National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# CYBER WARFARE: THE NEW DOMAIN AND FUTURE BATTLE SPACE

Maj C.W. Ethelston

| | |
|---|---|
| **JCSP 41** | **PCEMI 41** |
| **Exercise *Solo Flight*** | **Exercice *Solo Flight*** |
| **Disclaimer** | **Avertissement** |
| Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission. | Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite. |
| | |

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 41 – PCEMI 41
2014 – 2015

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

# CYBER WARFARE: THE NEW DOMAIN AND FUTURE BATTLE SPACE

Maj C.W. Ethelston

*“This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”*

Word Count: 5489

*“La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.”*

Compte de mots : 5489

## INTRODUCTION

Advancement in technology has caused drastic changes in the way that wars are conducted or how adversaries attack their enemies. From the earliest of times wars were fought on the battlefield in direct contact with swords until there was a victor. As time passed, bow and arrows, and later smoothbore muskets, were developed to create standoff between conflicting parties. The one element that did not change was the linear line and column formation held on both sides known as first-generation warfare.[1] Wars were often fought as either a battle of annihilation, pure physical destruction of the adversary, or one of attrition until there was a winner. As technology continued to advance, it led to the creation of new and improved weapons that allowed for more flexibility and a higher degree of lethality. This became known as the second generation of warfare, which included machine guns and eventually indirect artillery fire in World War I.[2] Further to this would also be the evolution of technology within the maritime and air components with the development of sophisticated ships and aircraft.

In today's age of conflict and war technology has created a vast amount of weaponry that is built and dependent upon the digital sphere of ones and zeroes. This technology has been embraced by all warfighting environments; land, sea, air and space and has the ability to reduce casualties and cost of war. Within a military context, forces have become reliant on this technology. More use has been made of Global Positioning Satellites (GPS) to aid with navigation as well as incorporated into smart munitions, such as the Excalibur artillery round used by the Canadian Armed Forces (CAF), that use GPS

[1] Richard D. Hooker, *Maneuver Warfare : An Anthology* (Novato, CA: Presidio, 1993), 4.
[2] *Ibid.*, 5.

guidance to hit targets with precision effects. Technological innovation involving the cyber domain is having a significant impact on the nature of conflict and the manner in which it is and will be conducted.[3]

This technology and use of the electromagnetic spectrum, or simply the concept of cyberspace, is not entirely new. Only more recently has operations within the cyber domain become more frequent and sophisticated as the world becomes increasingly dependent on technology and the internet. With a greater access to multiple enablers such as the internet, various weapons and weapon related technologies, the mobility, reach and lethality of an adversary will increase and become more difficult to identify and defend against.[4] The concern regarding this advancement and evolutionary reality of cyberspace has raised significant concerns. The Director of the U.S. Federal Bureau of Investigation stated in 2012 that threats from cyber-espionage, computer crime, and attacks on critical infrastructure will become the number one threat to the U.S. even above terrorism.[5] Concerns like this begin to raise the question as to whether cyber should be considered its own distinct domain as well as its own identifiable theatre of operations, or battlespace.

This paper will argue that cyber is the newest warfighting domain, is the future of international conflict and terrorism, and can be considered its own battlespace. All organizations and infrastructure will be affected from banks to electrical power plants to transportation networks and the military. This paper will contend that cyber should be separated from the land, sea, air and space environments by demonstrating its

[3] Canada. Department of National Defence, *Land Operations 2021 Adaptive Dispersed Operations the Force Employment Concept for Canada's Army of Tomorrow*, ed. Andrew B. Godefroy (Ottawa: DND Canada, 2007), 4.

[4] *Ibid*., 5.

[5] Angela Gendron and Martin Rudner, *Assessing Cyber Threats to Canadian Infrastructure* (Ottawa: Government of Canada,2012), 41.

applicability to, and use of, the five operational functions; Command, Act, Sense, Shield and Sustain, which are commonly applied in each of the current environments. Furthermore, this paper will argue that cyber warfare should be considered its own distinct battlespace. This will be supported through the emphasis that it has received from all nations, especially the North Atlantic Treaty Organization (NATO), in developing their own separate cyber commands and cyber defence policies. Further cyber activity will be discussed in relation to the fact that a cyber-attack can trigger a NATO Article 5 response as well as the advantages gained by conducting cyber warfare. It will also be argued that the new theatre of operations, or battlespace, is Computer Network Operations (CNO), which is conducted through its three components of Computer Network Attacks (CNA), Computer Network Defence (CND) and Computer Network Exploitation (CNE).

## CYBER TERMINOLOGY

In order to comprehend the concept and idea of the cyber domain it is important to understand the different terminology and their definitions. For the purposes of this paper, domain and environment will be used synonymously. There is no actual common terminology for cyber and it is all dependent on the nation or organization and the definition they determine to describe the different lexicon, which creates some ambiguity within the field. For the purposes of this paper, definitions will focus mainly on Canadian definitions from a land perspective.

