National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

OFFENSIVE CYBER IN THE CANADIAN ARMED FORCES: OPPORTUNITIES FROM BILL C-51

Maj N.B. Marshall

JCSP 42

Service Paper

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 42

Étude militaire

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 42 – PCEMI 42
2015 – 2016

JCSP SERVICE PAPER – PCEMI ÉTUDE MILITAIRE

OFFENSIVE CYBER IN THE CANADIAN ARMED FORCES: OPPORTUNITIES FROM BILL C-51

Maj N.B. Marshall

Word Count: 2584

Compte de mots: 2584

OFFENSIVE CYBER IN THE CANADIAN ARMED FORCES: OPPORTUNITIES FROM BILL C-51

AIM

1. The aim of this paper is to explore the potential opportunities that Bill C-51, The Anti-Terrorism Act, 2015, may create for the cyber domain within the Department of National Defence (DND) and to make recommendations on what strategy would be best to follow both internally and in collaboration with Other Government Departments (OGD) as the changes in laws are implemented.

INTRODUCTION

2. The Department of National Defence (DND) has long recognized the potential of cyber operations as a force multiplier to gain advantage over potential adversaries. However, DND has been restricted to defensive cyber operations because it lacked the legal mandate to carry out offensive cyber operations. With the changes in laws from the passing of Bill C-51, the Government of Canada has clearly expressed a desire to proactively use non-lethal force to reduce threats to the security of Canada. Offensive cyber operations, particularly those executed by DND, have the potential to support this new Government approach.

3. This paper will first examine the policy background and roles for cyber operations both for DND and for various Whole of Government (WoG) stakeholders. Second, the changes in law stemming from Bill C-51 will be examined, particularly with respect to the cyber domain. Potential courses of action will be developed and compared and, a recommended way ahead will be laid out.[1]

[1] Activities within the cyber domain are typically dealt with at the highest security classifications. This service paper is written at the UNCLASSIFIED level and its drafter has not been read into the classified aspects of cyber policy and plans. Additionally, references supporting this paper all come from the public domain to ensure that its content remains widely publishable. It is, therefore, entirely possible that DND cyber strategy has already been developed and has not been released to the public due to its classification. In that scenario, this paper addresses a solved problem.

DISCUSSION

Background

4. From the early days of the Internet, Canada has seen security and protection of cyber as a multi-departmental and multi-agency responsibility. Based on the 2010 *Canada's Cyber Security Strategy*, "cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks."[2] Threats to Canada's cyber infrastructure and the information residing on it can come from cybercrime, terrorism, or state-sponsored espionage and military activities.[3] Of particular note is the idea that in many cases "cyber-attacks are a central element of military strategy," for potential adversaries.[4] Overall, *Canada's Cyber Security Strategy* outlines the various departmental responsibilities for activities in the cyber domain.

5. Public Safety Canada. Public Safety Canada (PS) is the lead cyber coordinating body for all of Canada. Through the Canadian Cyber Incident Response Centre (CIRC) it "will continue to be the focal point for monitoring and providing advice on mitigating cyber threats, and directing the national response to any cyber security incident."[5] PS also has the mandate to improve public awareness of the cyber threat and how every Canadian can reduce the risks.[6]

6. Department of National Defence. DND receives its mandate for the defence of Canada from the *National Defence Act*, where the Canadian Forces are named as the "armed forces of Her Majesty raised by Canada and consist of one Service called the Canadian Armed Forces."[7]

---

[2] Canada, Public Safety Canada, *Canada's Cyber Security Strategy*, Government of Canada (2010), 2.
[3] Ibid, 5.
[4] Ibid.
[5] Ibid, 10.
[6] Canada, Public Safety Canada, *Action Plan 2010-2015 for Canada's Cyber Security Strategy*, Government of Canada (2013), 12.
[7] *National Defence Act*, (1985): 14.

In the cyber domain, DND is tasked with the security of its own military networks[8] and, through Defence Research and Development Canada, it is responsible for cyber security science and technology "not specifically assigned to another department or agency."[9] Additionally, DND will "work with other Government departments to identify threats and possible responses."[10]

7. Communications Security Establishment. Communications Security Establishment (CSE) is an Agency under DND. CSE has three mandates, directed by the *National Defence Act*:

A. To acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities.

B. To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada.

C. To provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.[11]

8. Notably, CSE cannot target Canadians abroad or anyone in Canada under its (A) and (B) mandates. Only with a warrant and request from the law enforcement or security agency can it target Canadians or anyone in Canada under its (C) mandate.[12] Further, it outlines an expectation that the Canadian Armed Forces (CAF) will support CSE's activities, specifically, "the Minister

