDoS to achieve the intention of the attack.

Sensitivity

In Australian Army doctrine, it states "The ability of a logistic asset to continue to operate in support of the commander's plan is integral to the success of that plan. Logistic installations, units and information systems are high-value targets."[184] Due to the relative importance of logistics in the conduct of war, the information contained in LogIS is valuable to the enemy. As outlined in chapter 2, Singer and Friedman propose that "there are only three things you can do to a computer: steal its data, misuse credentials, and hijack resources."[185] LogIS are vulnerable to all three motives for a cyber-attack.

Data stored in information systems can provide valuable information on the location and capabilities of units. An adversary can use this information to inform a coordinated kinetic attack on tactical units or commercial logistics providers, preventing

[184] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Combat Service Support*, 22.

[185] Singer and Friedman, *Cybersecurity and Cyberwar*, 39.

replenishment to the operational theatre. Adversaries demonstrated this vulnerability through the reconnaissance conducted before the cyber-attack against the Target Corporation case study.

Efficient and effective logistics at the tactical and operational levels of war is reliant on accurate data. This data resides in LogIS. A cyber-attack that alters the integrity of the data held within LogIS can have a disproportionate effect on the logistics support to military operations. An overwhelming number of demands placed within a supply system would make it very difficult for the Australian Army to differentiate between legitimate demands and those raised by an adversary. Modifying maintenance records for helicopters, for example, would cause mass confusion and potentially result in aircraft becoming operationally grounded until the accuracy of data could be assured.

Data integrity and trust in information systems is a key component in achieving efficient logistics systems. Contemporary Just In Time (JIT) logistics techniques are reliant on accurate information held in information systems. Like the scientists in the Iranian Uranium enrichment facilities, any trust deficit in the relationship between the operators and their information systems results in a return to manual processes and subsequent inefficiencies, negating benefits currently realized by digital systems.

Denial of service attacks to LogIS will impact the efficiency of logistics support. Denying the availability of LogIS, such as SAP would prevent access to maintenance records and stockholdings, upon which logisticians have come to rely. This tactic would, in turn, prohibit and inhibit logistics operations at both the tactical and operational level. A DDoS attack on the Logistics Information System itself would prevent the reordering and movement of stock to meet demands at the right place and right time.

While the Estonian DDoS attacks had no long-term impact, the short-term inconveniences felt by people not being able to conduct normal financial transactions could prove catastrophic in military logistics operations. At a tactical level of war, during high-intensity conflict against a near-peer enemy, the stockholding of ammunition and fuel, for example, is constrained to 2-5 days of supply. A DDoS cyber-attack preventing the resupply of these commodities would result in land operations reaching their culmination point and limiting their operational reach.

Impact

Confidentiality and integrity cyber-attacks occur using malware and zero-day vulnerabilities to gain a foothold in the targeted network. Availability motives can be accomplished through the employment of botnets to overwhelm the network. These methods were used in the case studies outlined above, and are likely to achieve the desired cyber-attack effect against Australian Army LogIS in the cyberspace domain.

Malware can be used by adversaries both to access a targeted network and to achieve either confidentiality, integrity or availability outcome within networks. LogIS are vulnerable on all fronts. Malware is malicious software developed by an adversary, to exploit vulnerabilities in specific networks, software or operating systems. In order to develop the malware, adversaries must conduct reconnaissance on the targeted network architecture and users of the network.

The Defence Secret Network (DSN) is an air-gapped system, but as demonstrated by Stuxnet, this does not make it impervious to malware as an attack vector. The Defence Protected Network (DPN) is not air-gapped, and as users of the DSN are also users of the DPN, there are multiple vulnerabilities for malware to exploit. These vulnerabilities include users who use the same password on both systems and poor cyber hygiene practices used by users of both systems who use removable storage devices including CDs, DVDs, and USBs to transfer data between systems to overcome the air gap for legitimate reasons.

Logisticians regularly work with commercial logistics providers outside of the Department of Defence. These contacts and the required sharing of information increase the risk of malware transferring from e-mail or removable storage to the DPN. Logistics programs reside on both the DPN and the DSN and information transfer is required, but not facilitated by a formal process. Removable storage devices increase the potential for malware to be introduced by the internet, e-mails or macros onto the DPN and transferred to the DSN. This process is similar to the initial foothold established in the attacks against the Target Corporation, and the spread of Stuxnet by removable storage devices.

Malware can also target specific users of networks through spear phishing attacks, watering holes, and malvertising. The Australian Army newspaper, and social media websites all routinely publish photos of current serving members, often including their names below the images. In this way, it would be relatively easy for adversaries to identify key leaders within Australian Army logistics organizations to be targets of phishing campaigns. Similarly, media releases and articles regularly identify key contractors and commercial logistics providers to the Australian Defence Force making reconnaissance relatively easy.