First to be addressed is the cyber domain. According to the Canadian Army Land Warfare Centre the cyber domain consists of the communications and information exchange that enables computer-based networks and is the environment in which computer network operations are conducted.[6] The next term to be defined is cyber war or warfare, which is a difficult term to find defined in any country. The online Oxford dictionary defines cyber war as:

> The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of communication systems by another state or organization: ‘cyberwar is asymmetric, which means it benefits lesser military powers as much as military goliaths’[7]

The latter part of the definition indicates that cyber has the ability to provide insignificant actors with a disproportionate amount of power making it more desirable for an inferior organization or adversary. Cybersecurity analyst and expert Jeffery Carr defines cyber warfare as, “the art and science of fighting without fighting, of defeating an opponent without spilling their blood”[8] indicating that the end state is to be achieved with no bloodshed. The final term to define with respect to the cyber domain is cyberspace, which is defined in Canada’s Cyber Security Strategy written in 2010. For Canada, cyberspace is the electronic world that is created by interconnected networks of information technology as well as the information on those networks.[9]

Now that the cyber terminology has been defined and shown to relate to electronic and computer networks, the remaining terminology to understand is CNO and its three components as they are heavily involved in cyberspace. CNO is defined as “actions that can be taken to defend, exploit or attack information that is resident on

[6] Canada. Department of National Defence, *No Man's Land: Tech Considerations for Canada's Future Army* (Kingston, ON: Army Publishing Office, 2014), 5-10.

[7] "Oxford Dictionaries Language Matters." http://www.oxforddictionaries.com/definition/english/cyberwar (accessed 12 April, 2015).

[8] Jeffery Carr, *Inside Cyber Warfare, Mapping the Cyber Underworld*, ed. Mike Loukides, 2nd ed. (Sebastopol, CA: O'Reilly Media, Inc., 2011), 2.

[9] Canada. Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: Govt. of Canada, 2010), 2.

Information Systems (IS) and/or IS themselves."[10] In order for this to be achieved CNO is comprised of three components which are attack, exploitation and defence. CNA is defined as:

> a directed activity conducted through the use of computer networks to intentionally disrupt, deny, degrade or destroy adversary computers, computer networks, and/or the information resident on them.[11]

CNE is defined as:

> a directed, covert activity conducted through the use of computer networks to remotely enable access to, collect information from, and/or process information on computers or computer networks.[12]

CND is defined as:

> an activity conducted through the use of one's own computer networks to protect, monitor, detect, analyze, and respond to unauthorized activity within computers or computer networks.[13]

Beyond cyber and CNO definitions it is also important to define Electronic Warfare (EW) as discussions may at times involve the idea that cyber is no different than EW. CAF EW doctrine has adopted the NATO definition, which is:

> Military action to exploit the electromagnetic (EM) spectrum which encompasses the interception and identification of EM emissions, the employment of EM energy, including directed energy, to reduce or prevent hostile use of the EM spectrum and actions to ensure its effective use by friendly forces.[14]

By this definition EW deals specifically with the EM spectrum with the focus of denying an adversary the use of the radio frequency spectrum used for either voice or data

[10] Canada. Department of National Defence, *C4ISR Capability Development Plan* (Ottawa: DND Canada, 2009a), 37.

[11] Canada. Department of National Defence, *Canadian Forces Computer Network Operations (CNO) Policy Draft Version 2.1* (Ottawa: DND Canada, 2009b).

[12] *Ibid.*

[13] *Ibid*.

[14] Canada. Department of National Defence. B-GL-358-001/FP-001, *Land Force Information Operations Electronic Warfare* (Ottawa: DND Canada, 2004), 17.

command and control or for other sensors that use the EM spectrum. This is different from some of the operations in cyberspace where the intent is to influence the information resident within operating systems or software programs or affecting the actual hardware, software, cable/fibre/wireless transmissions in order to achieve a desired effect.[15] This relates more specifically to computer networks and hardware, which is ultimately the focus of CNO. The influence activity of CNO relates to Information Operations (IO). Both EW and CNO activities are required to conduct influence activities and create a desired non-kinetic effect and will be discussed within the Act function. If EW and CNO are able to conduct influence activities then it makes sense that they can be considered as subcomponents of IO. Furthermore, as subcomponents of IO that both use the EM spectrum, then cyber can be considered as the overarching domain that incorporates both EW and CNO, along with communications and information systems, signals intelligence and EM spectrum operations.[16] To argue that these activities belong together under the cyber domain would be the focus of a separate paper. Instead, this paper will only focus on defining cyber as its own environment and new battlespace.

There are many supporters that believe cyber should be considered its own domain on one hand and on the other there are those that think it should only be a subcomponent to the other environments. The CF Integrated Capstone Concept, published in 2009, advocates that the strategic environment should expand to include cyberspace[17] and views cyberspace as a separate domain. The document states:

[15] J. C. Walkling and Canadian Forces College, *Considerations: Canadian Forces' Efforts in the Electromagnetic Spectrum and Cyber Operating Environment*, Vol. JCSP/PCEMI 39-78 (Toronto, Ont.: Canadian Forces College, 2013), 1.

[16] *Ibid*., 5.

[17] Canada. Department of National Defence. A-FD-005-002/AF-001, *Integrated Capstone Concept* (Winnipeg: 17 Wing Winnipeg Publishing Office, 2009), 27.