[8] "DAOD 6003-0, Information Technology Security," accessed January 16, 2016, http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-6000/6003-0.page.
[9] "Cyber Security in the Canadian Federal Government," accessed January 16, 2016, http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-eng.aspx.
[10] Canada, Public Safety Canada, *Canada's Cyber Security Strategy*, 10.
[11] "What we do and Why we do It," accessed January 17, 2016, https://www.cse-cst.gc.ca/en/inside-interieur/what-nos.
[12] Government of Canada, *National Defence Act*, 273.64.

of National Defence may issue directions for the Canadian Forces to support [CSE] in carrying out activities."[13]

9. Canadian Security Intelligence Service. The Canadian Security Intelligence Service (CSIS) investigates "activities suspected of constituting threats to the security of Canada, and [reports] on these to the Government of Canada," as mandated in the *CSIS Act*.[14] CSIS has a role in the cyber domain, specifically to work "closely with other government departments and international partners in order to remain abreast of the global threat."[15] They are also responsible to "analyze and investigate domestic and international threats to the security of Canada," including cyber threats.[16]

10. Royal Canadian Mounted Police. The Royal Canadian Mounted Police (RCMP) draw their authorities from the *RCMP Act* to investigate "suspected domestic and international criminal acts against Canadian networks and critical information infrastructure."[17] It operates the Cyber Crime Fusion Centre in order to "advance situational awareness and analysis of cyber-crime trends" and is the lead agency for the *Canadian Cyber Crime Strategy*.[18]

11. Clearly, the Government of Canada sees its interests in cyber as a team effort. PS is the coordinator, running the CIRC and leading the public awareness campaign. CSIS, with its broad intelligence mandate, deals with all threats to Canadian security, including cyber. The RCMP focuses on cyber-crime while CSE collects foreign cyber intelligence, helps protect Canadian cyber infrastructure, and provides cyber assistance to other agencies. Finally, DND secures its military networks, conducts cyber research, and supports OGD identifying threats and responses.

---

[13] Ibid, 273.65(6).
[14] "Role of CSIS," accessed January 16, 2016.
[15] "Cybersecurity and Critical Infrastructure Protection," accessed January 16, 2016, https://www.csis-scrs.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php.
[16] Canada, Public Safety Canada, *Canada's Cyber Security Strategy*, 10.
[17] Ibid.
[18] Canada, Public Safety Canada, *Action Plan 2010-2015 for Canada's Cyber Security Strategy*, 12.

12. Interestingly, no organization had been given the mandate to carry out offensive cyber operations, or Computer Network Attack (CNA), which would be defined as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[19] This changes with the passing of Bill C-51.

Bill C-51

13. Following two domestic terrorist attacks killing two uniformed CAF members in three days in October 2014, the Government shortly thereafter introduced Bill C-51, the *Anti-Terror Act, 2015,* which was introduced to Parliament in January 2015 and received Royal Assent in June 2015.[20] Essentially, the Bill was intended to strengthen Canada's security through the better sharing of information and the better targeting of potential threats to Canada.[21,22]

14. Bill C-51 is separated into four distinct parts. Each part includes its own text and several amendments to existing Acts in order to properly reflect the Bill's intentions.

15. Part I – Security of Canada Information Sharing Act. The first part deals with the establishment of the *Security of Canada Information Sharing Act,* which was established "to encourage and facilitate the sharing of information among Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada."[23] Sharing security information between 17 departments and agencies is identified with the expectations to

---

[19] Steve Winterfeld and Jason Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Amsterdam: Syngress/Elsevier, 2013), 73.
[20] Aaron Wherry, "The Long and Short of C-51, the Anti-Terror Act," *Maclean's* (June 25, 2015).
[21] Ibid.
[22] The bill remains contentious and the new Liberal government promised to repeal unconstitutional elements of Bill C-51 – the specifics of which have yet to be released (Fine, 2015). Nevertheless, it is unclear what changes may be possible as the mandate for domestic collection of intelligence was not changed under C-51 (Wherry, 2015). It appears, then, that the government will focus on oversight and not make any significant changes to intelligence collection policy. (Fine, 2015).
[23] *Anti-Terrorism Act, 2015*: 6.

"disclose information … if the information is relevant to the recipient institution's jurisdiction or responsibilities."[24]

16. Part II – Secure Air Travel Act. The second part expands on the use of "no-fly" lists to enhance the security of air travel. Of particular note, the Act stipulates that the Minister of Transport may access any data on a computer network within any aircraft, or air transport facility without a warrant provided that the data is not to be used for criminal prosecution.[25] Potentially, this would allow bulk access to the data on travellers' personal mobiles and computers once they are connected to airport Wi-Fi networks.