Once reconnaissance is complete, a phishing campaign would begin. Australian Army logisticians would open e-mails that appear to be from trusted organizations such as Linfox or BAE as they are a known Defence contractor. It is unlikely that individual users would check to determine if the hostname within an e-mail address was correct, as long as it was similar. Reconnaissance could also identify frequently visited internet sites such as DHL, Toll Group, and Linfox and insert malvertising to install malware onto DPN terminals. While malware and anti-virus software monitor and protect the DPN, malware is becoming more sophisticated, and it can camouflage itself as legitimate software and avoid detection. Malware has increasingly used stolen credentials and digital certificates as demonstrated through both the Target and Stuxnet case studies to avoid detection by network monitoring systems.

Like all software programs, LogIS are susceptible to zero-day-vulnerabilities. While patches are released by software developers to remedy zero-day vulnerabilities, they are often released after an adversary has exploited the vulnerability elsewhere. Networks and information systems are protected by cyber-hygiene practices which include installing patches and upgrades as soon as they are released.

A COTS Logistics Information System, such as SAP is an improvement on the previous software platform, MILIS used by the Australian Army. Bespoke information systems such as MILIS have very few users. Therefore there is less motivation for the software company to identify potential vulnerabilities and release patches. Conversely, the more users of an information system, such as SAP the more motivation an adversary has to identify zero-day vulnerabilities within software applications.

A zero-day-vulnerability can provide direct access to the network, or assist malware propagation within a network until the target system is accessed. A vulnerability identified by an adversary in the SAP software would be able to be exploited by an adversary quickly. This initial foothold can be exploited to give access and permission profiles to instigators of the attack. An adversary can retain access to the target network even after a patch protecting against a zero-day-vulnerability is applied. Similar to the Stuxnet case study, zero-day vulnerabilities are virtually impossible to protect against and make detection of an Advanced Persistent Threat (APT) within a network difficult.

As demonstrated earlier in the Estonian case study a DDoS attack using botnets is simple but effective. In order to deny access to SAP and impact Australian Army logistics operations, detailed reconnaissance would need to be conducted by an adversary. It is likely that an adversary would attempt to deny access to the network backbone. This denial could be conducted through cyberspace or by a kinetic attack on infrastructure. It is also possible that server locations could be targeted by DDoS overwhelming the capacity of the network, as demonstrated in the DDoS attack on Estonia.

Malware, zero-day-vulnerabilities and DDoS attacks are all viable methods of conducting a cyber-attack against Australian Army LogIS. Any of the methods in isolation or combination can produce negative results on logistics operations at the tactical and operational levels of war. The extent of the damage caused will depend on the motivation for the attack, and whether the cyber-attack is an isolated act of war or part of a more complex multi-domain attack.

Success

As discussed in chapter 2, the Australian Army's principles of logistics can be used to analyze the success of a cyber-attack against Australian Army LogIS. The principles of responsiveness, economy, balance, sustainability, and survivability are particularly relevant to a cyber-attack. The case study analysis reveals that confidentiality motivated cyber-attacks are likely to have minimal impact on these principles of logistics. This type of attack would provide an adversary with intelligence to potentially shape kinetic maneuver operations as opposed to having a direct effect on logistics operations at the operational or tactical levels.

The responsiveness of LogIS enables the strategic, operational and tactical logistics support to military operations. A compromise of these systems through integrity or availability motivated cyber-attacks will likely result in logisticians not being able to provide the right support at the right time and place, and in the right condition, to meet the commander's needs.[186] An integrity attack makes it difficult for logisticians to determine which demands placed are legitimate, and those that are generated by an adversary. Similarly, the adversary could delete legitimate demands for key commodities to ensure that demands are not satisfied. Maintenance records can be modified forcing commanders to accept risk and waste resources ensuring aircraft, artillery and vehicles are available to support operations safely. DDoS attacks prevent demands from being raised or satisfied, inherently delaying logistic support to operations.

Achievement of economy within logistics occurs when effective support is provided using the fewest resources at the least cost and within acceptable levels of risk.[187] In a communications, permissive environment logisticians have the luxury of efficiency and adopt JIT principles. Redundancy of both data and stockholdings is a solution to mitigate the impact of a cyber-attack at the operational and tactical level.

[186] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Logistics*, 10.

[187] Ibid.

However, redundancy is manpower and resource intensive resulting in inefficient logistics operations.

The logistic system must balance the need for efficiency with the need for effective support in a battlespace.[188] In a military environment with a high cyber threat, JIT logistics risks the operational reach of a unit due to the lack of responsiveness. However, adopting a Just In Case (JIC) logistics stockholding policy to mitigate the impact of a cyber-attack expends greater resources. The increased stockholdings decrease the flexibility and maneuverability of the logistics elements at a tactical level and may impede the tempo and agility of the maneuver plan.

Survivability requires planning for the dispersion and protection of critical nodes of the logistics infrastructure, within both the theatre and the National Support Base.[189] Currently, Australian LogIS do not appear to be resilient enough to withstand a cyber-attack similar to the case studies analyzed above. Data redundancy, JIC stockh/oldings, and processes to restore information following a cyber-attack aimed at damaging the integrity of the data held in LogIS are non-existent and do not form part of the training environment.