> The new question should be, “Can the physical world create effects in cyberspace (e.g. destroy information)?” The answer is certainly “yes” since individual nodes, sensors, and hardware components can be effectively destroyed; however, once video, imagery, data, information, and misinformation are placed within cyberspace, it becomes impossible to remove. For these reasons, cyberspace is a separate domain where elements of national power and influence are clearly exercised.[18]

In order for an environment to be identified as its own domain all of the operational functions must apply and be addressed to it as previously stated. To understand why cyberspace should be considered as the 5th domain it will be shown that cyberspace addresses all five of the operational functions similar to the other warfighting environments. This paper will focus the domain analysis mainly between cyberspace and the land environment.

## CYBER AND THE OPERATIONAL FUNCTIONS

Command is inherently a human undertaking but also involves aspects of cyber activities. According to Canadian doctrine:

> Command is the operational function that integrates all the operational functions into a single comprehensive strategic, operational or tactical level concept. It provides vertical and horizontal integration through the planning, direction, coordination and control of military forces and other elements as allocated…and is reliant upon robust communications [and] good intelligence.[19]

In this aspect it can be considered as the nexus for the other four operational functions of which cyber plays an important role. In order for commanders to be successful in battle they must have good situational awareness that will provide a Common Operating Picture (COP) and they need to have strong command and control, all of which the cyber

[18] *Ibid.*, 31.

[19] Canada. Department of National Defence. B-GL-300-001/FP-001, *Land Operations* (Ottawa: DND Canada, 2008), 4-18.

environment is able to provide. With the development of technology this is accomplished through a complex network of communications, satellites and intelligence, surveillance and reconnaissance (ISR) assets like the Unmanned Aerial Vehicle (UAV), as one small example, that all use the cyber domain to collect and transfer information. Situational awareness does not only include awareness of one's own networks but also of the enemy networks to complete the COP for the commander.

It is essential that cyber operations be commanded as it is critical to keeping the network functioning. Cyber activities represent options that a staff may wish to inject into operations but the activities must be led by a commander. Cyber warfare is similar to manoeuvre warfare where speed and agility are two of the most important factors that a commander must be aware of when making decisions.[20] Manoeuvering in the cyber environment may cause an adversary to become exposed and defeated along with the possibility of undermining friendly manoeuvre. For these reasons the responsibility of cyber operations must be entrusted to a commander that understands the cyber environment and its potential effects on operations.[21] Just like the other domains, cyber capabilities can also be attacked. Satellites, radars, networks and databases can all be targeted and disabled significantly impacting a commander's ability to command and control the operation, which demonstrates its suitability of addressing the command function similar to the other environments.[22]

[20] William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (Sep, 2010), 97-108.

[21] Canada. Department of National Defence, *No Man's Land: Tech Considerations for Canada's Future Army*, 5-36.

[22] W. C. McGuffin and Canadian Forces College, *Soldiers of FORTRAN: Militarization of the 5th Dimension*, Vol. JCSP/PCEMI 39 (Toronto, Ont.: Canadian Forces College, 2013), 45.

Sense is the next function that will be taken into consideration and argued that it is also manifested within the cyber environment. This function is responsible for integrating sensor and sensor analysis into one single concept to provide commanders with timely and relevant information critical for making key decisions.[23] This is accomplished through ISR assets such as UAVs, radars, networks and other various assets, most of which use cyber in order to obtain, process and deliver the information. As stated earlier, it is important to not only understand one's own network but to also know the adversaries system. This assists in identifying its vulnerabilities and to get into their network to obtain important information that will assist commanders in making their plans. This is achieved through either CNA or CNE activities.

Exploiting and attacking an adversary's network will not only help to identify the vulnerabilities within their network but will also assist in acquiring sensitive and relevant information on the adversary. This can also have an impact on the civilian population by identifying economic or structural network vulnerabilities that can be targeted. It is through ISR that the information is gathered and therefore heavily reliant on the cyber domain to ensure that key decision makers have the right information at the right time. Intelligence is a key component in any decision making process and cyberspace has the ability to allow governments and stakeholders to assess the effects of cyber-attacks. This allows for the opportunity to mitigate the risks and to streamline their cyber security.[24] Information integrity is an important factor to consider and must be verified to prevent potentially deadly consequences for a commander in battle should misinformation be

[23] Canada. Department of National Defence, *Land Operations 2021 Adaptive Dispersed Operations the Force Employment Concept for Canada's Army of Tomorrow*, 12.

[24] Gendron and Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, 48.

provided by the adversary.[25] This adversarial information sabotage could be extremely dangerous and cause significant harm but is only one of the few counter arguments for this function. This counter, however, is weak because the sense function would still be occurring within the cyber domain. It is not the type of information collected that is important but rather the information collection itself. Misinformation by an adversary could also be obtained physically by personnel on the ground during a reconnaissance operation if the adversary were to leave false documents in an abandoned position or create false battle positions to confuse their adversaries. This can occur not only within the land environment but in all environments as they all incorporate a human factor and not just cyber. Due to the fact that sense can be affected in both the physical and cyber domain demonstrates that it is just as suited at addressing the sense function as the other environments.

