National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CANADA'S CYBERSECURITY STRATEGY – BETWEEN CYBER WARRIORS AND CYBER MODERATES?

LCol J.M. Ingimundarson

JCSP 41

Exercise *Solo Flight*

Disclaimer

PCEMI 41

Exercice *Solo Flight*

Avertissement

Canada

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

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CANADA'S CYBERSECURITY STRATEGY – BETWEEN CYBER WARRIORS AND CYBER MODERATES?

LCol J.M. Ingimundarson

Word Count: 3057

Compte de mots : 3057

Introduction

Arguably, within the last decade in particular, nations have dedicated significant time, resources and effort to grapple with the concept of cybersecurity. Given the numerous national strategies written on the subject, including one by Canada, there appears to be a consensus that cybersecurity is a part of a larger national security issue. From within military circles, the term cyber has taken on a whole new dimension. Once used primarily to refer to the developing digital network environment populated by computers, data servers and the routers that moved the flow of information across the optical cable and wireless virtual paths, the term cyber has now come to refer to a completely new domain of operation that has literally interconnected the planet. In the same vein as the physical air, land and maritime environments, cyber is now accepted by western militaries as the new domain in which wars or at least military conflicts will be fought either exclusively in the future or in combination with actions taken in the other traditional physical environments. In a very similar manner, law enforcement makes a similar argument. Cyber becomes the new domain on the war on crime and the new front in protecting the resources and citizens of the nation state.

This then becomes part of the challenge in defining the roles of traditional security actors within the cyber domain. As mentioned, nations including Canada have taken steps to try and articulate through strategy documents the way forward or at least the framework in which these various agencies are to work in this domain. An inherent challenge with the cyber domain is that it does not respect national boundaries. The cyber domain operates at incredible speeds. The cyber domain is arguably not owned by any one person, agency, state or non-state entity. How then does Canada propose to meet threats that may present themselves in this new frontier?

This paper will present a comparative analysis of the cybersecurity policy espoused by Canada and some of its close allies, followed by an examination of possible options to strengthen Canada's cybersecurity policy.

What is cybersecurity?

Before launching into an analysis of selected states cyber strategies, this paper will start by defining a few relevant terms.

The term "cyber" at its most basic understanding will be accepted in this discussion to include those things of or relating to computers or computer networks.[1] With this basic dictionary definition; however, we will also accept that cyber refers to a domain in which individual and state activity virtually takes place. Unlike the physical environments of land, sea and air cyber is limited only by the communication infrastructures governed in part by the natural physical laws of the three traditional environments. The cyber domain transcends almost all borders and operates at speeds in excess of any currently available transportation platform. Arguably, it has interconnected individuals, states and non-state agencies and organizations in a manner never before thought possible with potential opportunity for both great positive and disastrously negative effects also never before considered or realized.

More germane then to this paper is the notion of cybersecurity. The NATO Cooperative Cyber Defence Center of Excellence (CCD COE) maintains a repository of cyber related definitions taken form a variety of states, national and international organizations.[2] Several significant observations can be made from reviewing the posted

[1]Merriam-Webster on line dictionary, http://www.merriam-webster.com/dictionary/cyber

[2]NATO Cooperative Cyber Defence Centre of Excellence. "Definitions" Last modified 10 May 2015, https://ccdcoe.org/cyber-definitions.html

definitions. First, each contributor has a slightly different take on the concept of cybersecurity. Common to the majority of these definitions is the notion of protecting or safeguarding the information residing within the information systems of that country, regardless of whether they are state, commercial or personal computer systems. Where the definitions seem to start to differ is in level of additional detail. South Africa by example highlights the need for policies, training and guidelines in its definition of cybersecurity.[3] Saudi Arabia, the USA and the National Institute of Standards and Technology (NIST) also include the ability to protect and defend their networks as part of their interpretation of cyber security.[4] For the sake of simplicity then I will refer again to the Miriam-Webster definition of cybersecurity which states that it is the measures taken to protect a computer or computer system against unauthorized access or attack.[5]

Security normally arises where one has conflict or war. Considering the notion of cyber conflict, I suggest that a strong definition for this term can be taken from the Proceedings of the 5th International Conference on Information Warfare and Security, which defined cyber conflict as a confrontation between two or more parties where at least one of the parties employs a cyber attack (i.e. use a computer to launch a virtual or information attack) against the other.[6] The conference expounded on their definition to explain that the nature of the conflict will differ depending on the goals or objectives of the parties involved. This is an inclusive definition of cyber conflict as the confrontation between parties could be criminal in nature – and hence a cybercrime – or could be

---

[3]Ibid

[4]Ibid

[5]Mirriam-Webster on line dictionary, http://www.merriam-webster.com/dictionary/cyber%20security

