National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

DEVELOPING A COMPREHENSIVE CYBER CAPABILITY FOR THE CANADIAN ARMED FORCES

Major A.E. Ferriss

JCSP 40

Exercise *Solo Flight*

Disclaimer

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.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2014.

PCEMI 40

Exercice *Solo Flight*

Avertissement

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.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2014.

Canada

CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES

JCSP 40 / PCEMI 40

SOLO FLIGHT

DEVELOPING A COMPREHENSIVE CYBER CAPABILITY FOR THE CANADIAN ARMED FORCES

By Major A.E. Ferriss

12 May 2014

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.

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.

Word Count: 5234

Compte de mots : 5234

> "those who win every battle are not really skillful -- those who render others' armies helpless without fighting are the best of all."
>
> SunTzu (544-496 BC)

Sun Tzu's concept of winning a war without fighting was likely deemed laughable by Carl Von Clausewitz whose theories suggested that war can only be won by force in which one army destroys another army in one, or a combination of decisive victories. In Clausewitz's defense, few philosophers or theorists could have predicted the monumental changes in technology that would shape the nature of warfare in the coming centuries. Conventional militaries of the 21st century have become highly dependent upon technology to move (using GPS), to communicate (using computers and digital communications networks) and even fight (using GPS guided munitions and unmanned aerial vehicles (UAVs)).

The information age has given rise to a whole new arena for militaries to exploit and exercise military power.[1] Traditionally, power projection has been defined as the ability of a state to conduct expeditionary warfare.[2] For a conventional force this has meant the ability to project naval, land and air power abroad. According to US Army doctrine, land power is, "the ability – by threat, force, or occupation – to gain, sustain, and exploit control over land, resources, and people."[3] Similarly, the US Department of the Navy identifies sea power as "the sum of a nation's capabilities to implement its interests in the ocean, by using the ocean areas for political, economic, and military activities in peace or war to attain national objectives – with principal components of sea power being naval power, ocean science, ocean industry, and ocean

---

[1] V.P. Österberg. Military theory and the concept of Jointness. Last Accessed on 7 May 2013, http://forsvaret.dk/fak/documents/fak/fsmo/specialer/03-04/military_theory_and_concept_of_jointness.pdf

[2] U.S. Department of Defence, "Joint Operational Access Concept (JOAC)," last Accessed on 7 May 2014, http://www.defense.gov/pubs/pdfs/joac_jan%202012_signed.pdf

[3] U.S. Department of the Army, ADRP 3-0, Unified Land Operations (Washington, DC: Department of the Army, 2012), Glossary-4

commerce."[4] Even still, the Royal Air Force defines air power as, "the ability to project power from the air and space to influence the behaviour of people or the course of events."[5] What these definitions have in common is the understanding that given the domain, the respective military looks to pursue a position whereby they can control all aspects of the domain in order to influence the battlespace and establish the conditions for victory.

The continuous evolution of technology has expanded mankind's reach in as much as a new, completely man made domain now exists: cyberspace.[6] In 2009, the CAF's Chief of Force Development (CFD) proposed that the cyberspace be recognized as a new domain in which military forces and adversaries will attempt to exercise power and influence.'[7] Other nations have identified the need for cyber capabilities. The US Air Force, widely considered to be at the forefront of cyber capability development has taken the lead on cyber and has changed its definition of air power to, 'Air power is the ability to project military power or influence through the control and exploitation of air, space, and cyberspace to achieve strategic, operational, or tactical objectives'.[8] Appreciating the importance and cross-service implications of cyberspace the US created an integrated military-civilian Cyber Command to coordinate America's cyber agenda. There is ongoing discussion among scholars as to whether cyberspace is actually its own

---

[4] William L. Brackin, *Navy Orientation* (Washington, DC: United States Government Printing Office, 1991), 1

[5] Ministry of Defence, British Air and Space Power Doctrine, AP 3000 (Shrivenham, UK: Air Staff. 2009), 7

[6] Department of Defense, Strategy for Operating in Cyberspace. last Accessed on 7 May 2014. http://www.defense.gov/news/d20110714cyber.pdf

[7] Chief of Force Development. A-FD-005-002/AF-001. Integrated Capstone Concept. Winnipeg, MB: Department of National Defence (17 Wing Publishing Office), 20 October 2009. http://publications.gc.ca/collections/collection_2012/dn_nd/D2-265-2010-eng.pdf

[8] U.S. Department of the Air Force, *Air Force Doctrinal Document 1* (Washington DC: Department of the Air Force, 2011), 11.

domain and whether, or not, it ought to simply be included as an additional sub-component of air, sea or land power, much like what the US Air Force has done with including cyber in the definition of air power.[9,10] This paper will not attempt to prove that cyber is its own domain, or that cyber power is the appropriate term to identify a nation's ability to control activities in the electromagnetic spectrum. For commanders, computers and networks are strengths and weaknesses and adversaries will attempt to gain freedom of movement in the medium in order to leverage the capabilities that technology offers. Whether this medium is a domain, an environment, or something completely different is an exercise in semantics. Domain and environment will be used synonymously throughout the paper to describe the 'space' where cyber activities are conducted.