The Act function is explicitly addressed in cyberspace and is defined in Canada's Land Operations as follows:

> Act integrates manoeuvre, firepower and offensive information operations [influence activities] to create a desired effect and end state through the synchronized application of the entire array of available capabilities, both lethal and non-lethal.[26]

Influence activities involve the distribution of key messages, conducting show of force demonstrations or by providing assistance to individuals or organizations. These can be conducted physically by individuals or by using the cyber domain. The use of telecommunications or internet is an extremely useful and powerful way to conduct these

[25] McGuffin and Canadian Forces College, *Soldiers of FORTRAN: Militarization of the 5th Dimension*, 43.

[26] Canada. Department of National Defence, *Land Operations 2021 Adaptive Dispersed Operations the Force Employment Concept for Canada's Army of Tomorrow*, 12.

activities as they can be distributed and received by a much wider audience due to the unlimited boundaries of the internet and cyber. The Act function, like many of the other operational functions, can be heavily dependent on cyber and its ability to conduct Computer Network Attacks (CNA) as well as the advantages that can be attributed to conducting CNA operations.

There are three main types of attacks that have been identified by the Canadian government as cyber threats: state sponsored cyber espionage and military activities, terrorist use of the internet, and cybercrime.[27] There have been reports of foreign states stating that a central element of their military strategy is cyber-attacks, which are designed to sabotage an adversary's infrastructure and communications. Further to this, cyber actors will also attack emergency response and public health systems in order to put lives at risk.[28] There is no true safe organization or environment when it comes to threats of cyber-attacks.

Terrorist networks are also embracing the 21st century technology and using the internet to support their insurgency through recruitment, fundraising and propaganda activities as demonstrated by ISIS and al-Qaeda.[29] It is not just the terrorist groups that can take advantage of cyberspace but friendly forces can also leverage cyber capabilities to achieve mission objectives. To win the hearts and minds of the population it is important to deliver key messages through the cyber domain as that is the modem of

[27] Canada. Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*, 5.

[28] *Ibid*.

[29] *Ibid*.

communication amongst the new generation. In 2010, cyberspace was considered as the global commons where more than 1.7 billion people were linked together.[30]

There are several reasons that make cyber-attacks attractive. One of the most significant advantages is the difficulty in identifying an attacker who is not bound by state territorial borders. Globalization of cyber allows an adversary to conduct a cyber-attack through a network that can begin in one country and end in another creating significant jurisdictional and attributional difficulty linking an attack to the originator. This makes attribution difficult and anonymity a success. To further avoid attribution of cyber activities, states are using non-state actors allowing them to disguise their own involvement.[31] Another military advantage of conducting cyber-attacks is that the enemy can be neutralised without placing friendly troops' lives at risk as well as neutralising the enemy without causing bloodshed on the other end[32] as stated in Jeffery Carr's definition of cyber warfare. This is a tremendous benefit both politically for the government but also personally for commanders and their troops.

One may argue that the applicability of cyber within the Act function may be speculative and that it may actually be more comparable to that of a special forces capability supporting the other environments efforts.[33] Other arguments against the value and validity of offensive cyber also include the uncertainty of the outcome from the attack and the deterrent value and effectiveness of the weapon following the attack.[34]

[30] *Ibid*., 2.

[31] Gendron and Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, 29.

[32] Steve Ranger, "Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar," TechRepublic, http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/ (accessed 8 March, 2015).

[33] McGuffin and Canadian Forces College, *Soldiers of FORTRAN: Militarization of the 5th Dimension*, 1.

[34] Fred Schreier, "On Cyberwarfare" DCAF Horizon 2015 Working Paper No. 7), 96-97.

There is no means by which to measure or calculate the deliberate or collateral damage that may occur from an attack making it more risky than conducting a regular kinetic attack. Furthermore, once the attack has been conducted it is possible that the weapon will no longer be of value as the capabilities of the weapon will have been exposed and it is possible to now build a defence against that type of attack and therefore render it useless. This author would disagree with these statements simply due to the number and degree to which attacks are conducted in order to degrade or disrupt an adversary. One example of such an attack that can have a significant impact on the civilian or military environment is the attack on supervisory control and data acquisition (SCADA) networks.

SCADA networks are often used to keep dams from overflowing, electrical grids from collapsing and transportation networks from malfunctioning.[35] An example of a successful cyber-attack on a SCADA system was the Stuxnet worm that was allegedly masterminded by the U.S. and caused damage and delay to the Iranian nuclear program.[36] The Stuxnet worm attacked and disabled the nuclear centrifuges that were operated by a SCADA system and overloaded them by overriding the primary software.[37] The damage was substantial and significantly disrupted the nuclear program creating a serious delay in any advancement of the program. Attacks on this type of a network can have serious implications on a population and adversary while at the same time creating significant advantages for the originator, all of which further validates the applicability of the Act function within cyberspace.

[35] Canada. Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*, 12.

[36] Ranger, *Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar*.

[37] Schreier, *On Cyberwarfare*, 114.

