National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE CHALLENGES OF OFFENSIVE CYBER OPERATIONS IN THE CANADIAN ARMED FORCES

Maj Kristin Strackerjan

JCSP 43 DL

Exercise *Solo Flight*

Disclaimer

PCEMI 43 AD

Exercice *Solo Flight*

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

THE CHALLENGES OF OFFENSIVE CYBER OPERATIONS IN THE CANADIAN ARMED FORCES

Maj Kristin Strackerjan

Word Count: 2463

Compte de mots: 2463

THE CHALLENGES OF OFFENSIVE CYBER OPERATIONS IN THE CANADIAN ARMED FORCES

INTRODUCTION

Canada's role, throughout much of history, has been one of peacemaker, peacekeeper and one in stark contrast to our more powerful neighbours to the south, the United States. Although we have been active participants in large scale wars and conflicts, stretching form the First World War onwards, we have intentionally avoided entering the more controversial conflicts such as the War in Vietnam and the War in Iraq. The ethical, moral, political and legal implications that allowed us to avoid involvement in these wars are not dissimilar to the collective aversion to engaging in offensive, or active, cyber operations. Such engagement requires a change in perspective and an understanding that challenges the concepts of conventional warfare. This essay will focus on where Canada currently stands in comparison to its Allies, specifically NATO, the United Kingdom and Australia, and the real and perceived barriers for Canada to engage in offensive cyber operations in international conflicts.

WHAT ARE OFFENSIVE CYBER OPERATIONS?

Offensive Cyber Operations (OCO) are defined as "activities that, through the use of cyberspace, actively gather information from computers, information systems, or networks, or manipulate, disrupt, deny, degrade, or destroy targeted computers, information systems or networks"[1]. As with Offensive Air Operations, the intent is to destroy weapons, systems or

[1] Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, Subject: Joint Terminology for Cyberspace (November 2010): p13.

infrastructure, prior to their use by an adversary. Unlike conventional warfare, this battle ground for OCO does not occupy a consistent physical space. Using networks that travel or link through any number of nations and territories, it is possible to gain access to the networks of an adversary without them knowing. The ultimate element of surprise.

When and how OCO techniques are employed is not always well-defined or understood for most nations, even those who currently possess these weapons. Canada's current defence policy highlights that "we will develop the capability to conduct active cyber operations focused on external threats to Canada in the context of government-authorized military missions"[2] while reflecting Canadian values and recognizing that this is uncharted legal territory.[3] These statements offer little in the way of clear guidance but give Canada and its defense forces the opportunity to explore OCO.

WHAT ARE THE RISKS?

Since the Second World War, nations have made considerable progress in their efforts to avoid the escalation of conflicts by using diplomacy and cooperation. These means of engagement have further built trust between nations. The strength of this trust will continue to be tested and cyber operations have the potential to undermine it. The twenty-first century has a battlefield, the internet, that is global. Any changes which occur within its boundaries will have an impact on all. In an age of 'fake news' we are already seeing the power that those with the cyber means, namely Russia and China, yield. What will occur when the internet and everything that connects to it can no longer be trusted?

---

[2] Minister of National Defence, Strong, Secure, Engaged: Canada's Defence Policy, (Ottawa: DND, 2017), p72.

[3] *Ibid*., p8.

Powerhouse nations such as the United States (US) are at the leading edge of developing offensive cyber weapons.[4] Stuxnet, "one of the most advanced and sophisticated viruses ever developed"[5] demonstrated that the US has the means and the will to use its offensive cyber capabilities. Yet, while they are strong, they are also incredibly vulnerable. China has repeatedly outplayed the US in cyber-attacks, stealing personal information of millions of American citizens as well intellectual property from Western corporations.[6]

"The best defence is a good offence"
- *unknown*

Terrorist and non-state actors are not new; however, they have exploited cyberspace to spread their doctrine, recruit new members and engage in offensive cyber activity. The risk of unreliable or ineffective cybersecurity is that it allows others to take advantage of our networks. Nations do not want to allow for unfettered access to their networks and, as such, have spent more time establishing their defensive, passive posture of deterrence by resilience rather than taking a more active role using deterrence by retaliation. These nations remain on their heels rather than in a position of control.