Many definitions of cyber and cyberspace have been presented by academics and military officials. In their article, *Toward Attaining Cyber Dominance,* researchers Martin Stytz and Sheila Banks suggest that cyberspace is,

> 'composed of four elements: (1) data, (2) computing technologies (such as computer hardware, computer software, computer networks/infrastructure, network protocols, virtualization and cloud computing), (3) information analysis/comprehension technologies (including information visualization, artificial intelligence, collaboration, data mining technologies and big data technologies) and (4) information interaction/management technologies (including human-computer interaction, intelligence agents, human intent differencing and database technologies).'[11]

---

[9] Vincent Manzo, "Deterrence and Escalation in Cross-domain Operations Where Do Space and Cyberspace Fit?," JFQ, issue 66, 3rd Quarter 2012, 9.

[10] Matt Murphy, "War in the fifth domain," The Economist, Last Accessed on 7 May 2014, http://www.economist.com/node/16478792.

[11] Martin Stytz and Sheila Banks. Toward Attaining Cyber Dominance. Strategic Studies Quarterly. Vol 8 no. 1 (Spring 2014): 81.

Conversely, the Canadian Cyber Security Strategy (2010) defines cyberspace as, 'the electronic world created by interconnected networks of information technology and the information on those networks'.[12] The US Cyber Space Review (2009) provides another perspective suggesting that cyberspace is, 'the globally interconnected digital information and communications infrastructure [that] underpins almost every facet of modern society.'[13] For the purpose of this essay, the definition proposed by the Canadian Cyber Security Strategy (2010) will be adopted as the discussion will be grounded in a Canadian context.

This paper will avoid the debate regarding hacktivists, organized crime and jurisdiction between police and military officials by framing the debate around wartime, or armed conflict. In that context, the paper will argue that the Canadian Armed Forces (CAF) needs to develop offensive and defensive cyber capabilities to provide commanders with the broadest range of capabilities to render an opponent ineffective in order to obtain an identified military end state. To support this thesis, the paper will break down military efforts in the cyber domain into three distinct activities: Computer Network Defence (CND), Computer Network Exploitation (CNE) and Computer Network Attack (CNA).[14] For each activity, the paper will demonstrate the capability that the activity provides for a commander and the force generation possibilities surrounding the employment of the capability.

Computer Network Defence

[12] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London: Routledge, 2007), 36.

[13] Ibid. 36

[14] J.C. Walking. "Considerations: Canadian Forces Efforts in the Electromagnetic Spectrum and Cyber Operating Environment" (master's thesis, Canadian Forces College, 2013), 41.

CND is the least controversial element of cyber power. It is the application of technologies that protect one's cyber assets from cyber-attacks so that data and networks remain useable to attain an end state.[15] Protection involves preventing intruders from entering the system by continuously updating software and security patches that protect against code based vulnerabilities. It also means ensuring firewalls are adequate to prevent intrusion and that the physical components of the network, the hardware, are correctly installed, maintained and upgraded to reduce the probability of intrusion. In 2010, the Canadian government released *Canada's Cyber Security Strategy*, which clearly states the government's policy on CND:

> The Department of National Defence and the Canadian Forces will strengthen their capacity to defend their own networks, will work with other Government departments to identify threats and possible responses, and will continue to exchange information about cyber best practices with allied militaries.[16]

Maintaining a robust cyber defence posture is extremely important for the CAF/DND. Operational planning, intelligence gathering, storage and analysis and dissemination of orders are just some examples of activities that occur over departmental classified and unclassified networks. Network breaches could provide adversaries with operationally sensitive information that could put Canadian troops or the nation's strategic objectives in jeopardy. In addition to protecting the integrity and secrecy of information transmitted in the cyber domain, there is also the requirement to defend against attacks that could deny CAF the ability to use their own networks. During the CAF mission in Afghanistan, the Canadian Army expended significant

---

[15] Martin Stytz and Sheila Banks. Toward Attaining Cyber Dominance. Strategic Studies Quarterly. Vol 8 no. 1 (Spring 2014): 81.

[16] Government of Canada, *Canada's Cyber Security Strategy: For A Stronger and More Prosperous Canada* (Ottawa: Public Safety, Canada, 2010), last accessed 1 May 2014, http://www.publicsaftey.gc.ca/prg/ns/cybr-scrty/ccss-scc-eng.aspx

resources in digitizing the battlefield through the employment and expansion of the Land Command Support System (LCSS). LCSS is a,

> 'highly integrated tactical system composed of many communication, networking and information management sub-systems that support the Army-wide command function. It forms a part of every Canadian Army vehicle, weapon platform and headquarters and is made up of numerous hardware, firmware and software elements…. The Land Command Support System will continue to evolve over time thanks to initiatives such as the Intelligence Surveillance Target Acquisition and Reconnaissance Project, the Land Command Support System Life Extension Project which was launched in 2010, and other related endeavours.[17]

The Royal Canadian Air Force (RCAF) and Navy (RCN) have also become dependent on networks to plan, coordinate, access and analyze intelligence and maneuver. The RCAF is evaluating a wider use of UAVs in surveillance and other operations. The control and data collected by UAVs is done through networks and computer systems that need to be protected. In 2006, CF-18s were outfitted with link 16.