[6]Rain Ottis and Peeter Lorents, "Cyberspace: Definitions and Implications," The Proceedings of the 5th International conference on Information Warfare and Security, 8-9 April 2010, 269. http://books.google.ca/books?hl=en&lr=&id=nmMHBAAAQBAJ&oi=fnd&pg=PA267&dq=definition+cyber+conflict&ots=G17ttpYPTI&sig=Jnf_bb0EldOKLE3udecVHamdtRE#v=onepage&q=definition%20cyber%20conflict&f=false

outside the boundaries of law enforcement and be more military in nature, hence the potential for cyber warfare. Of interesting note, the NATO CCD COE does not list a definition of cyber conflict.

This brings us to the notion of cyber warfare. For the sake of this paper, cyber war and cyber warfare will be accepted as the same connotation. I believe that one of the better definitions or descriptions of cyber war comes from John Arquilla and David Ronfeldt of the RAND Corporation who defined cyber war as information related conflict where an enemy's command, control, communication and information systems become specific targets.[7] An objective of such a cyberwar would be to, at minimum, disrupt if not outright destroy the military communication systems that a nation would rely upon to develop situational awareness of and issue orders to its own forces while preserving an ability to know as much about your adversary and preserve your forces ability to organize and manoeuver.[8] It should be noted that the concept of cyberwar is not universally accepted. Thomas Rid, a noted cyber expert holds a competing theory that cyberwar has never taken place and instead what the world has witnessed is a modern, technologically advanced form of sabotage, espionage and subversion played about by and against state and non-state actors.[9] While compelling, a second competing counter argument also put forward by Arquilla and Ronfeldt in their definition of cyberwar is the concept of netwar.[10] Simplistically, netwar removes the military aspect of cyberwar but opens the range of effect options. A netwar can pit state on state or state on non-state actors against each other with the potential objectives of their attacks to include economic, political and

---

[7]John Arquilla and David Ronfeldt, *Cyberwar is Coming!*.(Washington, D.C.: RAND, 1993), 28. . http://www.rand.org/pubs/reprints/RP223.html

[8]*Ibid,* 30.

[9]Thomas Rid, "Cyberwar will Not Take Place," *Journal of Strategic Studies 35*, no. 1 (February 2012): 6. http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939

[10]John Arquilla and David Ronfeldt. "Cyberwar is Coming!" . . . ,28.

resource allocations. Given the potential for a netwar to arguably become militarized at some point in its conduct, the concept of cyberwar will be accepted as valid for the purposes of this research paper.

What is the threat?

In short, it is the very nature of cyber itself. National and international communication systems link individuals, businesses, commerce and trade to name but a few activities in seamless and instantaneous ways. Machines of industry, vehicle traffic control (air, land, sea, railway) and power generation can be monitored and controlled remotely. Financial transactions are not only transferred at near speed of light across global distances but these financial holdings are increasingly if not now the majority recorded solely by electronic means. Militaries, governmental leadership and law enforcement at all levels are at some point connected to and thru the same commercial communication infrastructure used by ordinary civilians. The potential for damage to a nation's economy, civil infrastructure not to mention the ability to influence national decision making are significant. The world has already been witness to several alarming incidents. In an interview former US Presidential Cyber Advisor Richard Clarke highlighted several incidents where several young 14-year old hackers, citizens of the USA, had managed to remotely take control of key civil infrastructure including dams on the Colorado River and an airport flight control tower in Massachusetts.[11] While the motivation for these "cyber incidents" appears intent only on either fulfilling a dare of skill or proving their cyber prowess, other incidents are potentially darker in tone. As

[11]Elizabeth Wasserman, "Top Cybercop Richard A. Clarke, the special Advisor to the President for Cyberspace Security, on the Threat of Cyberterrorism, Weapons of Mass Disruption, C-3PO, and the Power of 14-Year-Old Hackers." *Yahoo! Internet Life 8*, no.2 (February 2002): 76-78

James Joyner points out in his look at various national cyber visions, two east European nations have felt the effects of cyber attack. The Estonian government and aspects of Estonian life including newspaper access, banking and certain companies were significantly disrupted and halted for a short period as result of internet denial of service attacks against these areas over a dispute dealing with a ceremonial statue.[12] In a similar fashion Georgia experienced denial of service attacks against state internet services weeks before a conventional land and air invasion of Georgia's borders by Russian forces.[13] In short, while the benefits of the cyber domain are plentiful, the threats are also very real.

How do we compare?