Are the risks greater for OCO than conventional offensive military operations? Friendly fire incidents have not been eliminated but they have been mitigated by ensuring that, for example, allies are able to effectively communicate. The rules of engagements in conventional warfare are clear and precise. Limiting the impact on civilians is paramount. Advances in technology have helped to ensure that the above-mentioned limitations and rules, among many others, are adhered to. In the virtual or cyber world, how are these assurances made? What are the unintended consequences of a cyber-attack on civilians? What order of precision is required? How is attribution made? These are all challenging questions with answers that are broad and have significant technical and knowledge requirements. Just as with the use of conventional

[4] Thomas J. Wright, *All Measures Short of War: The Contest for the Twenty-first Century and the Future of American Power*, (London: Yale University Press, 2017), p49.
[5] *Ibid.*, p49.
[6] *Ibid.,* p49.

weapons, it is essential that "the commander […] weigh up the potential for achieving operational goals against the risk of collateral effects and damage" and that there may not be a way to claim plausible deniability of its actions.[7]

WHAT ABOUT OUR ADVERSARIES?

Our lives are dependent on the continued success of a safe, trusted and protected cyberspace. We have developed our communications, financial and governmental infrastructures around interdependent networks. Our efficiencies have grown and so have our vulnerabilities. These advanced networks have offered many advantages, but they also come with great risks to our safety and security.

> IT-dependency often goes hand-in-hand with IT-capability; states that have developed an advanced cyber infrastructure are also the most likely to possess offensive cyber capabilities.
>
> - Micheal N. Schmitt & Liis Vihul[8]

Many nations with which our policies are not aligned are actively engaged in offensive cyber operations. They are active, they are flexible, and they are determined. China has been accused of stealing intellectual property, North Korea has used cyber tools to steal money, and Russia is accused of using various online means to influence the 2016 US presidential elections as well as has been engaged in bringing down Ukrainian power stations and the government websites of Estonia and Georgia.[9]

Although Allies, such as the US, are also moving forward with their own cyber capabilities, it is perhaps more relevant, due the size of our economies and militaries, that we focus on the efforts being put forward by Australia and the United Kingdom.

---

[7] Fergus Hanson, Tom Uren, "Policy Brief: Australia's Offensive Cyber Capability", p8.

[8] Micheal N. Schmitt, Liis Vihul, "Proxy Wars in Cyberspace", *Fletcher Security Review*, Vol I, Issue II (Spring 2014), p60.

[9] *Australia's Offensive Cyber Capability*, p.5.

WHAT ABOUT OUR ALLIES?

NATO

Following the meeting of the North Atlantic Council at the level of Defence Ministers on 8 November 2017, NATO Secretary General Jens Stoltenberg announced the creation of a Cyber Operations Centre which would allow nations to use their cyber capabilities within the context of NATO Operations.[10] This shift in position on the use of offensive cyber capabilities is significant and is likely in response to Russia's relentless cyber-attacks in recent years. The potential for NATO to invoke Article 5[11], NATO's mutual defence clause, should be considered to protect ally nations, such as the Baltic states. The threat of US OCO capabilities in the events of a Russian cyber-attack is a credible deterrent.

NATO has acknowledged that its accepted defensive posture is no longer sufficient. It is necessary policy and practice to keep up with the times and determine how the collective cyber capabilities may be used and shared. NATO will need to address how safely-guarded cyber intelligence is shared and how to overcome the reluctance of nations to share their single-use cyber weapons. In order to accommodate individual nations, and the legal and political issues which each will need to address, these cyber capabilities will remain under the control of the nations'[12] bringing the capabilities and not by NATO as other, traditional, assets are.

---

[10] http://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/, Created on: December 7, 2017.

[11] *The North Atlantic Treaty (1949)*

[12] https://ccdcoe.org/cyber-security-strategy-documents.html, Accessed on 21 May 2018.

AUSTRALIA

The current Australian cyber strategy[13] was established in 2016 with a focus on cyber-security and cyber defence. Australia's Cyber Security Strategy mentions offensive cyber capabilities but provides no details on how they will be used.