> 'Link 16 provides real-time, jam-resistant secure transfer of combat data, voice and relative navigation information between widely dispersed battle elements. Participants gain situational awareness by exchanging digital data over a common communication link that is continuously and automatically updated in real time, reducing the chance of fratricide, duplicate assignments or missed targets.'[18]

Similarly, the RCN has undergone a number of upgrade projects such as the Digital Maritime Operations Plot (DMOP), the Electronic Charts Precise Integrated Navigation System (ECPINS) and the Common Operational Picture – Image Display Server (COP-IDS) all with the intention of leveraging technology to increase the capabilities of Canada's fleet.

---

[17] Canadian Armed Forces, "The Land Command Support System," last Accessed 7 May 2014, http://www forces.gc.ca/en/news/article.page?doc=the-land-command-support-system/hgq87xe4

[18] Defense Industry Daily. Canadian CF-18s Finally Get Link 16, While H-92s Get Link 11. Last Accessed 7 May 2014. http://www.defenseindustrydaily.com/canadian-cf18s-finally-get-link-16-while-h92s-get-link-11-01720/

The implementation of such 'digitization' projects highlights the trend toward a more network enabled battlefield. To date, CAF has used 'cyber' technologies for command and control, intelligence gathering and navigation. However, the technologies are capable of delivering much more aggressive effects. UAVs for example are used by some nations to remotely deliver kinetic effects on the battlefield. Canada does not currently employ UAVs to achieve kinetic effects, but one day that policy may change. The Americans witnessed the importance of defending UAV networks when, in 2011, a CIA operated drone fell into Iranian hands. According to Iranian officials, an Iranian engineer was able to take control of the drone, change its flight path and had it land near the city of Kashmar.[19] American government officials claimed the drone had a glitch that caused operators to lose control of the drone and dismissed the Iranian claims. The next year, researchers from the University of Texas at Austin's Radionavigation Laboratory hijacked a small surveillance drone by infiltrating the machine's navigation device. The academics were able to override the drone main control channel and thus change its flight path.[20] In both cases, the drones were unarmed surveillance UAVs, however, the stakes may have been much higher had drones been carrying ordnances.

The ways that technology is being used on the battlefield has made conventional militaries more efficient fighting machines.[21] This is not to say that a modern military without a network would be rendered helpless. Training is still conducted to develop basic skills, however, with pressure to decrease training days and the arrogance of western militaries in their perception of cyber dominance has reduced the amount of training on low tech combat skills. The trend is

---

[19] Daily News. Iran claims it can control captured American drone. Last Accessed 7 May 2014. http://www.nydailynews.com/news/world/iran-claims-control-captured-american-drone-article-1.990815

[20] Thomas Rid. Cyber War Will Not Take Place. (Oxford University Press, New York, 2013), 15.

[21] Max Boot. "The Paradox of Military Technology," *The Journal of Technology and Society*. (Fall 2006): 26-27.

more technology on the battlefield and in training, not less. CND is important because it enables the commander to have access to all the technologies that produce operational and strategic advantages on the battlefield.

CND is an ongoing concern as new threats, better technology and more clever approaches to attacking networks are constantly being developed. The continual bombardment of the system by adversaries means that a robust capability needs to be in place to secure the system. A network is only as strong as its weakest link and therefore network defenders need to be well trained in the development, installation and administration of CAF networks. Network defence and administration can and has been contracted to outside agencies. In Afghanistan, much of the network administration, particularly on the unclassified network, was contracted to a civilian agency - Calian. Hiring contractors to perform defensive functions enables a military to have access to the most current skills and additional resources at a cost that is likely less then developing and maintaining the skillset internally. The concerns with outsourcing are the same as with the outsourcing of most military functions in that the organization is subject to market prices, contractors may refuse to partake in certain critical activities or missions and eliminating the skillset internally will make the organization dependent on market forces. Maintaining a defensive posture is not inexpensive in terms of the cost of training individuals and the requirement to continually upgrade hardware and software.

The DND and the CAF have identified the importance of CND and have established the Canadian Forces Network Operations Center (CNOC). CNOC monitors all CF networks against intrusion. The army communications non-commissioned members (NCM) trades have recently been re-organized to place greater emphasis on computer network security and administration with the creation of the Army Communication and Information Systems Specialist (ACISS)

parent trade and the Communication Systems Technologist (CST) and the Information Systems technologist (IST) sub-occupations. The Canadian Forces School of Communications and Electronics (CFSCE) has developed courses that give soldiers and officers a better appreciation of CND and how to administer networks. The government, commanders and the field force are all on the same page and appreciate the significance of defending CAF networks. The only controversy is continuing to build capacity at the expense of other CAF capabilities in a time of reduced budgets.