Attribution

Given the security measures and network monitoring conducted on the DPN and DSN, it is likely that the greatest threat is a sophisticated adversary capable of launching an APT. This type of attack is likely to be conducted by a Nation State due to the

[188] Commonwealth of Australia, *Land Warfare Doctrine 4-0 Logistics*, 10.

[189] Ibid.

resources and reconnaissance that is required. However, the participation of non-state actors is not unfeasible. Given the sophistication of such attacks, it is likely that attribution will not be able to be proved and the investigation into the attack would take months. The lack of attribution provides an adversary plausible deniability and time to synchronize these cyber-attacks with other kinetic effects before Australia would be able to leverage security alliances or launch a kinetic offensive in retaliation.

DDoS attacks require little technical knowledge, less reconnaissance compared to confidentiality or integrity motivated attacks and are therefore possible for nation-state, non-state, or politically motivated actors. The outsourcing of DDoS attacks, as demonstrated in Estonia is possible meaning that attribution is unlikely. DDoS are also less likely to be considered comparable to a kinetic attack, limiting the probability Australia to invoke alliances such as ANZUS. Given the modus operandi appears to be to outsource DDoS attacks, attribution is difficult to prove with any level of certainty.

Prevention

Prevention is always better than cure. Having identified the vulnerabilities of LogIS to cyber-attack, it is essential to identify preventative measures from a holistic perspective to mitigate the impact of an attack or prevent an attack from occurring. Preventative measures need to address the people who use the system, the network architecture, and logistics practices which will prevent military forces from culminating at the tactical level.

As identified in chapter 2, Australian Army logistics doctrine fails to adequately address the threat posed by cyber-attacks. This gap in doctrine contributes to users of the DPN and DSN having poor cyber hygiene practices and who are oblivious to legitimate threats against LogIS and their role in preventing or mitigating an attack. Most users are aware of identity theft and malware as measures used to steal money; less are aware of the methods used by adversaries to gain access to networks. This lack of awareness coupled with ambivalence and an unfounded assumption that the DPN is impenetrable leaves LogIS vulnerable to cyber-attack.

Education programs for all users of the DPN are essential in preventing cyber-attacks. Education should be mandatory for contractors and third-party logistics providers who also have access to DPN. This level of education should focus on cyber hygiene. Additional education programs should be mandatory for logisticians to understand the threat posed to LogIS, emphasizing processes for reporting unusual behavior, and the importance of auditing access permissions.

Training serials should be introduced into annual exercises so that SOPs and doctrine can be developed to understand the cyber threat posed to LogIS specifically. Training serials should not just focus on DDoS, but also attacks that compromise data integrity. Training should help reinforce the importance of cyber hygiene, raise awareness of the threat and develop processes and procedures to mitigate the impact.

Identification fo LogIS as a potential foothold for an adversary to gain access to the DPN or DSN is a necessary step towards ensuring that LogIS network security is prioritized and adequately resourced. All contractors or commercial logistics providers who will have access to SAP or the DPN should have a cyber-assessment conducted on their networks to ensure that they meet the Australian CERT. This requirement should be monitored closely as part of the contractual obligations.

The requirement for logisticians to share information between the DPN and DSN needs to be acknowledged, as a mission requirement while also being a risk to cybersecurity. The initiation of a formalized process to safely transfer data between networks while avoiding the reliance on removable storage devices will enhance network security and mitigate against the threat of adversaries using LogIS as an initial foothold.

Protection of the DPN and DSN need to be resourced appropriately with an adequate number of people who trained appropriately. Exercises should be regularly conducted to identify weaknesses in the network architecture and to rehearse response measures and processes. A threat report should be produced to raise awareness among the Australian Army community of cyber threats faced by the DPN and DSN. This report will help to establish the viability of a cyber-attack on Australian Army information systems and reinforces the education and cyber hygiene practices.

To complement the training initiatives outlined above, doctrinal responses that can be implemented by logisticians can mitigate the effects of a cyber-attack on the maneuver plan at the tactical level. A move from JIT logistics towards JIC logistics is a necessary step in a communications denied environment and this should be simulated, wargamed and rehearsed before deployments in a conventional environment. Stock redundancy will have consequences on the operational reach, flexibility, and maneuverability of logistics units at the tactical level. Reliable communications systems have diminished the reliance on the Daily Replenishment Implementation Program (DRIP), a schedule of logistics commodities pushed to units on a daily basis established before deployment to a field environment. Rehearsal of this process during training is essential to the continuation of logistics support in a communications denied environment. Likewise, secondary and alternate communications methods should be identified and rehearsed during training serials to ensure that logisticians have not become reliant on digital communications as a sole source of information.

Summary

Analysis of the Target Corporation, Stuxnet and Estonian case studies using the ACSC assessment criteria has identified vulnerabilities of the Australian Army LogIS operating in the cyberspace domain. These systems are vulnerable to confidentiality, integrity, and availability motivated cyber-attacks, in similar ways to the case studies analyzed. The Australian Army Logistics Information System case study looked at the sensitivity and value of the information held within the system, intrusion vectors including malware, zero-day-vulnerabilities, and botnets that could be used to conduct a cyber-attack and outlined concerns with attribution of a potential cyber-attack. This analysis has answered the primary research question, what are the vulnerabilities facing the Australian Army's LogIS within the cyberspace domain?