The next operational function to address is Shield, which is associated with defence. Shield is the operational function that provides protection, which facilitates forces' survivability and freedom of action.[38] With the advancement in technology and the increased dependency on the digital network, vulnerabilities will increase and therefore require a growing importance on the ability to protect that network. Now that everyone is becoming electronically and digitally connected there is a greater threat to these systems. Just as friendly forces wish to determine and find vulnerabilities in the adversaries' network, they will attempt to do the same. In 2013, a cyber security study indicated that 36% of Canadian businesses were subject to cyber-attacks[39] while in the U.S. the IT association ISACA conducted a survey that showed 46% of respondents expect to see a cyber-attack against their organization in 2015.[40] The only way to prevent attacks from being successful is to create a strong Computer Network Defence (CND) capability which is the primary role of cyber operations in the Shield function.

This function will quite often work simultaneously with Sense or be in a supporting role to the Sense function. In order to defend against adversary attacks one must have situational awareness of the network environment, which is where the Sense function is able to assist. Furthermore, once the threat of an attack, or actual attack, occurs on a network then a response must be taken to defend the network, which is the role of the Shield function. Whether at sea, in the air, or on land the same response is provided by each environment. Once again, this reveals the fact that cyberspace

[38] Canada. Department of National Defence. B-GL-300-001/FP-001, *Land Operations*, 4-20.

[39] David Paddon, "Cyber Attacks have Hit 36 Per Cent of Canadian Businesses, Study Says," *The Globe and Mail*18 Aug 2014.

[40] "As State of the Union Tackles Cybersecurity, New ISACA Survey shows 86% See a Cybersecurity Skills Shortage." ISACA, http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/As-State-of-the-Union-Tackles-Cybersecurit-New-ISACA-Survey-Shows-86-See-a-Cybersecurity-Skills-Shortage.aspx (accessed 8 March, 2015).

adequately addresses and includes the Shield function within its domain just as the other strategic environments do. This is common not just in all of the environments within the military but in governments as well when concerned about protecting critical infrastructure and their population, further substantiating why cyber should be considered a new battlespace as some of the following examples will show.

Canada's cyber security strategy was built on three pillars: securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online.[41] Knowing that cyber was becoming a greater threat and that the use of the internet and technology was on the rise, the Government of Canada understood the requirement to build a strategy focused on CND in order to protect itself from attack. Since many government infrastructures work on the SCADA system and attacking it could cause significant harm to the local population, it is important to have a strong CND. According to former Director of U.S. National Intelligence, Mike McConnell, the main priorities of the U.S. government should be to protect its critical infrastructure from cyber-attack, which includes the electric power grid, transportation network and the financial sector.[42] As indicated earlier, terrorist groups like al-Qaeda and ISIS continue to keep apprised with the advancement in technology and will also use it to conduct strategic attacks against countries' critical infrastructure and Canada must be prepared to defend against such attacks.[43] Their vision of doing so is seen as an economic jihad focussing on critical infrastructure like banks,

[41] Canada. Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*, 9.

[42] Gendron and Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, 46.

[43] Canada. Public Safety Canada, *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy* (Ottawa: Government of Canada, 2013), 26.

government-owned property and energy infrastructure in order to cause maximum losses to the economy vice maximum casualties.[44]

Terrorist groups are not the only organizations a state must defend against. In 2006, U.S. organisations were hacked by Chinese military hackers, believed to be from the Chinese People's Liberation Army, to steal information that would be useful to competitors in China.[45] These men were charged by the U.S. and it was the first time that charges were laid against a state actor for such an offence.[46] In 2008, U.S. Department of Defence computer networks were compromised when a malicious code was uploaded onto a network run by U.S. Central Command. This code allowed data to be transferred to servers under foreign control and deliver operational plans into the hands of an unknown adversary.[47] The sophistication and damage that can be caused by these attacks demonstrates that organizations need to be prepared to defend against both state and non-state actors and that the cyber environment is becoming more popular as a means of waging war and therefore requires a strong CND capability.

NATO has recognized the importance of cyber defence identifying it as one of its core collective defence tasks[48] and established the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) following the cyber-attacks against Estonia in 2007.[49] Along with the establishment of the centre, NATO also developed a Cyber Defence

[44] Gendron and Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, 23.

[45] Steve Ranger, "Chinese 'Military Hackers' Charged with Cyber Espionage Against US Companies," ZDNet, http://www.zdnet.com/article/chinese-military-hackers-charged-with-cyber-espionage-against-us-companies/ (accessed 8 March, 2015).

[46] *Ibid*.

[47] Lynn III, *Defending a New Domain*, 97-108.

[48] "Cyber Security." North Atlantic Treaty Organization, www.nato.int/cps/en/natohq/topics_78170.htm (accessed 11 April, 2015).

[49] Gergely SZENTGÁLI, "The NATO Policy on Cyber Defence: The Road so Far," *AARMS: Academic & Applied Research in Military Science* 12 (06, 2013), 84.

Policy that was accepted and established in 2008. The intent of the Policy was to emphasise the need for NATO and its nations to protect key information systems; share best practices; and assist Allied nations in countering a cyber-attack if requested.[50] Due to the ever changing cyber threat, this policy continues to be reviewed and in June 2014 the NATO Defence Ministers endorsed a new updated policy.[51]

There are some challenges with cyber that must also be taken into consideration. Since technology is continuously changing through technological advancement, cyberspace and defence is constantly in a state of flux and must be flexible. This constant change, with opponents developing new methods and ways to exploit vulnerabilities, results in expenses to conduct more research and development in order to defend against attacks. NATO considered cyber to be such an important factor that in 2012 it was determined that 58 million euros would be dedicated to upgrading its network security.[52] Although there may be challenges, constant advancement in technology requiring constant changes and significant cost to protect the network, it still does not override the importance of CND and the requirement to protect networks.