Computer Network Exploitation

According to Thomas Rid, author of *Cyber War Will Not Take Place,* an effect military application of cyber is espionage. In his book he highlights the difference between human intelligence (HUMINT) and signals intelligence (SIGINT). HUMINT is as old as conflict itself and involves sending intelligence officers to collect information from other humans, or documented sources. SIGINT involves the interception of civilian and military radio signals, satellite links, telephone traffic, mobile phone conversations and the gaining of access to communications between computers and accessing information contained in storage devices.[22] Intercepting communications traffic is not a new battlefield concept and SIGINT units have been operating in most conventional armies since wireless communications became commonplace on the battlefield. However, digitization and the proliferation of computers and mass data storage devices has provided an additional opportunity for CNE. Traditionally, SIGINT has been a passive activity. Using various techniques, SIGINT operators would gather information that was propagating freely through the airwaves. A networked battlefield now enables operators to enter

[22] Thomas Rid. Cyber War Will Not Take Place. (New York, Oxford University Press, 2013), 83.

into the communications network of an adversary and gather information and send it back to a collection point. SIGINT is no longer only passive in nature, but it can be an offensive activity.[23]

The magnitude of what is possible in CNE can be gleaned from the cyber espionage conducted against US military and government networks in 2003. The 'attack' was codenamed Titan Rain by US officials. After an analysis of Titan Rain, Major General William Lord, director of information, services and integration in the Air Forces Office of War fighting integration reported that 10 to 20 terabytes of data had been downloaded from the US unclassified, but sensitive IP router network: Non-Classified Internet Protocol Router Network (NIPRNET). Canada has not been immune to cyber espionage. From 2009-11, coordinated espionage activities referred to as Night Dragon[24] stole sensitive information from Canadian oil and gas companies. The information was on company operations, financial statements and intellectual property regarding industrial processes.[25] There have been other reports of cyber espionage against Government of Canada service and research networks. As with most espionage, the effects of the security breaches to national security, or industrial superiority, are not immediately observable and therefore difficult to quantify.

One characteristic of operating in the cyber environment is attribution. Attribution means that it is difficult, if not impossible to link SIGINT activities back to the originator of the action. To a commander this means that information can be collected without putting a person behind enemy lines to physically collect information – it can be done remotely and the chances of

---

[23] Ibid. 83

[24] KPMG. Cyber Crime – A Growing Challenge for Governments. Last Accessed 7 May 2014 https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf

[25] Steven Starr. Cyber-attack threat in Canada's oil patch raises risk of disruptions, stolen data. Last Accessed 7 May 2014. http://business financialpost.com/2013/01/03/cyberattack-threat-in-canadas-oil-patch-raises-risk-of-disruptions-stolen-data/?__lsa=fa25-6865

getting 'caught' are minimal. Thomas Rid does argue that a cyber-intruder may want to show their presence in an adversary's network. This can be a powerful statement that demonstrates to the adversary that you can penetrate their system. This is likely to cause the adversary to lose faith in their system and may alter the way they employ the system going forward. If the adversary chooses not to use the system, then they are being denied the advantages that technology provides. Abandoning technology may also be contrary to their training and doctrine which may further impact their operations. Whether a commander wants to access information noticed, or unnoticed will be a decision he, or she, will need to make based on the strategic, operational and tactical objectives. Regardless of how the components of CNE are applied, this paper argues that the CAF should ensure that commanders have the tools to conduct CNE activities during times of war.

Despite the intrusiveness of the SIGINT activities, according to the laws of armed conflict, cyber espionage and data collection is not considered an act of war, or an armed attack. As a result, nations like the United States, in addition to using military resources, use other government agencies such as the NSA and CIA to contribute to Americans CNE capability.[26] The NSA has even hired contractors to assist with data collection, which has created a firestorm for the Obama Administration, after Edward Snowden, a contractor with Booz Allen Hamilton released top secret information regarding NSA CNE activities. Collecting airwaves for analysis takes many years of training. Becoming an expert in infiltrating an opponent's network and being able to syphon information away without detection is a whole new level of skill development. Assuming the security clearances process can properly vet contractors (the same as properly vetting CAF members) the employment of contractors brings the most current skills to

[26] Richard Clarke. *Cyber War: The Next Threat to National Security and What to do About it* (New York, HarperCollins, 2010): 37-39.

the fingertips of commanders. Considering the investment that needs to be made in order to train a CAF member to be proficient in CNE, the contractor option may be less expensive than maintaining the skillset internally. Conversely, commanders could rely on other government departments to provide the capability, however, there ought to be a concern regarding the responsiveness of other agencies to DND.

CAF has a SIGINT capability but the Canadian military does not participate in clandestine, or espionage operations. The Canadian Security Intelligence Service (CSIS) maintains computer surveillance and data gathering capabilities, but the Canadian government maintains that CSIS does not conduct clandestine operations, despite recent reports on CSIS collecting information on Brazilian companies and politicians. The unclassified nature of this paper does not permit a thorough discussion of CAF and CSIS SIGINT capabilities. That being said, the details are not important. What is important to recognize is that information obtained from an adversary's networks is of great value to a commander. Collection and analysis is done by highly skilled individuals who can be military, public servants or contractors and in a time of war CAF should have the capability to conduct the widest range of CNE operations.