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

> Throughout the struggle, it was in his logistic inability to maintain his armies in the field that the enemy's fatal weakness lay. Courage his forces had in full measure, but courage was not enough. Reinforcements failed to arrive, weapons, ammunition and food alike ran short, and the dearth of fuel caused their powers of tactical mobility to dwindle to the vanishing point. In the last stages of the campaign they could do little more than wait for the Allied advance to sweep over them.
>
> — Dwight D. Eisenhower, *British Army Doctrine Publication, Volume 3*

Introduction

Logisticians in general and those in the Australian Army, in particular, achieve efficiency on a daily basis by leveraging capabilities available through digital information systems. These systems are essential to supporting military operations, and every effort should be made to automate and digitize our military forces to take advantage of available technology. However, the Australian Army should no longer assume that it will operate in a permissive communications environment.

This research aimed to raise awareness among the Australian Army logistics community regarding the vulnerabilities of LogIS in the cyberspace domain. The current state of oblivion amongst logistics planners, operators and users has its foundations on the assumption of cyberspace superiority and a permissive communications environment. This paper aimed to answer the following primary research question, what are the vulnerabilities facing the Australian Army's LogIS within the cyberspace domain?

Chapter 4 included the analysis of the cyber case studies including the Target Corporation, Stuxnet, and Estonia against the ACSC assessment criteria sensitivity, impact, success, and attribution. The addition of a fifth criterion, prevention along with a discussion of the implications for Australian LogIS helped to determine the relevance of each case study to LogIS. Australian Army LogIS was found to be vulnerable to confidentiality, integrity, and availability motivated cyber-attacks executed through malware, zero-day-vulnerabilities, and botnet intrusion vectors. Having identified Australian Army LogIS as vulnerable, this paper identifies doctrinal, training and materiel solutions that can help mitigate against these vulnerabilities to LogIS within the cyberspace domain.

This chapter will interpret the findings identified in chapter 4, provide fidelity and discuss the implications of the results captured during the conduct of this research. Recommendations and conclusions describe actions the Australian Army can take to mitigate the vulnerabilities of Australian Army LogIS operating in cyberspace. These recommendations answer the secondary research question.

Interpretation of Findings

A cyber-attack on LogIS is plausible and yet largely unidentified in academic literature or research either from commercial or military perspective. This finding is made having assessed three case studies in chapter 4. The motivations for conducting an attack to steal data, modify data or deny access to data held on a network remains valid for Australian Army LogIS.

As a viable threat, it is important to raise awareness about the existence of the threat itself and adopt mitigation measures in response. Awareness and mitigation should not prohibit digital innovation in support of more efficient or effective provision of logistics within the battlespace. Rather, identifying the threat and mitigating it should be perceived as making technology-dependent solutions more reliable, robust, and secure.

The vulnerability of LogIS to cyber-attack should not be cause for sensationalism. The vulnerabilities identified in this research apply in general terms to other information systems employed by the Australian Defence Force and are not limited to logistics. Rather, the cyber-risk of LogIS should be assessed and managed as part of a whole network risk management assessment. In assessing the network as a whole, it is important to emphasize a number of factors that make Australian Army LogIS an attractive network foothold for the DPN or DSN, in addition to LogIS being a viable target in its own right. These factors are the exposure to commercial logistics providers, the requirement to transition data regularly from DPN to DSN and the reliance on digital information.

The reliance on LogIS by the Australian Army, the lack of doctrine and poor awareness regarding the cyber domain in the Australian Army underpinned an expectation that research conducted would identify a capability gap. Unexpectedly, the research revealed that in both the Target Corporation and Stuxnet attacks cyber awareness and poor cyber hygiene practices contributed to a far greater extent than anticipated when commencing this research. It also revealed that in a DDoS attack cyber hygiene and awareness training matters far less than the network architecture, response protocols, and bandwidth. Identifying the risk to potential zero-day exploits of the SAP software platform was also unexpected.

Conclusions and Recommendations

The research conducted has enabled several conclusions to be drawn from the three case studies. Primarily, that Australian Army LogIS is vulnerable to cyber-attack and that current doctrine, training, and education of Australian Army logisticians is insufficient to help mitigate the vulnerabilities identified. However, a number of recommended actions are presented to improve the cyber awareness and hygiene of users of Australian Army LogIS and therefore mitigate against these identified vulnerabilities.

Conclusions

Conclusion 1: Australian Army LogIS are vulnerable to cyber-attack. The intrusion vectors used in all three case studies would have achieved successful outcomes for the attacker if applied to the Australian Army LogIS network. The data that resides on Australian Army LogIS is an attractive target for attacks motivated by confidentiality, integrity or availability. These motivations would all have an impact on the ability for logisticians to provide operational reach and prevent early culmination at the operational and strategic level. However, it does appear that the impact of a cyber-attack aimed at data integrity or data availability would have the most profound impact.

