National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER SECURITY IS THE FUTURE

Maj J.T.M. Willis

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.

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.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 40 – PCEMI 40

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CYBER SECURITY IS THE FUTURE

Maj J.T.M. Willis

Word Count: 2712

Compte de mots: 2712

CYBER SECURITY IS THE FUTURE

INTRODUCTION

A recent theme in popular fictional television shows has been the exploitation of web-based applications to allow heroes and villains alike to meet their objectives. In the last twenty-four months, several major networks have sparked the imagination. There has been *Jack Bauer* attempting to regain control of armed jets after hacked UAVs have begun attacking friendly positions on the latest season of *24*.[1] *Huck*, *Walter* and *Sylvester* loom around the Internet to find information, extract funds, and override security systems on *Scandal*[2] and *Scorpion*.[3] The latest addition to the mix, more bluntly entitled *CSI Cyber*,[4] deals with the vast range of cyber security issues. Is this all science fiction, or are any of these exploits within the realm of possibility? They are dramatized, of course, exaggerated, always – as one would expect from Hollywood. However, the contribution and growing importance of cyber security to security and defence is real.

This paper aims to demonstrate that cyber security is the future. As the US Deputy Secretary of Defense has stated, Cyber is the next domain, alongside Air, Land, Navy and Space.[5] This implies there are both opportunities and vulnerabilities that the Canadian Armed Forces must address in order to remain relevant. The paper will discuss those opportunities and vulnerabilities; it will then discuss more directly the challenges and next steps for the Canadian Armed Forces.

---

[1] http://en.wikipedia.org/wiki/24:_Live_Another_Day
[2] http://abc.go.com/shows/scandal
[3] http://www.cbs.com/shows/scorpion/
[4] http://www.ctv.ca/CSICyber.aspx
[5] William J. Lynn III, *Defending a New Domain - The Pentagon's Cyberstrategy*, Foreign Affairs, October 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

OPPORTUNITIES: THE GLASS HALF FULL

There are a number of opportunities that the increasingly connected and technologically advanced world present to security and military professionals. Sabotage, Espionage and Info Ops are specific examples. Although these disciplines are not new to war fighting, exploiting cyber capabilities to support those activities can be an exceptional force multiplier. Furthermore, the use of cyber capabilities may lead to the achievement of military, security and political objectives with less violence, reducing harm and collateral damage.[6]

Sabotage

Sabotage, or the ability to cause harm to assets – to degrade or destroy them - can be achieved by cyber-attack. A few vehicles exist to accomplish this goal.

It is possible to overwhelm an information system, degrading its response capability and affecting it system performance. Overloading the demand on an information system to render it inoperative is one way to sabotage an information network; this is often referred to as a denial of service attack.[7]

Various computer-controlled industrial systems, which can be key military targets, such as radar stations, electrical grids, or nuclear power plants, are typically monitored and controlled by specific types of computer systems, known as Industrial Control Systems, ICS.[8] These ICS monitor the performance of the system, such as temperature, pressure or throughput, for example, and give commands such as opening or

[6] Thomas Rid, *Cyber War Will Not Take Place*, (New York: Oxford University Press, 2013), xiv
[7] *Ibid*, 6.
[8] Thomas Rid, *Cyber War Will Not Take Place*, (New York: Oxford University Press, 2013), 51.

closing valves. They keep the system running optimally and safely. Some are semi-automated, sending status information to a human operator, which selects courses of action and sends commands; others are increasingly automated and complex. Various methods of infiltration can allow an outside agent to take control of the system covertly, and can even send erroneous data to a human operator to make it seem as if all systems are running as expected. Although the automated ICS systems are intended to be segregated from other networks for cyber security reasons, a few flaws have proven to breach the security gap. The first would be, very simply, human error, uploading malware (knowingly or unknowingly) with a USB stick that has been used on an infected network and subsequently inserted within the ICS. In the search for optimization, enterprise level software solutions that oversee demand, supply chains, stock levels and throughput also gather information about the status of a system. These web-based business networks can unintentionally create a security breach within the ICS infrastructure. Thousands of Industrial Control Systems are even connected directly to the internet, possibly without the operator's knowledge, as these control systems become so large and complex that no one individual necessarily has the full picture of the entire system.[9]