Against this backdrop we will look at Canada's Cyber Security strategy in comparison to two of its close allies. To aid in this analysis, we shall consider elements from the Bartholomees strategy model focussing fundamentally on aspects pertaining to national interest and ends, ways, means of strategy implementation.[14]

Canada

In 2004 Canada produced its first national security policy. It outlined three primary security interests for Canada: protecting Canada and Canadians at home and abroad, ensuring Canada is not a base for threats to our allies and contributing to

[12]James Joyner, "Competing Transatlantic Visions of Cybersecurity." in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* edited by Derek S. Reveron, (Washington: Georgetown University Press, 2012), 61.

[13]Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Canada Communication Group, 2004), vii.

[14]J Bartholomees Jr, "Appendix II, Guidelines for Strategy Formulation" in *U.S. Army War College Guide to National Security Issues, Vol. II: National Security Policy and Strategy.* 3rd ed., edited J. Boone Bartholomees, Jr. (Carlisle, PA: Strategic Studies Institute: U.S. Army War College, June 2008): 277.

international security.[15] In order to address these core security interests the Canadian government highlighted several measures to be launched in key areas. Specific to this discussion, under the area of Emergency Planning and Management, the Canadian government committed to two specific measures pertaining to the cyber domain. The first was to increase the government's capacity to predict and prevent cyber attacks against its network while the second was to develop a national cyber security strategy.[16]

Six years later the government released the Canada Cyber Security Strategy. The strategy is defined around three pillars or objectives: securing government systems, partnering to secure vital cyber systems outside the federal government and helping Canadians to be secure online.[17] Its creation alone fulfills a key measure outlined in the overall national security strategy. Second, the cyber strategy documents the creation of Canada's Cyber Incident Response Centre (CCIRC), thus at least in part increasing government's capacity to predict and prevent a cyber attack and fulfilling a second measure of the national security strategy. The remainder of the document makes the case for the necessity of a cyber strategy and lays out the plan for achieving implementation, In terms of its first cyber objectives, the government makes clear the roles of each federal department meant to contribute to cyber security. Of interest is how little is mentioned about the role and manner in which the Department of National Defence is to be involved short of ensuring defence of its own networks and working in collaboration with allies on policies and legal frameworks for military cyber security aspects.[18] Arguably the strategy is very law enforcement and intelligence centric. CSEC is identified as not only the centre

[15]Privy Council Office. *Securing an Open Society: Canada's National Security Policy . . .*, vii.
[16]*Ibid,* ix.
[17]*Ibid,* 7.
[18]*Ibid,* 10.

for foreign intelligence on cyber incidents, but the response centre for attacks against federal government systems. The report informs Canadians that Canada is one of the few non-European nations to sign the Council of Europe's Convention on Cybercrime,[19] that the RMCP will create a Cyber Crime Fusion Center to better coordinate with CCIRC on cyber crime related activities and finally a number of proposed changes to national laws to better enable law enforcement to pursue cyber crimes. The strategy also points out that Canada will work in coordination with other international bodies such as NATO, the G8 and the UN on cyber issues in particular in developing an international governance structure for cyber conduct. Finally, the strategy highlights educating Canadians on methods they can personally employ as a means of strengthening Canada's cyber security. Privacy, the rule of law and accountability are also prevalent themes. It is interesting to note that it took until 2013 for the Government to round out is Cyber Strategy with a more detailed action plan. That action plan further announced a separate action plan between Public Safety – the Canadian Cyber Security lead – and the US Department of Homeland Security. Essentially, one thin strategy and two smaller action plans constitute the grand Canadian cyber strategy.

The United States of America

From the onset the US approach to cyber strategy is unique and extremely comprehensive. In two significant documents issued by different successive Presidents, the US has split its cyber strategy into a separate national and international one. Within its national strategy, Department of Homeland Security leads the charge to organize and unify the national US response to cyber incidents. The US national strategy is composed

[19] *Ibid,* 8.

of three objectives: prevention of cyber attack against America's critical infrastructure, reduction of national vulnerability to cyber attack and to minimize the damage and time to recover from a cyber attack.[20] These objectives are further refined around five cyber security priorities which can be briefly summarized as: improving response to a cyber incident, reducing cyber threat vulnerability, improved awareness and training programs, securing government networks and developing both national and international cooperation.[21] The US national strategy stresses government and commercial partnership to improving methods and response processes to national cyber incidents. Education of the public and industry leaders on self protection measures in cyber space are prevalent. There is a focus on protection of critical national civil infrastructure to include financial, health and agriculture.[22] Defence in the national strategy is focussed more on aspects of protecting its own networks. This is contrasted significantly in the international strategy where the US makes clear that it reserves the option, under the right to self-defence, to respond to hostile cyber acts with all options including a military one.[23] Both strategies also make mention of the importance of international partnerships. Within the national document the emphasis is on domestic intelligence gathering of cyber activities focussing on the FBI, the national police agency, and a direct reference to desiring to work with Canada and Mexico to develop North American cyberspace security.[24] International cooperation through forums such as G8, OAS, UN, ASEAN and others is mention

---

[20]Executive Office of the President of the United States. *The National Strategy to Secure Cyberspace.* (Washington, D.C.: U.S. Government Printing Office, 2003), viii.