Conclusion 2: Doctrine, Training, and Education of Australian Army logistics officers is inadequate in identifying and mitigating the risk to LogIS in cyberspace. As identified in chapter 2, the doctrine at the unclassified level is insufficient at addressing the threat to the Australian Defence Force through cyberspace. Given the vulnerability is not acknowledged it is not surprising that training and education do not reflect the threat faced by LogIS in cyberspace.

Conclusion 3: Cyber hygiene and awareness training of the Australian Army is important in preventing a cyber-attack. Air-gapped systems are not impervious to cyber-attack. In the Target Corporation and Stuxnet case studies it was evident that poor cyber awareness and cyber hygiene practices of the personnel who operated the computer systems contributed directly to the achievement of the initial foothold. While anti-virus and anti-malware programs can be effective, personnel require further training on the use of external storage, and phishing attacks, watering holes and malvertising.

Recommendations

Recommendation 1: Doctrine needs to incorporate cyberspace threats and measures for mitigation. The threat posed to logistics by cyberspace is under-represented in Land Warfare Doctrine 4-0: *Logistics*. Despite being reviewed and released in 2018, this doctrine fails to frame the problems faced by LogIS in cyberspace, and its mitigation measures are too broad to be effectively implemented. It would benefit the Australian Army as a whole to have an unclassified cyberspace capstone document similar to Joint Publication 3-12 (R) *Cyberspace Operations*. This doctrine would enable an update of LWD 4-0 to focus on how logistics doctrine might be able to mitigate the effects of cyber-attack, potentially through data and stock redundancy.

Recommendation 2: Training serials need to simulate cyber-attacks against Australian Army LogIS in field exercises. Given the threat posed to data integrity and DDoS attacks posed by cyber-attack, field exercises need to simulate these effects. Exercises would then provide the data to inform doctrinal practices to mitigate against a successful cyber-attack. While this research indicates that LogIS are vulnerable to cyber-attack, it does not quantify the impact of such an attack at the operational or tactical levels. Training serials impacting logistics support at Brigade level and above would provide valuable data in stockholding levels required in a communications denied environment.

Recommendation 3: Career courses for logisticians need to incorporate the threats posed by cyberspace, in particular against LogIS. Given the infancy of cyberspace awareness within the Australian Army, it is likely that this should initially focus on awareness and understanding of the problem. Having quantified the problem set through training exercises, it would be apt to include the impact of cyber-attacks in Tactical Exercises Without Troops (TEWTs) and Staff Military Appreciation Process (SMAP) exercises. It would also be an ideal problem set to give to the Logistics Officers Advanced Course to identify measures at the tactical level which might mitigate a cyber-attack at the strategic level. Additionally, CERT, ASD and the newly formed Information Warfare Division may be able to provide products and information to inform learning outcomes for incorporation into the Logistics Officer Training Curriculum.

Recommendation 4: Identification of the cyber-risk in any new procurement purchase or contract is essential in minimizing the risk to LogIS in cyberspace. Initiation of retrospective cyber risk assessments on in-service equipment that is connected using networks, with a particular focus on items purchased through COTS is critical in quantifying the risk. A network is only as strong as its weakest link. Given the delays in upgrading to Windows 10 and legacy software that is continuing to run on the DPN,[190] it is plausible that adversaries have already penetrated our networks. It is also likely that there are information systems and platforms connected to the DPN or DSN that could be

[190] Hannah Francis, "Revealed: Australian Government Pays Hefty Price to Keep Outdated Windows Operating Systems Secure," *The Sydney Morning Herald*, 5 August 2015, https://www.smh.com.au/technology/revealed-australian-government-pays-hefty-price-to-keep-outdated-windows-operating-systems-secure-20150804-girdcd.html, (accessed 10 March 2018).

exploited to gain access to our networks. These prior procurements should be assessed to identify any cyber-risk posed by their connectivity, and an assessment conducted whether the risk can be mitigated or should be accepted. Similarly, organizations and contractors that have access to LogIS should be evaluated to ensure that their network architecture or cyber hygiene practices do not place the Australian Army networks at risk.

Recommendation 5: Cyber awareness training should be developed to encourage good cyber hygiene practices by all users of the DPN and DSN. Underpinning the Stuxnet and Target Corporation attacks were poor cyber hygiene practices at the lowest levels. Cyber awareness of the Australian Army needs to be improved, and while mandatory training is one answer, it is only part of the process. The use of CDs to transfer information from DPN and DSN places networks at unnecessary risk. A procedure or mechanism of transferring information safely from the DPN to the DSN needs to be established to ensure that the transfer can occur without the risk. Password management, awareness of pass the hash techniques and an understanding of sophisticated spear phishing, watering holes and malvertising techniques all need to be included in the training.

Recommendations for further study. The impacts of cyberspace on logistics systems and processes are under-represented in academic literature and research from both a commercial and military perspective. Therefore, the potential for further research is vast. However, specific research into network risk management assessments to further understand the likelihood of a cyber-attack on Australian Army LogIS would prove invaluable. Similarly, a risk-benefit analysis of the use of cloud or blockchain technology to mitigate threats posed to LogIS through cyberspace would provide invaluable in informing future LogIS network structures.