A recent example of ICS sabotage is the Stuxnet virus, designed and delivered into an Iranian nuclear enrichment plant to disrupt the system in random ways. It achieved not only tactical effects (the plant running sub-optimally), but the strategic

[9] Kim Zetter, *10k Reasons To Worry About Critical Infrastructure*, Wired, 24 Jan 12, http://www.wired.com/2012/01/10000-control-systems-online/

effect of decreasing the level of confidence in the technology, in an effort to slow the progress of nuclear capability in Iran.[10]

An operational example of the use of cyber-attack for sabotage in a military context was the temporary disabling of a Syrian radar station by the Israeli Air Force in September of 2007. This allowed fighter aircraft to enter airspace undetected, reach their targets, and destroy the construction site of a nuclear reactor.[11] In previous air campaigns, such as Operation Desert Storm of 1991, both the radar stations and communication networks may have been attacked first to allow for covert intrusion of bombers.[12] In this example, the cyber-attack disabled the air defence system, eliminating the need for the physical destruction of the radar station and communications networks; these would have otherwise been targeted with violent use of force.

Espionage

The world of espionage is often divided between HUMINT and SIGINT, or human intelligence and signals intelligence. Cyber capabilities can and do support both.

The use and exploitation of information made widely available on social media, such as Facebook, Twitter or LinkedIn, to name a few, can provide operationally relevant information from comments or pictures posted.[13] These social media also provide information about relationships amongst groups of people, and tone used to

---

[10] David E. Sangerjune, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, The New York Times, 1 June 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0

[11] Carroll Ward, Israel's Cyber Shot at Syria, Defense Tech, 26 November 2007, http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria/

[12] Benjamin S. Lambeth, *The Winning of Air Supremacy In Operation Desert Storm* (Santa Monica: RAND, 1993)

[13] Open Source Information in Conflict Zones, https://www.youtube.com/watch?v=aBXz7gJswRE

communicate. This knowledge can be used to create targeted e-mails that appear legitimate, but embed malware. Although the conversations of late within the Canadian Armed Forces surrounding social media and espionage are primarily focused on vulnerabilities, which will be discussed later, there is indisputably an opportunity to be seized by exploiting the cyber dimension within the existing HUMINT framework.

The original capabilities of SIGINT upon its inception, intercepting enemy radio signals to decipher and using them to friendly advantage, are essentially put on steroids in this cyber-centric new world. The amount of data and information that can be collected, analyzed and processed to produce intelligence products for friendly advantage is astounding. Perhaps it is this vast amount of data that can render the acquisition of useful information difficult. Nevertheless, the exploitation of information on computerized networks is only the tip of the iceberg.

Countless industrial systems are unknowingly connected directly to the Internet,[14] rendering them vulnerable to espionage and sabotage. Malware may be developed to infect computer systems. Not only may it be used to relay files on hard drives or network drives to the exploiting command and control center; it may also be used to remotely and covertly turn on microphones and cameras to computers or cell phones to record and transmit voice and images without being detected by the target.[15] In the information era, the distinctions between HUMINT and SIGINT become increasingly blurred.

---

[14] Kim Zetter, *10k Reasons To Worry About Critical Infrastructure*, Wired, 24 Jan 12, http://www.wired.com/2012/01/10000-control-systems-online/

[15] Thomas Rid, *Cyber War Will Not Take Place*, (New York: Oxford University Press, 2013), 94.

Information Operations

IO Campaigns aiming to affect popular support, or shift alliances towards friendly objectives can exploit cyber capabilities. Various cyber-attacks have taken aim at the credibility, reputation and trust of various companies, governments and public figures.[16] As National Will and Public Support tend to be Centers of Gravity to recent operations, the use of cyber-attacks can assist to target those directly.

In these examples of sabotage, espionage or information operations, utilizing cyber-capabilities is an incredible force multiplier, achieving with a few lines of code what otherwise might have required a physical attack, or placing friendly human assets in harm's way. The exploitation of cyber-capabilities can allow for the attainment of military and political objectives with less violence, less collateral damage, and less exposure to risk for friendly forces.