In April 2016, Prime Minister Turnbull confirmed that Australia has an offensive cyber capability.[14] This was among the first statements from any nation to publicly declare such a capability. The use of their defensive and offensive capabilities will enable them to deter and respond to the threat of cyber-attacks. The use of these capabilities is seen as consistent with their continued support for the international rules-based order and their obligations under international law. Australia has been clear that any cyber operations will continue to follow the laws of armed conflicts and will require higher levels of approval for particularly sensitive targets.

In a system of checks and balances, Australia has identified four key areas which must be addressed when considering cyber operations: necessity, specificity, proportionality and harm.[15] Legal, foreign policy and national security advice are sought from outside of defence.

UNITED KINGDOM

The UK's five-year cyber strategy[16] was renewed in 2016. In a similar approach to Australia, the UK has declared its ability to use its offensive cyber capabilities when and where needed. They have a taken a strong position by stating that they "will deliver clear messages about consequences to adversaries who threaten to harm [their] interests, or those of [their] allies,

---

[13] Australia's Cyber Security Strategy, (Commonwealth of Australia: 2016).
[14] *Australia's Offensive Cyber Capability*, p.4.
[15] *Ibid.,* p8-9.
[16] National Cyber Security Strategy 2016-2021, (HM Government: 2016).

in cyberspace".[17] Unlike the Australian Cyber Strategy, the UK created a small space to highlight the use of offensive capabilities through its National Offensive Cyber Program.

Key to the success of any significant programmatic or operational change is the need to ensure adequately skilled personnel. The UK has the desire to become "a world leader in offensive cyber capability" and has highlighted the need to establish "a pipeline of skills and expertise to develop and deploy […] sovereign offensive cyber capabilities."

HOW DOES CANADA COMPARE?

Canada's Cyber Security Strategy[18] has not been updated since 2010 and, without it, there is no over-arching strategic level document which focuses solely on Canada's cyber capabilities. The current Defence Policy, *Strong, Secure, Engaged*, released in 2017, highlights a more assertive posture in the cyber domain and it is set as one of the key areas for growth and investment. The new defence policy gives the military the green light to "develop active cyber capabilities and employ them against potential adversaries," which means it will be able to conduct offensive operations online.[19]

National defence and the role of the military overseas is consistently under scrutiny. Its actions are questioned, and every misstep analyzed. It is crucial that the public perceptions be addressed to minimize the backlash if or when any OCO take place. While there are guidelines written into the CSIS Act[20], there is a reasonable expectation of privacy for Canadian citizens. How does the government balance that need for privacy with that of National Security, at home and abroad? The process for approving CSIS warrants to conduct its investigations is secret. As

---

[17] *National Cyber Security Strategy*, p9.

[18] Minister of Public Safety, Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada (Ottawa: PSEP, 2010).

[19] http://www.cbc.ca/news/politics/cyber-weapons-canada-1.4164696, Last Updated: June 18, 2017.

[20] Canadian Security Intelligence Service Act, (Ottawa: 1985).

such, the public at large is not part of that process and would largely be unaware of the activities being conducted.[21]

Bill C-59[22] was introduced in the House of Commons in June 2017. This Bill is an overhaul of the CSIS Act and, among other things, provides "new cyber mandate that will allow [CSE] to attack as well as defend cyber threats, on top of its signals-intelligence and cyber defence role."[23] This expansion into an offensive role cannot infringe upon the global information infrastructure in Canada nor the *Canadian Charter of Rights and Freedoms*. These limitations were made to ensure that the privacy of Canadian citizens is held paramount without compromising national security.

SSE also refers to the authorization for the CAF to conduct OCO, or active cyber operations, in government-authorized missions. There will be an investment in future cyber capabilities which will increase our abilities to "target, exploit, influence and attack in support of military operations"[24]. To ensure that there is no confusion or misunderstanding, it is explicit when it refers to cyber operations and that they will be "subject to all applicable domestic law, international law, and proven checks and balances such as rules of engagement, targeting and collateral damage assessments"[25].