17. Part III – Criminal Code. The third part makes amendments to the *Criminal Code*. The critical change is to make "communicating statements" advocating or promoting "the commission of terrorism offences in general" a crime punishable to up to five years in prison.[26] As an adjunct, it also allows the courts to compel the removal of "terrorist propaganda" from computer networks by the system's custodian.[27]

18. Part IV – Canadian Security Intelligence Service Act. The forth part increases CSIS' mandate to include the ability to take measures to reduce the threats to Canadian security. The relevant sections are reproduced here in detail:

> (1)If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat.

---

[24] Ibid, 5(1).
[25] Ibid, 28.
[26] Ibid, 16.
[27] Ibid.

(2) The measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat.

(3) The Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to other Canadian law, unless the Service is authorized to take them by a warrant issued under section 21.1 [which outlines the warrant process].

(4) For Greater certainty, nothing in subsection (1) confers on the Service any law enforcement power.

(5) In taking measures to reduce a threat to the security of Canada, the Service shall not cause, intentionally or by criminal negligence, death or bodily harm to an individual; willfully attempt in any manner to obstruct, pervert or defeat the course of justice; or violate the sexual integrity of an individual.[28]

19. Additionally, CSIS can request support in fulfilling this mandate and a judge can compel any person to assist with the execution of a warrant.[29]

20. Part V – Immigration and Refugee Protection Act. The final part of the Bill adds some minor amendments to the processes of implementation and review of Security Certificates.[30]

21. Although not explicitly stated in Bill C-51, it is clear that cyber plays a significant role in the Government's tougher stance on security. Part II provides blanket access to all data that touches aircraft or airports and Part III allows for the electronic seizure of terrorist propaganda.

---

[28] Ibid, 42.
[29] Ibid, 45.
[30] Ibid, 52-59.

More importantly, one of the most likely methods of executing a non-lethal threat reduction will be the use of cyber operations, particularly CNA.

22. Further, Parts I and IV both lay out expectations of sharing and mutual support between departments and agencies with a view to improving security overall.

23. Given the changes stemming from the passing of Bill C-51, DND needs to decide what its response will be with respect to offensive cyber operations. There are three distinct courses of action (COA) available to the Department: take a narrow interpretation of the Bill, refrain from taking any interpretation at all, or take a wide interpretation.

Course of Action 1 – Narrow Interpretation

24. Generally, this COA sees no implied tasks arising from the changes of Bill C-51. Since DND received no additional tasks and there were no amendments to the *National Defence Act*, then it is very straightforward to conclude that there is nothing new here for defence. This assessment would lead to DND notifying its partners, particularly CSIS that any changes required to cyber capabilities are a CSIS-internal matter. This is simply not a DND problem.

25. The advantages here are that DND can stay static, consolidating its current capabilities while simultaneously being able to appear decisive to its defence and security partners. The disadvantages are that should a CNA capability be required in the future, then the Department would be no further ahead and that DND would be seen to not be contributing to the WoG approach and shirking any further contribution to Canada's security.

Course of Action 2 – No Interpretation

26. This COA sees no decision being taken at this time. Although there *may* be implications in Bill C-51 suggesting offensive cyber capabilities and that there *may* be a request for DND to support should this be the case, there is just too much uncertainty to do anything at this time. It

would be far more prudent to wait until CSIS and other departments digest the changes and see what happens.

27. This is the low-risk option since not taking a stand allows DND to adopt a capability if later asked or to continue to do nothing if no request for support comes. It is also a simple plan as it maintains the status quo. The chief disadvantage is that it cedes the initiative – DND would no longer have an opportunity to shape how overall cyber operations in Canada are conducted. Second, if DND is later asked to help with CNA then it will be unprepared to do so, perhaps embarrassing the Department.

Course of Action 3 – Wide Interpretation

28. This COA sees DND assuming that CSIS will need assistance in the reduction of foreign and domestic threats through cyberspace. Further, it is likely that the Department of Justice may require assistance removing terrorist propaganda, particularly when it is hosted outside of Canada. Therefore, DND, using both CSE and elements of the CAF, will create a CNA capability offering it as an asset to assist the WoG tackle the tough security challenges that it faces.

29. Not only does this COA offer the advantage of improving the overall security capability of Canada but also allows DND to shape the Government's cyber strategy as well as creating a new, potentially war-winning, military capability for the Department. This plan, however, would be risky. First would be the technical and fiscal challenges of creating a CNA capability. More important, though, is that OGDs may feel threatened by DND "taking over" cyber and that there would be potential policy and legal "rules of engagement" and targeting issues. Finally, public affairs may be an issue if the media begins to report on the "militarization of the Internet in Canada."