Once attacked or the threat of an attack is sensed, measures and actions must be taken to protect one’s force, organization or critical infrastructure. It is important to have a CND capability that is capable of protecting critical infrastructure and networks against attacks. It is also important that governments and organizations work together to keep abreast with the latest defence technology and mechanisms no matter the cost as cyber

[50] *Ibid*.

[51] "Cyber Security."

[52] SZENTGÁLI, *The NATO Policy on Cyber Defence: The Road so Far*, 86.

will soon be the new environment of waging war and likely considered to be a new battlespace.

Sustain is the final operational function to be addressed. This function integrates strategic, operational and tactical levels of support to generate and maintain force capability.[53] Sustain can be referred to in the cyber domain as the capability to maintain the networks in use by a force. Once again with the greater dependence and use of technology within society and the military sustainment of the networks will be critical for success. If the networks are not sustained then commanders will lose situational awareness along with command and control of their forces. Also, in order for the networks to be sustained then they must also be protected meaning that Shield would also support Sustain.

Further to this, the future Adaptive Dispersed Operations (ADO) concept for Canadian military forces envisions an operating environment that will involve complex, multidimensional conflict in a non-contiguous dispersed operational framework.[54] This environment will require adaptive forces to be net-enabled[55] to ensure communication, command and control between all forces to maintain a COP for the commander as forces will potentially be widely dispersed throughout the area of operation. Along with the priority to sustain this network for the reasons stated is also the focus of logistics on the availability of the network and its components to maintain its forces at every layer.[56] Logistics and the sustainment of one’s force will be accomplished through a network

[53] Canada. Department of National Defence, *Land Operations 2021 Adaptive Dispersed Operations the Force Employment Concept for Canada's Army of Tomorrow*, 12.

[54] *Ibid*., 16.

[55] *Ibid*., 18.

[56] Canada. Department of National Defence, *No Man's Land: Tech Considerations for Canada's Future Army*, 5-38.

enabled system that will ensure distribution and supply of equipment and materiel. This exhibits that the cyber environment is in fact a key enabler of the Sustain function.

One could argue that the actual Sustain function does not occur in cyberspace and therefore negates the possibility of cyber being its own environment. This would indicate that the provision of information technology equipment, the links between them and the specialists to install, repair and operate the systems all occur in real space.[57] Albeit true, this is still a weak argument to disprove cyberspace's ability to be its own distinct environment. Just because the sustainment may be driven by an occurrence in real space does not make this any different than the other environments. Although ships and aircraft have the ability to conduct air to air refueling or replenishment at sea, many other sustainment factors occur outside of their specific domain. For example, in order for a ship to undergo a refit or to be repaired it must be docked at shore and requires personnel and materiel from land to work on it. This is also true for any air and space sustainment requirements to fix broken equipment, etc. Not all sustainment can occur at sea, in the air or in space just as the ability for cyber to sustain forces will require external input or assistance outside of its domain. The reliance on the digital sphere in operations needs to be sustained and is required for the sustainment of forces as described by the focus of logistics on the network and shows the ability of cyberspace to address the Sense function.

[57] McGuffin and Canadian Forces College, *Soldiers of FORTRAN: Militarization of the 5th Dimension*, 46.

## NATO AND CYBER

Other than just the applicability of all five of the operational functions to cyber, there are other reasons that constitute the validity of cyberspace being its own strategic environment as well as the new battlespace. There has been much debate within NATO and amongst its allies as to whether or not Article 5 of the North Atlantic treaty is applicable to a cyber-attack. The implication of cyber provoking an Article 5 response is that an armed attack against one member state is to be considered an attack against all and that Parties to the treaty will come to the aid of another.[58] In the past, this article was only applicable to an armed attack but has now changed due to the recent update to the NATO cyber defence policy in 2014. According to the new policy approved by the defence ministers in June 2014, NATO now recognizes that international law applies to cyberspace and therefore an attack of such a nature can invoke a collective defence response in accordance with Article 5.[59] This further validates the importance that NATO has placed on cyberspace, as they now consider a cyber-attack equivalent to that of a physical attack. Before the release of this information of a cyber-attack invoking an Article 5 response and the cyber defence policy update, a cyber-attack was only considered to be a political attack and therefore not fall within the definition or provision of Article 5.[60]

NATO is not the only organization to place a high level of importance on cyber. There are over 100 other nations that have created cyber commands responsible for the

[58] "The North Atlantic Treaty 4 April 1949." NATO, http://www.nato.int/cps/en/natolive/official_texts_17120.htm (accessed 15 April, 2015).

[59] "NATO Summit Updates Cyber Defence Policy." NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html (accessed 11 April, 2014).