GAPS

Although our strategic cyber documentation is significantly out-of-date, Canada appears to be on a similar path as our closest allies insofar as our desire to participate and the acceptance

[21] Craig Forcese, Bill C-59 and the Judicialization of Intelligence Collection, p40.
[22] https://www.macleans.ca/politics/ottawa/the-roses-and-thorns-of-canadas-new-national-security-bill/, Created on June 20, 2017.
[23] *Ibid.*
[24] *SSE*, p41.
[25] *SSE,* p15.

of our role in OCO. There seems to be a larger gap in our ability to fulfill these roles. There are personnel, legal and technological gaps which must be addressed prior to Canada becoming a serious partner in cyber operations.

The *SSE* identified the need to invest in personnel to address the increasing demands in the field of cyber and the need to attract skilled people to the highly technical cyber domain.[26] At a time when the CAF is suffering from some significant retention and recruitment issues, this task may be one of the more significant ones to address. "This means attracting and keeping the brightest young minds, the sharpest skilled local talent and the most experienced technology veterans to drive and grow a pipeline of cyber specialists, and in turn help protect and serve… military and economic interests".[27]

Legally, NATO will need to address its understanding and application of Article 5[28]. An attack against one or more of the NATO members shall be considered an attack against them all in both the armed and cyber sense. There will need to be an understanding of what the different types of cyber weapons are capable of and what limits should be placed on them. Although NATO is not new, the use of hybrid methods creates challenges in terms of "detection, attribution and response for Canada and its allies".[29] Understanding the limits of each participant country will also factor into how NATO may react as a cohesive group to outside cyber threats.

Finally, technology. Technology is changing faster than laws can keep up with it. Canada, as well as all other nations, will be buried by the potentially huge amounts of data that could be drawn from operations around the globe. How to address big data, changes in the rules

---

[26] *SSE*, p13.
[27] *Australia's Offensive Cyber Capability*
[28] *The North Atlantic Treaty*
[29] *SSE,* p53.

of Internet usage and computer processing powers are all on-going challenges and the laws which allow or prohibit them will need to keep pace.[30]

CONCLUSION

The direction from the Government of Canada in the strategic use of offensive cyber capabilities against non-Canadian entities is an exciting shift from the limitations of conventional warfare. An in-depth assessment of the current NATO, Australian and UK positions on their intended uses of cyber as a weapon indicates that Canada is not too far off the current pace. While we are not likely to ever to be the most aggressive players, we are in the game and are now willing to play by similar rules. There are many possibilities for Canada to invest in options to develop our own approach to OCO, but time will tell whether we are able to meet the personnel, legal and technical requirements to become contenders with are closest allies. These challenges are current and relevant to all of our allies and so we will likely face them together.

[30] https://www.canada.ca/en/security-intelligence-service/news/2017/06/amendments_to_thecsisact-dataanalytics.html, last updated: 2017/06/20.

BIBLIOGRAPHY

Forcese, Craig, Bill C-59 and the Judicialization of Intelligence Collection (April 6, 2018). Ottawa Faculty of Law Working Paper No. 2018-13.

Government of Canada. Minister of National Defence, Strong, Secure, Engaged: Canada's Defence Policy, (Ottawa: DND, 2017).

Government of Canada. Canadian Security Intelligence Service Act, (Ottawa: 1985).

Government of the United States of America. Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, Subject: Joint Terminology for Cyberspace (November 2010).

Government of Australia. Australia's Cyber Security Strategy, (Commonwealth of Australia: 2016).

Hanson, Fergus, Tom Uren. "Policy Brief: Australia's Offensive Cyber Capability"

Schmitt, Micheal N., Liis Vihul. "Proxy Wars in Cyberspace", *Fletcher Security Review*, Vol I, Issue II (Spring 2014)

https://ccdcoe.org/cyber-security-strategy-documents.html

http://www.cbc.ca/news/politics/cyber-weapons-canada-1.4164696

https://www.macleans.ca/politics/ottawa/the-roses-and-thorns-of-canadas-new-national-security-bill/

https://www.canada.ca/en/security-intelligence-service/news/2017/06/amendments_to_thecsisact-dataanalytics.html

http://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/

Wright, Thomas J. *All Measures Short of War: The Contest for the Twenty-first Century and the Future of American Power*, (London: Yale University Press, 2017)

The North Atlantic Treaty (1949)