VULNERABILITIES

If the existence of cyber capabilities implies opportunities, it certainly also implies vulnerabilities. Our modern weapon systems are becoming increasingly software-centric. The RCAF is in the midst of the largest recapitalization program since WWII. The complexities of the integration of software systems within platforms have not only resulted in programmatic delays for the F35 and CH148; they have also exposed the extent to which operational capability is reliant on hardware and software. The Cyclone, for example, integrates 64 computers, with millions of lines of code to produce an

[16] *Ibid*, 26

operationally relevant Maritime Helicopter from the S92 civil variant. The RCN is modernizing, and then replacing all its ships.

These modern platforms leverage, but also rely on and are controlled by software. It is possible to attack these systems in a similar way to how industrial systems have been hacked, despite the air-gaps and other mitigating measures.[17] Aircraft in particular have been reported to be vulnerable to cyber-attack.[18] Some security breaches have already occurred on some of our assets, impacting the operational capabilities within our Fleets.

A savvy attacker could, in theory, gain access to and control of our platforms, turning them into remote-controlled toys. To create a system-specific attack, they would require intimate knowledge of the system's code, and extensive effort to weaponize a virus to enact the attack. A much simpler solution to achieve a similar goal is to confuse a system's embedded GPS system by providing a stronger signal, and convincing the weapon system that it is in a different location, allowing the attacker to alter course. These types of GPS spoofers can be built under $1000[19] and this technology was initially believed to have caused a CIA-operated drone to land in Iran.[20]

Although these attacks are theoretically possible, the security risk associated with these threats is generally assessed as being fairly low. The assumption tends to be that

---

[17] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier, Version 1.4*, Symantec, February 2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[18] Matthew Hoye and Rene Marsh, *GAO: Newer aircraft vulnerable to hacking*, CNN, 14 April 15, http://www.cnn.com/2015/04/14/politics/gao-newer-aircraft-vulnerable-to-hacking/

[19] John Roberts, EXCLUSIVE: Drones vulnerable to terrorist hijacking, researchers say, Fox News, 25 June 2012, http://www.foxnews.com/tech/2012/06/25/drones-vulnerable-to-terrorist-hijacking-researchers-say/

[20] Catherine Herridge, *US data in Iranian hands after downed drone?*,10 February 2012, http://www.foxnews.com/politics/2012/02/10/us-data-in-iranian-hands-after-downed-drone/

there are no entities that wish to do harm; or, if they do, that they would not possess the information necessary, or skill required to retrieve the information to gain access to the weapon systems. It seems that this is a grossly insufficient and neglectful approach to cyber security. As computer scientists point out, there is no "security by obscurity."[21] Relying on an expectation that no one will attempt to gather the required data on the systems or use it to their advantage is negligent.

Another vulnerability is The CAF's increased dependence on software systems to communicate, coordinate and ultimately fight. It is astounding how the usability of software tools has resulted in paralysis and confusion when they have been temporarily unavailable. Should they become permanently compromised, the organizational impact would be significant.

Finally, the increasingly connected world implies Operational Security challenges, as previously alluded. Using photos posted on Facebook, one could reconstruct the allied camps in Afghanistan in their entirety. With information posted on Facebook, ISIS has created a list of the soldiers involved in the fight against them, and has publicized the names and locations of their families – the soldier's spouses and children are seen as legitimate terrorist targets to whomever wishes to take independent action. The Operational Security implications of working in a connected world, and employing connected individuals are multifaceted. The use of social media has an impact on today's security environment and is used by state and non-state actors. The opportunities to use cyber-influence activities and the threats associated with radical

[21] Thomas Rid, *Cyber War Will Not Take Place*, (New York: Oxford University Press, 2013), 73

actors exploiting social media were tabled at a recent social media and cyber-influence workshop.[22]

CHALLENGES AND NEXT STEPS

The Canadian Armed Forces are lagging behind the superpowers as it pertains to the development of a military cyber capability that is able to either protect the CAF or exploit opportunities. The 1993 RAND report proposed that Cyber War was coming.[23] In 2005, the US Air Force proclaimed Cyberspace to be the fifth domain of warfare, alongside Air, Navy, Army and Space;[24] by 2010, USCYBERCOM had reached Full Operational Capability.[25] The US, UK, Israel,[26] and China,[27] to name a few are already leading the path to exploiting cyber capabilities for military advantage.