Computer Network Attacks

The third aspect of the cyber domain to be discussed is computer network attacks. As previously stated, this paper is focusing on the CAF's development of cyber capabilities including offensive cyber-attack tools that can be used against an adversary in times of declared war, or conflict. This distinction was done purposefully to remove the discussion around the legal debate of the threshold of when a cyber-attack constitutes an act of war. The definition of act of war in a cyber-context is not a trivial notion and NATO has had to deal with such a concern in the past. In 2007, the former Soviet Satellite of Estonia, a member of NATO at the

time, experienced a denial of service (DOS) attack against government and commercial interests in the country. Estonian officials were able to connect the attacks back to Russia and the Estonian government requested that NATO intervene under the collective security agreement as Estonia viewed the cyber activity as an attack on Estonian sovereignty. NATO did not view the event as an attack on Estonia and only provided Estonian with technical support to overcome the DOS event - the response was much less than what Estonia was seeking. The 'attack' however detrimental to Estonia was not considered an act of war or attack that would warrant intervention by the collective security agreement.

While scholars and the international community attempt to define what constitutes a cyber-act of war or whether a cyber-only war is even possible, practitioners need to be more practical in assessing how these capabilities can be leveraged in times of open conflict. The power of such an attack capability on the battlefield can best be highlight by OPERATION ORCHARD which was executed by the Israeli Defence Force (IDF) in 2007. OPERATION ORCHARD was a combined strike operation using air and cyber power assets. The kinetic portion of the attack was executed on 6 September 2007, however, the time and duration of the cyber component of the operation remains classified. At some point in time prior to 6 September 2007, IDF forces were able to insert code into the Syrian air defence system. When activated, the IDF was able to gain control of the Syrian air defence and send the system false sensory information that showed the system that there was no unauthorized activity in the Syrian airspace. When the IDF had control of the system they sent a squadron of F-15I and F-16I warplanes undetected to a Syrian nuclear reactor site in Dayr ez-Zor in Northern Syria. The squadron was able to enter Syrian airspace, destroy the facility and return to Israel without Syrian defence forces knowing what was occurring. The magnitude of what can be accomplished

using cyber power provides commanders with an extraordinary tool at their disposal. In the IDF case presented above, the Israeli's were able to strike deep into Syrian territory with minimal risk to Israeli forces. The attack also severely undermined the trust that Syrian officials had in their air defence system.

The media and scholars have presented concerns about a cyber-9/11, or cyber Pearl Harbour type attack. The closest real life example of an attack using only cyber capabilities is the joint US-Israeli Stuxnet attack on the Iranian nuclear programme. Although many of the aspects of the attack remain classified, information from the Whitehouse has revealed that Stuxnet was a multi-year campaign that spanned from November 2005 to June 2012.[27] Stuxnet was a worm, malicious code that enters into a network and seeks out a particular vulnerability in a network to exploit. If the worm does not find the vulnerability it does nothing. If it finds the vulnerability it exploits it as per the programmers intended effect. In the case of Stuxnet, the worm exploited a vulnerability in the firmware of a Siemens 6ES7-315-2 and 6ES7-417 programmable-logic-controllers (PLC). A PLC is essentially a microchip that controls various industrial processes – in this case, components of the Iranian nuclear enrichment programme. These particular PLCs were used in the centrifuges of Iranian nuclear reactors. When a PLC became infected, it would cause the centrifuges to spin out of control, while at the same time reporting normal readings back to the master control station. Iranian engineers could not explain why centrifuge motors were burning out and they continuously re-evaluated their processes wasting time and spending extra money. The Stuxnet virus demonstrated that cyber power can be used to destroy the equipment used in industrial processes. A later research project at the Sandia National

[27] John Leyden. US officials confirm Stuxnet was a joint US-Israeli op. Last Accessed on 7 May 2014 http://www.theregister.co.uk/2012/06/01/stuxnet_joint_us_israeli_op/

Laboratories confirmed the potential destructive nature of a cyber-attack. Using only code, the researchers were able to cause a gas generator, much like the ones connected to the US power grid, to malfunction and eventually explode.[28] There are some academics, like Thomas Rid, who suggest that cyber activities are not destructive as it is not the code that does the damage but rather the object itself that malfunctions and explodes.[29] To a commander, the net effect is what is important and a cyber-attack capability that can degrade a legitimate military target by itself, as with Stuxnet, or in conjunction with other capabilities, such as OPERATION ORCHARD, is desirable.