Closing Remarks

The Australian Army has benefited greatly from digitization, networks, and improvements in communications systems. These improvements have enabled logistics to become more efficient and effective. However, these technological improvements come with vulnerabilities in the cyberspace domain. Unfortunately, general cyberspace awareness in the Australian Army is poor, and these vulnerabilities are unidentified and underrepresented in doctrine, training, education, and academic research.

The requirement for logisticians to transfer information between unclassified, protected and secure networks results in Australian Army LogIS being vulnerable to cyber-attacks motivated at attacking data confidentiality, data integrity, and data availability. Reliance on LogIS combined with an assumption of a communications permissive environment has left the Australian Army ignorant of inherent risks to the network.

The consequences of ignoring these vulnerabilities could force an early culmination point of logistical support to combat operations. "Cyber weapons, particularly those allegedly being developed by China to exploit the U.S. military's logistics IT network, would complement conventional military operations."[191] In the current operating environment with a renewed focus on conventional warfare against a near-peer adversary and the popularity of multi-domain battle concept, attacking LogIS in

[191] Mazanec, *The Evolution of Cyber War*, 233.

cyberspace may provide adversaries with an Achilles heel against the Western Way of War.

BIBLIOGRAPHY

Books

Creswell, John W. *Qualitative Inquiry and Research Design: Choosing among Five Approaches*. 2nd ed. Thousand Oaks, CA: SAGE Publications, 20 December 2006.

Farivar, Cyrus. *The Internet of Elsewhere: The Emergent Effects of a Wired World*. New Brunswick, QC: Rutgers University Press, 08 June 2011.

Guba, Egon G., and Yvonna S. Lincoln. *Fourth Generation Evaluation*. Newbury Park, CA: Sage Publications, 01 October 1989.

Kramer, Franklin, Stuart H. Starr, and Larry Wentz, eds. *Cyberpower and National Security*. Washington, DC: Potomac Books, 30 April 2009.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 16 April 2007.

Libicki, Martin C., Lillian Ablon, and Tim Webb. *The Defender's Dilemma: Charting a Course Toward Cybersecurity*. Santa Monica, CA: RAND Corporation, 10 June 2015.

Mazanec, Brian M. *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. Lincoln, NE: Potomac Books, 01 November 2015.

Russell, Alison Lawlor. *Cyber Blockades*. Washington, DC: Georgetown University Press, 05 November 2014.

Shy, John. "Jomini." In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, edited by Peter Paret, 143–185. Princeton, NJ: Princeton University Press, 01 October 2010.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, NY: Oxford University Press, 04 December 2013.

Periodicals

Abrams, Rachel. "Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop." *The New York Times,* 05 August 2014. Accessed 28 January 2018. https://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html.

Armerding, Taylor. “The 17 Biggest Data Breaches of the 21st Century.” *CSO,* 26 January 2018. Accessed 28 January 2018. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

Austin, Greg. “A Cyber Revolution on Russell Hill.” *The Strategist,* 16 May 2017. Accessed 06 November 2017. https://www.aspistrategist.org.au/cyber-revolution-russell-hill/.

———. “‘Cyber Revolution’ in Australian Defence Force Demands Rethink of Staff, Training and Policy.” *The Conversation,* 03 July 2017. Accessed 23 September 2017. http://theconversation.com/cyber-revolution-in-australian-defence-force-demands-rethink-of-staff-training-and-policy-80317.

Broad, William J., John Markoff, and David E. Sanger. “Stuxnet Worm Used Against Iran Was Tested in Israel.” *The New York Times,* 15 January 2011. Accessed 4 February 2018. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Davis, Joshua. “Hackers Take Down the Most Wired Country in Europe.” *Wired,* 21 August 2007. Accessed 18 February 2018. https://www.wired.com/2007/08/ff-estonia/.

Farwell, James P., and Rafal Rohozinski. “Stuxnet and the Future of Cyber War.” *Survival* 53, no. 1 (1 February 2011): 23–40.

Ferrillo, Paul. “Defending Your Network Against DDoS Attacks.” *Tripwire,* 23 February 2016. Accessed 24 February 2018. https://www.tripwire.com/state-of-security/security-awareness/defending-your-network-against-ddos-attacks/.

Francis, Hannah. “Revealed: Australian Government Pays Hefty Price to Keep Outdated Windows Operating Systems Secure.” *The Sydney Morning Herald,* 5 August 2015. Accessed 10 March 2018. https://www.smh.com.au/technology/revealed-australian-government-pays-hefty-price-to-keep-outdated-windows-operating-systems-secure-20150804-girdcd.html.

Kolb, Sharon. “Grounded Theory and the Constant Comparative Method: Valid Research Strategies for Educators.” *Journal of Emerging Trends in Educational Research and Policy Studies* 3, no. 1 (01 January 2012): 83–86.

Kostadinov, Dimitar. “Estonia: To Black Out an Entire Country.” *InfoSec Institute*, 01 October 2013. Accessed 19 February 2018. http://resources.infosecinstitute.com/estonia-to-black-out-an-entire-country-part-one/.