For Canada to develop cyber capability, a few key enablers are needed: an established structure, subject matter experts, widespread basic understanding of the topic, and processes established to identify and communicate opportunities and risks.

Action Plan 2010-2015 for Canada's Cyber Security Strategy, an interdepartmental initiative, called for the establishment of a task force and subsequent

---

[22] Attendees included DG Cyber, Dr Craig Stone, representatives from PSYOPS, CDI, DRDC, SJS, DFADT, RCMP, Public Safety, CBC Radio, SMEs from York, Iowa, Waterloo and Ottawa Universities. http://dandurand.uqam.ca/uploads/files/evenements/201504_CNSS_Agenda.pdf

[23] John Arquilla and David Ronfeldt. *Cyberwar is Coming!* (Santa Monica, CA: RAND Corporation, 1993) http://www.rand.org/pubs/reprints/RP223.

[24] By amending its Mission Statement to add CyberSpace as another warfare domain, along with Air and Space. http://www.au.af.mil/info-ops/cyberspace.htm#usafcyber

[25] http://www.stratcom.mil/factsheets/2/Cyber_Command/

[26] Thomas Rid, *Cyber War Will Not Take Place*, (New York: Oxford University Press, 2013), 54

[27] William C. Hannas, James Mulvenon and Anna B. Puglisi, *Chineese Industrial Espionage – Technology Acquisition and Military Modernization*, (New York:Routledge, 2013)

Director General Cyber within the Canadian Armed Forces.[28] By 2013, our Director General Cyber had spent a few years considering and documenting options, without any decided path forward, imminent plans to actually establish defensive or offensive capability, and void of any understanding that the threats and opportunities are not limited to information networks, but include the most advanced weapons themselves.[29] Arguably though, the CAF has been in a situation of financial restraint, and the limited funding for developing capabilities appears to be constrained by the overstretched budgets attempting to maintain existing capabilities.[30] Nevertheless, the first step to attain a Canadian cyber capability was to establish an organization responsible for its development. This step has been completed; the organization has now stood up and begun establishing international and intergovernmental relationships, and evaluating options for capability development.[31]

The next step is to resource the organization with talent able to render it relevant in the Cyber domain. This is not trivial. The typical candidate the Canadian Armed Forces has historically tried to recruit is athletic, charismatic, outgoing, and outdoorsy – characteristics that may miss the mark if what is really required are computer-savvy experts. If what is needed are hackers, then the CAF needs to modify or adapt not only the target recruit, but also the recruiting strategy. As the desired candidate shifts, the organization must shift in order to be desirable to the candidate. In the US for example,

---

[28] Action Plan 2010-2015 for Canada's Cyber Security Strategy http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx

[29] Chris Thatcher, *Operationalizing the Cyber Domain* (Vangard, 26 June 2013). Interviewing BGen Greg Loos, then DG Cyber since 2011. http://vanguardcanada.com/operationalizing-the-cyber-domain/

[30] Gen Lawson, CDS address to 12 Wing Shearwater Town Hall, 21 November 2014.

[31] Action Plan 2010-2015 for Canada's Cyber Security Strategy http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx

the NSA's DG and head of Cyber Command presented a recruiting pitch at the largest hacker conference, wearing jeans and a T-shirt.[32]

Now, there are some software-savvy folks within the Canadian Armed Forces; just likely not enough, or not with the right skillsets. Within the Aerospace Engineering occupation, a number of software-related post-graduate opportunities exist. The limiting factor is that there are not enough engineers with software undergraduate degrees to be eligible for those advanced studies. As a subculture within the occupation, it is widely believed (not incorrectly so) that being associated with software talents is career-limiting. The information the software experts attempt to communicate is not well understood by the majority of peers, and they can become isolated.

To be able to truly benefit from the computer expertise the CAF has and will have, a baseline understanding of informatics should be widespread. DG Cyber proposes that cyber capability be driven by Command and integrated within the cross-functional teams supporting the Commanders. Although this is a great idea, for it to work there needs to be some understanding of what these subject matter experts can bring to the table. Without knowing what is in the realm of the possible, it will be difficult for Commanders and their coordinating ops and planning staffs to capitalize on the provided expertise. Within engineering communities, the generalists, desk officers for platforms or equipment management teams and project managers need some basic knowledge of software fundamentals to be able to comprehend the status, development or upgrade requirements of the platforms they oversee.