The cyber operations that have occurred to date demonstrate the force multiplying nature that cyber activities can have on the battlefield. Canadian commanders ought to have access to the full spectrum of capabilities that cyber can provide. The question is, does the CF need to force generate a CNA capability internally, or can cyber-attack activities be contracted to third parties, or be done by DND employees. According to Falliere, Murchu and Chein, the authors of W32.Stuxnet Dossier Version 1.4, 'programming such a complex agent [Stuxnet] required time, resources, and an entire team of core developers as well as quality assurance and management.'[30] This again goes to the point made earlier in the paper that the skills required to develop CND, CNE and CNA are not skills that are developed overnight. While an argument can be made that CND and CNE capabilities can be purchased from industry, this paper contends that the same is

---

[28] Perry Pederson. Aurora Project and the Smart Grid. Last Accessed 7 May 2014 http://www.whitehouse.gov/files/documents/cyber/Pederson%20Perry%20-%20Aurora%20and%20the%20Smart%20Grid.pdf

[29] Thomas Rid, *Cyber War Will Not Take Place* (New York, Oxford University Press, 2013): 34

[30] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response, February 2011, accessed on 10 February 2013, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

not true for CNA activities. The argument being made is that CAF would only deploy a CNA capability against an adversary in times of conflict. The specialists that would employ offensive cyber weapons during conflict ought to be uniformed CAF members. The argument for CNA being conducted by military professionals is made on two lines of reasoning. Firstly, offensive activities will be conducted during conflict and Geneva conventions for combatants and non-combatants must be respected. The Tallinn Manual, which was published in 2013, was a legal and academic approach by experts in the field of military law to interpret cyber activities in the context of current international customary law.[31] The contents of the manual are non-bidding legal interpretations. The panel of experts identified ninety-five rules that military commanders should consider when responding to cyber threats, or employing cyber capabilities. Rule 35 – Civilian direct participation in hostilities, suggests that, 'civilians enjoy protection against attack unless and for such time as they directly participate in hostilities. This rule is drawn from Article 51(3) of Additional Protocol I and Article 13(3) of Additional Protocol II of the Geneva Convention'.[32] The interpretation argues that civilian cyber specialists supporting military operations lose civilian status when supporting operations and can be targeted. In an increasingly complex operating environment, mixing military and civilian targets can prove detrimental. The interconnectivity of cyber enables activities to be conducted anywhere in the world. If researchers at a Canadian University or contractors working from an office building in Ottawa are supporting a cyber-capability, does the Canadian government want to invite a 'legitimate' attack on Canadian territory? Using academics, contractors or public servants on Canadian soil,

[31] NATO, Cooperative Cyber Defence Centre of Excellence, "The Tallinn Manual." Last accessed on 19 December 2012, http://www.ccdcoe.org/249 html

[32] Ibid. 102

or abroad, would make them legal targets. Involving civilians in offensive cyber operations only increases the 'fog of war' and puts civilians lives at risk.

Understandably, if Canada was in an all-out cyber conflict the desire to use civilian expertise would be high regardless if their lives were in danger. However, there still would not be a legal framework in which civilians could be used in direct acts of aggression. The second argument for why CNA must be conducted by military personnel is that the National Defence Act establishes the CAF as the armed forces authorized to conduct military activities on behalf of the crown. In order to be in the CAF, one needs to enroll as either a commissioned or non-commissioned member.[33] Canada's current legal framework does not enable civilians or contractors to participate in armed conflict. Arguments have been made that cyber is not 'armed' conflict as cyber activities are not violent in nature. Moreover, when destruction does occur, it is generally other forces that cause the destruction (such a centrifuge spinning out of control until it explodes) and not the code itself. Others extend the concept of armed to include any activity that degrades the military capacity of an adversary, which CNA certainly can do. What is interesting is that the terrorist attacks on the US (9/11) have somewhat expanded the traditionally definition of armed attack. The attacks of 9/11 occurred as a result of terrorists gaining control of commercial airliners and flying them into buildings. The Americans were successful in invoking NATOs collective security agreement under the auspice that the US had been subject to an 'armed attacked'.[34] We have seen that researchers, or Iranian government officials, have been able to hack into US drone and control their actions. They could cause drones to fly into

---

[33] Government of Canada. National Defence Act. Last Accessed on 7 May 2014. http://laws-lois.justice.gc.ca/eng/acts/n-5/page-1.html

[34] Carsten Stahn, Terrorist Acts as "Armed Attack": The Right to Self-Defense, Article 51(1/2) of the UN Charter, and International Terrorism. The Fletcher Forum of World Affairs. Vol.27:2 (Summer/Fall 2003): 35.

buildings. Or, hackers may be able to take control of a commercial airliner remotely and cause the autopilot function to fly the aircraft into a building. If following the historical example of 9/11, would that not be considered an 'armed attack'? Surely, the definition of armed attack is not premised on the concept of a human actually needing to be in the cockpit to steer a plane into a building. If a significant cyber activity were to occur against US interests at home, there is little doubt that American diplomats and politicos would argue it was an armed attack and seek international support in retaliation.

According to Ashton Carter and Job White, authors of *Keeping the Edge: Managing Defence for the Future*, the skills required to be proficient in cyber space are like building blocks. CND is the base, it is also most resource intense aspect of a cyber-capability[35], and without a robust defence capability it is likely that the cyber domain will be denied when a commander attempts to undertake activities in cyberspace. Someone who is skilled in CND, who understands the network, the systems and potential vulnerabilities, is more capable at infiltrating another network for either CNE or CNA activities.[36] If CAF is to develop CNA, it will need to develop CND and CNE to support the CNA capability. If, as argued by this paper, CNA ought to be performed by members of the CAF then the force generation of developing a CNA warrior will include significant CND and CNE training. So, if CAF wants a CNA capability, the institution will need to develop a military CND and CNE capability. That is not to say that CND and CNE cannot be augmented by civilian employees, or contractors. It is just to say that if CAF wants a full spectrum cyber capability it will need to be force generated from within.