Krebs, Brian. “Email Attack on Vendor Set Up Breach at Target.” *Krebs on Security*, 12 February 2014. Accessed 28 January 2018. https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.

———. “The Target Breach, By the Numbers.” *Krebs on Security*, 6 May 2014. Accessed 28 January 2018. https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

Kushner, David. “The Real Story of Stuxnet.” *IEEE Spectrum: Technology, Engineering, and Science News,* 26 February 2013. Accessed 25 January 2018. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Lachow, Irving. “The Stuxnet Enigma: Implications for the Future of Cybersecurity.” *Georgetown Journal of International Affairs* (Fall 2011): 118–126.

Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* 22, no. 3 (July 2013): 365–404.

Morrow, Susan L. “Quality and Trustworthiness in Qualitative Research in Counseling Psychology*.” Journal of Counseling Psychology* 52, no. 2 (April 2005): 250–260.

Sanger, David E. “Obama Order Sped Up Wave of Cyberattacks Against Iran.” *The New York Times,* 01 June 2012. Accessed 4 February 2018. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Shenton, Andrew. “Strategies for Ensuring Trustworthiness in Qualitative Research Projects.” *Education for Information* 22, no. 2 (2004): 63-75.

Thomas, Eileen, and Joan Kathy Magilvy. “Qualitative Rigor or Research Validity in Qualitative Research.” *Journal for Specialists in Pediatric Nursing* 16, no. 2 (01 April 2011): 151–155.

Torrence, James. “Spear Phishing: Dangers & Need for Education.” *Small Wars Journal,* 5 February 2017. Accessed 10 October 2017. http://smallwarsjournal.com/jrnl/art/spear-phishing-dangers-need-for-education.

Voss, Chris, Nikos Tsikriktsis, and Mark Frohlich. “Case Research in Operations Management.” *International Journal of Operations & Production Management* 22, no. 2 (01 February 2002): 195–219.

Williams, Brett. “The Joint Force Commander’s Guide to Cyberspace Operations.” *Joint Force Quarterly* (2nd Quarter 2014): 12–19.

Zetter, Kim. “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.” *Wired*, no. 11 (2011): 1–8.

Government Documents

Commonwealth of Australia. *Australian Cyber Security Centre 2016 Threat Report*. Canberra, ACT: Australian Cyber Security Centre, October 2016. Accessed 23 September 2017. https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf.

———. *Australian Cyber Security Centre 2017 Threat Report*. Canberra, ACT: Australian Cyber Security Centre, October 2017. Accessed 10 November 2017. https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf.

———. *Australia's Cyber Security Strategy*. Canberra, ACT: Department of the Prime Minister and Cabinet, 2016. Accessed 23 September 2017. https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf.

———. *Department of Defence White Paper 2016*. Canberra, ACT: Department of Defence, 2016. Accessed 2 November 2017. http://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.

———. *Essential Eight Explained*. Canberra, ACT: Australian Signals Directorate, February 2017. Accessed 5 December 2017. https://www.asd.gov.au/publications/protect/Essential_Eight_Explained.pdf.

———. *Land Warfare Doctrine 4-0 Combat Service Support*. Canberra, ACT: Australian Army, 2009. Accessed 23 September 2017. https://www.cove.org.au/doctrine/lwd-4-0-combat-service-support/.

———. *Land Warfare Doctrine 4-0 Logistics*. Canberra, ACT: Australian Army, 2018. Accessed 08 April 2018. https://www.army.gov.au/sites/g/files/net1846/f/lwd_4-0_logistics_full.pdf.

Chairman Joint Chiefs of Staff. Joint Publication 3-12 (R), *Cyberspace Operations.* Washington, DC: Government Printing Office, 5 February 2013. Accessed 23 September 2017. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Committee On Armed Services House of Representatives. *Cyberspace as a Warfighting Domain: Policy, Management and Technical Challenges to Mission Assurance.* Hearing Before the Terrorism, unconventional Threats and Capabilities Subcommittee of the Committee On Armed Services House of Representatives 111th Congress, 5 May 2009. Accessed 29 March 2018. https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg57218/pdf/CHRG-111hhrg57218.pdf.

Committee On Commerce Science, and Transportation. *A "Kill Chain" Analysis of the 2013 Target Data Breach.* Committee on Commerce Science, and Transportation. 26 March 2014. Accessed 15 January 2018. https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf.

Department of Defense. Department of Defense Instruction (DoDI)*, Cybersecurity*. Washington, DC: Government Printing Office, 14 March 2014. Accessed 5 November 2017. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf.

Headquarters, Department of the Army. Army Regulation 750-1, *Army Materiel Maintenance Policy.* Washington, DC: Government Printing Office, 12 September 2013.

House of the Armed Services Committee. *The Current State of U.S. Transportation Command*, House of the Armed Services Committee 115th Congress, 30 March 2017. Testimony of General Darren W. McDrew, USAF. Accessed 16 November 2017. http://docs.house.gov/meetings/AS/AS03/20170330/105767/HHRG-115-AS03-Wstate-McDewUSAFD-20170330.pdf.