Weighing the Courses of Action

30. Based on the general language and specific wording throughout Bill C-51, it is clear that enhanced cyber capabilities are needed to meet the security requirements outlined by the Government. Further, the need to reduce threats in the cyber domain means that offensive cyber operations are required – collecting intelligence and monitoring cannot remove foreign terrorist propaganda nor disrupt a terrorist communication network. So the question is, what organization should have the lead to conduct CNA? The RCMP's cyber capability is focused on cybercrime and CNA activities may taint ongoing or future criminal investigations, so they are not suitable. PS's role is focused on coordination and information, which makes them unsuitable too. CSIS has the actual mandate to reduce threats to security. Conceivably, they could take the lead for CNA. However, their organization has just been given a significantly broader mandate across all domains, including collecting and taking threat reducing action outside of Canada. It might be better for them to define the targets for CNA and rely on a partner to execute operations. In fact, Rauri Nicholson of Public Safety argues that the evolving disruption strategy animated through C-51 lends itself to increased cooperation across the security and defence community, particularly in relation between the CAF and CSIS.[31] DND, including CSE, already has a strong technical cyber defence and exploitation mandate to defend the networks and gather intelligence which could be easily realigned to carry out offensive cyber operations.[32]

31. Although COA 3 has the greatest risk to DND with the potential public affairs, policy, legal, and technical challenges, a proactive approach would help mitigate these risks. Further, these "cosmetic" risks pale in comparison to the national security risks of not adequately dealing

---

[31] Rauri Nicholson, "The Relevancy Deficit: Bill C-51 and the Decline of Canadian Intelligence" (Canadian Forces College Paper, 2016), 23.

[32] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Amsterdam: Elsevier, 2014).

with threats that stem from COAs 1 and 2. Not stopping a terror attack because of interdepartmental frictions would be a far greater public affairs nightmare than the potential "militarization of the Internet." COA 3 also allows DND to remain relevant in the cyber domain, create a new, potentially critical capability for the future and to significantly support OGDs.

32. In consideration of the various COAs, COA 3 is recommended. The specifics of implementation of this COA would need further study. However, a first cut might be to have CSE conduct CNA on behalf of Canada domestically and against non-military strategic threats, while the CAF conducts CNA against military threats and against all foreign tactical threats. This would ensure that CSE is focused on security and the CAF is focused on military application of CNA. The CAF could also specialize in CNA insertion into closed networks in coordination with special operations forces as part of covert or clandestine operations.

CONCLUSION

33. Canadian cyber policy sees responsibility for effects in cyberspace shared between many different departments and agencies with an expectation of mutual support and information sharing. The recently passed Bill C-51 reinforces this relationship and further adds the responsibility to reduce threats to Canadian security using methods that would include offensive cyber operations.

34. DND can take three approaches to the need for CNA in a Canadian context. It can make it clear that it has no role to play, it can take no position for now, or it can assume that it is in the best position to execute CNA and move to create this capability in order to support the Whole of Government. Based on the opportunities and the risks, particularly to ensure the best security for Canada, building a CNA capability within DND is the best approach.

RECOMMENDATION

35. It is, therefore, recommended that DND create a CNA capability in both CSE and the CAF in order to be prepared to assist with the reduction of threats to the security of Canada. This will help ensure that, as our potential adversaries arm themselves with cyber weapons, Canada will be able to respond with a full spectrum of cyber capabilities as a response.

36. The next step is to share this vision with CSE and throughout the CAF, particularly the Chief of Force Development, the Canadian Forces Information Operations Group, and the Cyber Task Force.

BIBLIOGRAPHY

Andress, Jason and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Amsterdam: Elsevier, 2014.

Canada. Canadian Security Intelligence Service. "Cybersecurity and Critical Infrastructure Protection." Accessed January 16, 2016. https://www.csis-scrs.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php.

———. "Role of CSIS." Accessed January 16, 2016.

Canada. Communications Security Establishment. "What we do and Why we do It." Accessed January 17, 2016. https://www.cse-cst.gc.ca/en/inside-interieur/what-nos.

Canada. Department of Justice. *Anti-Terrorism Act, 2015.*

Canada. Department of Justice. *National Defence Act,* 1985.

Canada. Department of National Defence. "DAOD 6003-0, Information Technology Security." Accessed January 16, 2016. http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-6000/6003-0.page.

Canada. Public Safety Canada. *Action Plan 2010-2015 for Canada's Cyber Security Strategy*: Government of Canada, 2013.

———. *Canada's Cyber Security Strategy*: Government of Canada, 2010.

———. "Cyber Security in the Canadian Federal Government." Accessed January 16, 2016. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-eng.aspx.

Fine, Sean. "How Bill C-51 may Change Under Trudeau's Government." *The Globe and Mail* (November 15, 2015, 2015).

Nicholson, Rauri. "The Relevancy Deficit: Bill C-51 and the Decline of Canadian Intelligence." Canadian Forces College Paper, 2016.

Wherry, Aaron. "The Long and Short of C-51, the Anti-Terror Act." *Maclean's* (June 25, 2015).

Winterfeld, Steve, Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Amsterdam: Syngress/Elsevier, 2013.