Conclusion

[35] Ashton Carter and Job White, *Keeping the Edge: Managing Defence for the Future*, (Cambridge, Harvard University Press, 2001): 93.

[36] Ibid. 93-96

The cyber domain is a continuously developing realm where the possibilities of use and exploitation may only be limited by the imagination of mankind. As with any new technology comes the fear of the unknown, the requirement to accurately define the concept and the development of a legal framework to regulate its use. Regardless of the definition of cyber, when it can and cannot be used, who it can and cannot be used against and whether or not cyber is a destructive tool, military practitioners need to identify that network technology and the developed world's use of technology provides both a military strength and vulnerability. In times of open conflict, an armed force will seek to use technology and deny their adversary the same. Moreover, it is evident that cyber activities can provide commanders with additional tools too directly, indirectly or in conjunction with other aspects of military power cause the degradation of an adversary's military capability.

This paper argues that the CAF ought to develop the full spectrum of cyber capabilities to include CND, CNE and CNA and that CAF members need to be the backbone of any cyber capability. It was argued that a CND capability is required to ensure that commanders are able to use secure, reliable, networks to conduct command and control activities on the battlefield. Unabated access to the electromagnetic spectrum also enables commanders to employ smart technologies that make war fighting more precise and efficient. The CAF has been mandated to maintain a CND capability and does so using CAF, DND and contractor assets. The argument has also been made that the CAF expand its CNE capability to include the full spectrum of information gathering techniques. While the CAF employs passive SIGINT capabilities a call for the development of more active SIGINT abilities for use in times of conflict is warranted. Such a capability may enable commanders to infiltrate an adversary's network and access sensitive information to be exploited toward the attainment of current, or future, military objectives. Such

activities are not considered acts of open aggression, or war and therefore can be conducted using a combination of military, civilian and contractor resources. Lastly, and perhaps the most controversial, the argument was made for the development of a cyber-attack capability, or CNA. CNA has the potential to be a strategic force multiplier by either directly degrading an opponent's military capability or assisting other facets of military force in rendering an adversary's capability ineffective. As CNA would only be used in a conflict scenario, the legal structure of the NDA would prevent commanders from using civilians in conducting attacks on an adversary, cyber or otherwise.

Canada's allies and potential adversaries are preparing for the cyber battlefield and the CAF needs to be in a position to project cyber power when called upon to protect Canada's interests. It may take years to come to a consensus of the definitions of cyber, if it's a domain, what is an attack or any of the other debates occurring in the political and academic areas. In the meantime, developing a capability for future use will ensure Canada is not at a strategic disadvantage in the next conflict when we arrive with limited cyber capabilities.

Bibliography

Arquilla, John and David Ronfeldt. "Cyberwar is Coming!" Rand Corporation, 2007. http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

Babad, Michael. "Chinese hackers suspected of raiding Nortel for decade," The Globe and Mail, Accessed on 19 December 2012. http://www.theglobeandmail.com/report-on-business/top-business-Canada. National Defence. "Projects." accessed on 26 January 2013, http://www.forces.gc.ca/site/pri/2/index-eng.asp.

Betz, David and Tim Stevens. Cyberspace and the State: Toward a Strategy for Cyber-Power. London: Routledge, 2011.

Boot, Max. "The Paradox of Military Technology," *The Journal of Technology and Society*. (Fall 2006): 13-31.

Brackin, William. *Navy Orientation* (Washington, DC: United States Government Printing Office, 1991).

Canada. Department of National Defence. *Securing Canada's Ocean Frontiers – Charting the Course from Leadmark.* Ottawa: DND Canada, 2005.

Canada. Government of Canada. *Canada's Cyber Security Strategy*. Ottawa: Her Majesty the Queen in Right of Canada, 2010.

Chief of Force Development. A-FD-005-002/AF-001. Integrated Capstone Concept. Winnipeg, MB: Department of National Defence (17 Wing Publishing Office), 20 October 2009. http://publications.gc.ca/collections/collection_2012/dn_nd/D2-265-2010-eng.pdf

Curry, Bill. "Serious Flaws in Ottawa's Defence Against Cyber Attacks: Auditor General." accessed on 14 February 2013. http://www.theglobeandmail.com/news/politics/ottawa-notebook/serious-flaws-in-ottawas-defence-against-cyber-attacks-auditor-general/article4630798/.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War*, Cambridge: University Press, 2012.

Falliere, Nicolas, Liam O Murchu, and Eric Chien."W32.Stuxnet Dossier." Symantec Security Response. February 2011. accessed on 10 February 2013. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Global Research. "US-Israeli Stuxnet Cyber-attacks against Iran: "Act of War"." accessed on 5 April 2013. http://www.globalresearch.ca/us-israeli-stuxnet-cyber-attacks-against-iran-act-of-war/5328514.