U.S. President. *The National Security Strategy of the United States of America*. Washington, DC: The White House, 27 May 2010. Accessed 16 October 2017. http://nssarchive.us/national-security-strategy-2010/.

Other Sources

Aorato Labs. "The Untold Story of the Target Attack: Step by Step." Report, Aorato Labs, Herzliya, Tel Aviv, August 2014. Accessed 15 January 2018. https://aroundcyber.files.wordpress.com/2014/09/aorato-target-report.pdf.

Assante, Michael J., and Robert M. Lee. "The Industrial Control System Cyber Kill Chain." Report, SANS Institute, North Bethesda, MD, October 2015. Accessed 4 February 2018. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

Bontea, Sirius. "The Cyber Threat to Military Just-In-Time Logistics: Risk Mitigation and the Return to Forward Basing." Monograph, School of Advanced Military Studies, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2017.

Cain, Scott A. "The Net Is Down, Now What Do We Do? Is The Air Force Prepared To Survive A Cyber Attack." Thesis, US Air Force School of Advanced Air and Space Studies, Maxwell Air Force Base, AL, June 2009. Accessed 24 February 2018. http://www.dtic.mil/docs/citations/ADA540670.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. “W32.Stuxnet Dossier.” Report, Symantec, Cupertino, CA, February 2011. Accessed 4 February 2018. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Geli, Mathieu, Darya Maenkova, and Alexander Polyakov. ”SAP Cyber Security in Figures -Global Threat Report 2016.” Research Report, ERP Scan, Palo Alto, CA, 2016. Accessed 5 December 2017. https://erpscan.com/wp-content/uploads/publications/Sap-Cyber-Threat-Report.pdf.

Joubert, Vincent. “Five Years after Estonia’s Cyber Attacks: Lessons Learned for NATO?” Research Paper, NATO Defense College, Rome, May 2012. Accessed 18 February 2018. https://www.files.ethz.ch/isn/143191/rp_76.pdf.

KPMG. “Defense ERP Overview by Country.” Report, KPMG, Melbourne, ACT, April 2016. Accessed 5 December 2017. https://assets.kpmg.com/content/dam/kpmg/pdf/2016/04/defense-erp-overview-by-country.pdf.

Lee, R. M. “The History of Stuxnet: Key Takeaways for Cyber Decision Makers.” Cyber Conflict Studies Association Paper, Armed Forces Communications and Electronics Association (AFCEA), Washington, DC, 4 June 2012.

McDrew, Darren. “Transcom Commander Discusses the Strategic Environment.” Speech, Logistics Officer Association Symposium, National Hall, Maryland, VA: 15 November 2017. Accessed 16 November 2017. https://cdn.dvidshub.net/media/video/1711/DOD_105079033/DOD_105079033-1920x1080-6221k.mp4.

Mueller, Paul, and Babak Yadegari. “The Stuxnet Worm.” Report, University of Arizona Computer Science Department, Tuscon, AZ, 2012. Accessed 26 January 2018. https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf.

North Atlantic Treaty Organization. “Member Countries.” Accessed 20 February 2018. http://www.nato.int/cps/en/natohq/topics_52044.htm.

———. “NATO Cooperative Cyber Defence Centre of Excellence.” NATO Cooperative Cyber Defence Centre of Excellence Website. 26 May 2014. Accessed 02 November 2017. https://www.ccdcoe.org/cyber-definitions.

NBC News. “Target Data Breach Cost for Banks Tops $200M.” 18 February 2014. Accessed 28 January 2018. https://www.nbcnews.com/business/business-news/target-data-breach-cost-banks-tops-200m-n33156.

Porche, Isaac R. III, Jerry Sollinger, and Shawn McKay. “A Cyberworm That Knows No Boundaries.” Report, RAND, Santa Monica, CA, 2011. Accessed 23 September 2017. https://www.rand.org/pubs/occasional_papers/OP342.html.

Radichel, Teri “Case Study: Critical Controls That Could Have Prevented Target Breach.” Report, SANS Institute, North Bethesda, MD, August 2014. Accessed 18 January 2018. https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

Riley, Michael, Ben Elgin, Dune Lawrence, and Carol Matlack. “Target Missed Warnings in Epic Hack of Credit Card Data.” Bloomberg, 17 March 2014. Accessed 18 January 2018. https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

SAP. “Military, Defense, and Security | Industry Software.” Accessed 5 December 2017. https://www.sap.com/industries/defense-security.html.

———. “SAP Paves Way for NATO’s Next-Generation Command and Control Systems.” SAP News Center Website, 26 July 2005. Accessed 5 December 2017. https://news.sap.com/sap-paves-way-for-natos-next-generation-command-and-control-systems/.

Stallard, Craig. “At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force.” Monograph, US Air Force School of Advanced Air and Space Studies, Maxwell Air Force Base, AL, June 2011.

Target Corporate. “Payment Card Issue FAQ.” Accessed 18 January 2018. http://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ.aspx.

———. “Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores.” 19 December 2013. Accessed 18 January 18 2018. http://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car.

Ware, Willis H. “Security and Privacy in Computer Systems.” Report, RAND, Santa Monica, CA, April 1967.