---

[32]Stacy Crowley, NSA wants to hire hackers, 29 July 2012, http://money.cnn.com/2012/07/27/technology/defcon-nsa/

Finally, an established process to communicate risks and opportunities, similar to operational, airworthiness or flight safety risks should be established or leveraged. These existing programs have had great success in communicating shortfalls, evaluating options and receiving direction and resources to pursue the chosen course of action. They tend to have very specific categorization, which renders them very effective and efficient for the purposes for which they are conceived; however, this also renders them too overly specific to be directly leveraged to communicate and mitigate cyber security risks without process modification.

CONCLUSION

The emerging cyber domain can be a powerful force multiplier, decreasing the violence required to meet military and political objectives. There are opportunities to leverage cyber capabilities for sabotage, espionage and influence operations, to name a few. The cyber domain also implies that the CAF are vulnerable to enemy or foreign state and non-state actors utilizing those same capabilities against us.

Furthermore, modern militaries are vulnerable to the cyber-attack of weapon systems, vulnerable by the increasing dependence on software-enabled enterprise solutions to communicate and coordinate, and vulnerable to the realities of compromised operational security from the social media presence of their members.

The Canadian Armed Forces must develop a cyber capability to exploit opportunities and defend against vulnerabilities if it wishes to remain viable and relevant.

BIBLIOGRAPHY

Arquilla, John and David Ronfeldt. Cyberwar is Coming! Santa Monica, CA: RAND Corporation, 1993. http://www.rand.org/pubs/reprints/RP223.

Brown, Moses, *Open Source Information in Conflict Zones*, https://www.youtube.com/watch?v=aBXz7gJswRE

Crowley, Stacy, NSA wants to hire hackers, 29 July 2012 http://money.cnn.com/2012/07/27/technology/defcon-nsa/

Falliere, Nicolas, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, Version 1.4, Symantec, February 2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Government of Canada, *Action Plan 2010-2015 for Canada's Cyber Security Strategy* http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx

Hannas, William C., James Mulvenon and Anna B. Puglisi, *Chineese Industrial Espionage – Technology Acquisition and Military Modernization*, (New York:Routledge, 2013)

Herridge, Catherine, *US data in Iranian hands after downed drone?,*10 February 2012, http://www.foxnews.com/politics/2012/02/10/us-data-in-iranian-hands-after-downed-drone/

Hoye, Matthew and Rene Marsh, *GAO: Newer aircraft vulnerable to hacking,* CNN, 14 April 2015, http://www.cnn.com/2015/04/14/politics/gao-newer-aircraft-vulnerable-to-hacking/

Lambeth, Benjamin S., *The Winning of Air Supremacy In Operation Desert Storm*, Santa Monica: RAND, 1993

Lynn, William J. III, *Defending a New Domain - The Pentagon's Cyberstrategy*, Foreign Affairs, October 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Rid, Thomas, *Cyber War Will Not Take Place*. New York: Oxford University Press, 2013

Roberts, John, *EXCLUSIVE: Drones vulnerable to terrorist hijacking, researchers say*, Fox News, 25 June 2012, http://www.foxnews.com/tech/2012/06/25/drones-vulnerable-to-terrorist-hijacking-researchers-say/

Sangerjune, David E., *Obama Order Sped Up Wave of Cyberattacks Against Iran,* The New York Times, 1 June 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0

Thatcher, Chris, *Operationalizing the Cyber Domain,* Vangard, 26 June 2013. http://vanguardcanada.com/operationalizing-the-cyber-domain/

Ward, Carroll, *Israel's Cyber Shot at Syria*, Defense Tech, 26 November 2007, http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria/

Zetter, Kim, *10k Reasons To Worry About Critical Infrastructure*, Wired, 24 Jan 12, http://www.wired.com/2012/01/10000-control-systems-online/

http://www.stratcom.mil/factsheets/2/Cyber_Command/

http://www.au.af.mil/info-ops/cyberspace.htm#usafcyber