Herzog, Stephen, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," Journal of Strategic Security, Volume IV Issue 2 2011, 49-60.

Joint Operational Access Concept (JOAC). Last Accessed on 7 May 2013, http://www.defense.gov/pubs/pdfs/joac_jan%202012_signed.pdf

Libicki, Martin C. *Cyberdeterrence and cyberwar*. Rand Corporation, 2009.

Libicki, Martin C. "Cyberspace is not a Warfighting Domain." 25 January 2012.

Libicki, Martin C. "The Specter of Non-Obvious Warfare." Strategic Studies Quarterly, Fall 2012.

Libicki, Martin C. "What Is Information Warfare?" National Defense University. October 1995.

Manzo, Vincent. "Deterrence and Escalation in Cross-domain Operations Where Do Space and Cyberspace Fit?," JFQ, issue 66, 3rd Quarter 2012, 9.

Ministry of Defence, British Air and Space Power Doctrine, AP 3000. Shrivenham: Air Staff, 2009.

Murphy, Matt. "War in the fifth domain," The Economist, Last Accessed on 19 December 2012, http://www.economist.com/node/16478792.

Musil, Stephen. "Anonymous declares war on Syrian government," CNET Last Accessed on 19 December 2012. http://news.cnet.com/8301-1009_3-57556333-83/anonymous-declares-war-on-syrian-government-web-sites/.

NATO Cooperative Cyber Defence Centre of Excellence. "The Tallinn Manual." Last accessed on 19 December 2012. http://www.ccdcoe.org/249.html.

Österberg, V.P. Military theory and the concept of Jointness. Last Accessed on 7 May 2013, http://forsvaret.dk/fak/documents/fak/fsmo/specialer/03-04/military_theory_and_concept_of_jointness.pdf

Raytheon. “Excalibur Precision Guided Extended Range Artillery Projectile.” accessed on 9 February 2013, http://www.raytheon.com/capabilities/products/excalibur/index.html.

Rid, Thomas. “Cyber War Will Not Take Place.” Journal of Strategic Studies, vol 35, no 1, 5–32, February 2012.

Rid, Thomas. Cyber War Will Not Take Place. C. Hurst & Co. (Publishers) Ltd 2013

Rosenzweig, Paul. “Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World.” Lawfareblog.com accessed on 24 February 90 2013. http://www.lawfareblog.com/2013/01/cyber-warfare-how-conflicts-in-cyberspace-are-challenging-america-and-changing-the-World/.

Sauer, Jeremy and Michael J. Kaiser. Changing the Strategic Dialogue: New Definitions for Landpower and Land Control. Small Wars Journal. http://smallwarsjournal.com/jrnl/art/changing-the-strategic-dialogue-new-definitions-for-landpower-and-land-control

Sghairi, M., A. de Bonneval, Y. Crouzet, J.-J. Aubert and P. Brot. “Challenges in Building Fault -Tolerant Flight Control System for a Civil Aircraft.” International Journal of Computer Science, Vol 35 issue 4 accessed on 20 February 2013. http://www.iaeng.org/IJCS/issues_v35/issue_4/IJCS_35_4_07.pdf.

Stytz, Martin and Sheila Banks. Toward Attaining Cyber Dominance. Strategic Studies Quarterly. Vol 8 no. 1 (Spring 2014) 81

United States. Department of Defense. *Formal Investigation into the Circumstances Surrounding the Downing of Iran Air Flight 655 on 3 July 1988*. 1988.

United States. Department of Homeland Security. “Critical Infrastructure Protection and Resilience Month 2012.” accessed on 21 February 2013. http://www.dhs.gov/cipr-month-2012.

United States. Department of Homeland Security. “Critical Infrastructure Protection and Resilience Month 2012.” accessed on 21 February 2013. http://www.dhs.gov/cipr-month-2012.

United States. Strategic Command. “U.S. Cyber Command.” accessed on 13 January 2013, http://www.stratcom.mil/factsheets/Cyber_Command/.

Wagenseil, Paul. “Obama, Bush Behind Stuxnet Worm, Report Says.” Technewsdaily.com, 1 June 2012 accessed on 25 February 2013. http://www.technewsdaily.com/7824-obama-bush-stuxnet-report.html.

Walking, J.C. “Considerations: Canadian Forces Efforts in the Electromagnetic Spectrum and Cyber Operating Environment,” Master’s thesis, Canadian Forces College, 2013.

Welch, Dylan. “Foreign spies with cyber eyes on our government,” Lase Accessed on 19 December 2012, http://www.smh.com.au/it-pro/government-it/foreign-spies-with-cyber-eyes-on-our-government-20110923-1kpgs.html.

Wolf, Walter. “21st Centruy EM Domain Capabilities.” The Journal of Electronic Defense. October 2011.

Wylie, J.C. *Military Strategy: A General Theory of Power and Control.* New York: Rutgers. 1967.