[60] SZENTGÁLI, *The NATO Policy on Cyber Defence: The Road so Far*, 87.

defence and sustainment of their networks.[61] The U.S. Pentagon formally recognizes cyberspace as a new domain of warfare and in May 2010 created the U.S. Cyber Command as part of U.S. Strategic Command.[62] As far back as 2004 the Chairman of the Joint Chiefs of Staff confirmed in their National Military Strategy that, "the Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains" and in March 2005 the U.S. identified in their National Defence Strategy that cyberspace was the new theater of operations.[63]

Not only are NATO and allied forces taking cyber seriously by developing cyber defence policies and creating cyber commands but nations such as China and Russia began developing their cyber domains further exemplifying the importance of allied cyber defence. China has formed cyberspace battalions and regiments and in 1999 they reported that, "Internet warfare is of equal significance to land, sea and air power and requires its own military branch."[64] The fact that NATO continues to review and update their cyber defence policy on a continuous basis, has established the CCDCOE, many nations have established cyber commands, and that cyber-attacks have now been approved and authorized to invoke an Article 5 collective defence response further exhibits that cyber-attacks are increasing, becoming more dangerous and can be the new battlespace.

[61] Ranger, *Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar*.

[62] Lynn III, *Defending a New Domain*, 97-108.

[63] Keith B. Alexander, "Warfighting in Cyberspace," *JFQ: Joint Force Quarterly*, no. 46 (Summer2007, 2007), 59.

[64] *Ibid*.

## CONCLUSION

The advancement in technology over the centuries from the earliest of battles in the Peloponnesian War to the most recent time has been extraordinary and highly developed. From the early days of battling face to face with fists and swords to now being separated by thousands of kilometers with no boundaries in sight is something not to be taken lightly. Cyberspace is the current and future way in which battles will be fought and the advantages are significant. Attribution of an attack is extremely difficult leading to a great deal of anonymity to an attacker. This anonymity can also be related to the absence of geographic boundaries in cyberspace. Individuals, groups, state and/or non-state actors can reside anywhere in the world and can attack anywhere in the world regardless of the distance and are able to do so without the possibility of being detected or putting their lives at risk. Imagine if this technology had been around during the time of World War II when the allied forces began their air bombing campaign against the German industry in an attempt to create economic collapse as well as rendering the enemy incapable of sustaining military operations.[65] Had technology been in place at that time a cyber-attack against a SCADA system would have proven just as effective without causing loss of life to innocent civilians or incurring significant costs as occurred. It would have also allowed for attacks to occur without putting allied forces lives in danger by having to fly aircraft in to enemy territory.

There is an increased dependence on digital networks and internet based communications and nothing seems to be accomplished without some form of cyber

[65] Robert Anthony Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, N.Y.: Cornell University Press, 1996), 259.

activity being related to it. This over reliance and dependency has led to vulnerabilities in all environments. Cyber-attacks are on the rise and becoming more frequent, organised and costly with respect to the damage they can inflict on government, economic and military networks as well as all critical infrastructure.[66] This creates an importance on defending one's networks and creating a cyber defence policy and strategy just as NATO and other nations have done.

The advantages of cyberspace are substantial and the increased reliance on it cannot be disputed. Cyberspace is capable of addressing all five operational functions in a military context, which is important when determining whether or not a domain is to be considered separate from the already defined strategic environments of land, sea, air and space. The emphasis that is placed on cyber and developing cyber defence policies, strategies and commands within the world, demonstrates that concern of cyber-attacks is real. Further to this, the fact that cyber-attacks appear to be on the rise validates that it is the future battlespace in which battles will be fought either in isolation or along with other conventional means.

[66] SZENTGÁLI, *The NATO Policy on Cyber Defence: The Road so Far*, 85.

# Bibliography

"As State of the Union Tackles Cybersecurity, New ISACA Survey shows 86% See a Cybersecurity Skills Shortage." ISACA. Accessed 8 March, 2015. http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/As-State-of-the-Union-Tackles-Cybersecurit-New-ISACA-Survey-Shows-86-See-a-Cybersecurity-Skills-Shortage.aspx.

"CSE: What do we Know about Canada's Eavesdropping Agency?" CBC News. Accessed 8 March, 2015. http://www.cbc.ca/news/canada/cse-what-do-we-know-about-canada-s-eavesdropping-agency-1.1400396.

"Cyber Security." North Atlantic Treaty Organization. Accessed 11 April, 2015. www.nato.int/cps/en/natohq/topics_78170.htm.

"NATO Adopts New Policy Calling for Collective Defence Against Cyber-Attacks." *Network Security* 2014, no. 9 (09, 2014).

"NATO Summit Updates Cyber Defence Policy." NATO Cooperative Cyber Defence Centre of Excellence. Accessed 11 April, 2014. https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html.

"Nato to Adopt New Cyber Defence Policy." *ComputerWeekly: IT Security* (.

"The North Atlantic Treaty 4 April 1949." NATO. Accessed 15 April, 2015. http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

"Oxford Dictionaries Language Matters.”. Accessed 12 April, 2015. http://www.oxforddictionaries.com/definition/english/cyberwar.

Alexander, Keith B. "Warfighting in Cyberspace." *JFQ: Joint Force Quarterly* no. 46 (Summer2007, 2007): 58-61.

Canada. Department of National Defence. *C4ISR Capability Development Plan*. Ottawa: DND Canada, 2009.

———. *Canadian Forces Computer Network Operations (CNO) Policy Draft Version 2.1*. Ottawa: DND Canada, 2009.

———. *Land Operations 2021 Adaptive Dispersed Operations the Force Employment Concept for Canada's Army of Tomorrow*, edited by Godefroy, Andrew B. Ottawa: DND Canada, 2007.

———. *No Man's Land: Tech Considerations for Canada's Future Army*. Kingston, ON: Army Publishing Office, 2014.

Canada. Department of National Defence. A-FD-005-002/AF-001. *Integrated Capstone Concept*. Winnipeg: 17 Wing Winnipeg Publishing Office, 2009.

Canada. Department of National Defence. B-GL-300-001/FP-001. *Land Operations*. Ottawa: DND Canada, 2008.

Canada. Department of National Defence. B-GL-358-001/FP-001. *Land Force Information Operations Electronic Warfare*. Ottawa: DND Canada, 2004.

Canada. Public Safety Canada. *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy*. Ottawa: Government of Canada, 2013.

———. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa: Govt. of Canada, 2010.

———. *Cyber Incident Management Framework for Canada*. Ottawa: Government of Canada, 2013.

Carr, Jeffery. *Inside Cyber Warfare, Mapping the Cyber Underworld*, edited by Loukides, Mike. 2nd ed. Sebastopol, CA: O'Reilly Media, Inc., 2011.

Colarik, Andrew M. and Lech Janczewski. *Cyber Warfare and Cyber Terrorism*. Hershey, PA: Idea Group Reference, 2007.

Gendron, Angela and Martin Rudner. *Assessing Cyber Threats to Canadian Infrastructure*. Ottawa: Government of Canada, 2012.

Godefroy, Andrew B. and Canada. Dept. of National Defence. *Land Operations 2021: Adaptive Dispersed Operations: A Force Employment Concept for Canada's Army of Tomorrow*. B-Gl-310-001/ag-001. Kingston, Ont.: Directorate of Land Concepts and Doctrine, 2007.

Goldstein, Matthew, Nicole Perlroth, and Michael Corkery. "DealBook: Neglected Server Provided Entry for JPMorgan Hackers." *NYT > Business Day* (2014).

Hildebrandt, Amber, Michael Pereira and Dave Seglins. "CSE Monitors Millions of Canadian Emails to Government." CBC News. Accessed 8 March, 2015. http://www.cbc.ca/news/canada/cse-monitors-millions-of-canadian-emails-to-government-1.2969687.

Hooker, Richard D. *Maneuver Warfare: An Anthology*. Novato, CA: Presidio, 1993.

Lynn III, William J. "Defending a New Domain." *Foreign Affairs* 89, no. 5 (Sep, 2010): 97-108.

McGuffin, W. C. and Canadian Forces College. *Soldiers of FORTRAN: Militarization of the 5th Dimension*. Masters Thesis (Canadian Forces College). Vol. JCSP/PCEMI 39. Toronto, Ont.: Canadian Forces College, 2013.

McLeary, Paul. "NATO Chief: Cyber can Trigger Article 5." *Defense News* (25 March 2015, 2015).

Osborne, Charlie. "Over 90 Percent of Data Breaches in First Half of 2014 were Preventable." ZDNet. Accessed 8 March, 2015. http://www.zdnet.com/article/over-90-percent-of-data-breaches-in-first-half-2014-were-preventable/.

Paddon, David. "Cyber Attacks have Hit 36 Per Cent of Canadian Businesses, Study Says." *The Globe and Mail,* 18 Aug 2014.

Pape, Robert Anthony. *Bombing to Win: Air Power and Coercion in War*. Cornell Studies in Security Affairs. Ithaca, N.Y.: Cornell University Press, 1996.

Ranger, Steve. "Chinese 'Military Hackers' Charged with Cyber Espionage Against US Companies." ZDNet. Accessed 8 March, 2015. http://www.zdnet.com/article/chinese-military-hackers-charged-with-cyber-espionage-against-us-companies/.

———. "Hostile State-Sponsored Hackers Breached Government Network." ZDNet. Accessed 8 March, 2015. http://www.zdnet.com/article/hostile-state-sponsored-hackers-breached-government-network/.

———. "Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar." TechRepublic. Accessed 8 March, 2015. http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/.

———. "NATO Updates Cyber Defence Policy as Digital Attacks Become a Standard Part of Conflict." ZDNet. Accessed 11 April, 2015. http://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/.

Schreier, Fred. "On Cyberwarfare." DCAF Horizon 2015 Working Paper No. 7, 2015.

SZENTGÁLI, Gergely. "The NATO Policy on Cyber Defence: The Road so Far." *AARMS: Academic & Applied Research in Military Science* 12, (06, 2013).

Walkling, J. C. and Canadian Forces College. *Considerations: Canadian Forces' Efforts in the Electromagnetic Spectrum and Cyber Operating Environment*. Masters Thesis (Canadian Forces College). Vol. JCSP/PCEMI 39-78. Toronto, Ont.: Canadian Forces College, 2013.