[21]*Ibid,* 3-4.

[22]*Ibid,* 16.

[23]Executive Office of the President of the United States. *The International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World.* (Washington, D.C.: U.S. Government Printing Office, 2011), 13-14.

[24]Executive Office of the President of the United States. *The National Strategy to Secure Cyberspace . . .*, 50-51.

throughout the international strategy. What is unique to some of this messaging is the US expression to help develop cyber capacity in other nations not only to fight cyber crime and ensure a safe, secure virtual financial system for all, but to ensure the cyber domain is and remains a safe forum for the fundamental freedoms of self-expression and personal privacy.[25] In this manner governance of the internet to create universal norms of behaviour by state actors is also seen as a priority.[26]

The United Kingdom

The UK cyber strategy is a single, very comprehensive document. The UK cyber vision makes clear that a safe, secure and resilient cyber domain guided by national values such as the rule of law, transparency, fairness and liberty will provide for a more economically and socially prosperous and strong protected and secure society thru the obtainment of four key objectives.[27] Like the other mentioned nations, the UK sees cyber crime and the creation or re-affirmation of resilient national computer networks as key to their cyber vision attainment. Perhaps unique to the UK strategy is the clear articulation in its objectives that one, it wishes to play a very active role in shaping the future development of the cyber domain, assumedly through governance shaping and second, that education and training to ensure the necessary cyber skills are available within the nation to directly contribute to and ensure cyber security are a national priority.[28] The UK makes it very clear that ensuring the security of cyber space is a top national actionable

[25]Executive Office of the President of the United States. *The International Strategy for Cyberspace . . .,* 23-24.

[26]*Ibid*, 21-22.

[27]Minister for the Cabinet Office and Paymaster General. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World.* (Whitehall, London: Cabinet Office, 2011), 8.

[28]*Ibid*, 29.

priority.[29] Military involvement in cyber is very prevalent throughout the document. Highlights include the threat of the military as a target for cyber attacks,[30] reinforcing the idea of defence of military systems save for a brief mention of being able to counter cyber attacks as appropriate.[31] The creation of a new Defence Cyber Operations Group focussing and unify defence cyber efforts contributes to the UK's plans to increase its cyber defence capabilities. As with other nations, international cooperation and collaboration are seen as essential to securing UK cyber interests.

What should be Canada's continued way forward?

I believe there are three significant ways forward for Canada. First, Canada should better publicly articulate where its military commitment in cyber should be and then put in place the resources to exercise this intent. This will be challenging given a state's normal desire to keep such abilities secretive. Yet both the USA and UK have made their intentions know, can Canada truly not do the same? In keeping with our national cyber strategy, the Canadian Armed Forces has certainly pursued military avenues to operate in cyber space, to include not just defence but offensive options.[32] A possible reason for not being so public could be to preserve Canada's more peaceful international reputation. This may explain the nation's focus on cyber crime as a more palatable public serving of cyber security. In this same vein Canada should join its allies in pursuing international governance defining norms of proper state conduct in cyberspace. This relatively inexpensive venture would seem to play well into a generally accepted view of Canada as diplomatic negotiator. Finally, the UK's education and

[29]*Ibid*, 15.
[30]*Ibid.*
[31]*Ibid*, 26-27
[32]Department of National Defence. *CAF Cyber Operations Primer.* (Ottawa: Canada, 2014), 3-4.

training initiative for developing future cyber experts should be developed. An investment in this area would not simply aid Canada's cyber security but could lead to exploitable technology innovation improving and helping drive the Canadian economy.

Conclusion

Canada's national cyber security strategy is now entering its tenth anniversary. While modest in detail compared to at least two of its allies, the strategy has none the less provided initial guidance upon which the nation can focus its efforts. Like its allies, Canada has chosen internal focus and coordination of national assets and agencies to begin to prepare the cyber defences of the nation. Cyber crime has been and will remain a focus of the government as its presence publicly assists in securing the citizenry and the critical infrastructure such as commerce and trade upon which it relies. Canada has demonstrated its international commitments through the signing of cyber crime conventions. It is time now for Canada to consider its next public steps in the area of cybersecurity. For like the domain itself, Canada's cyber security strategy must continue to advance and address the complexities of this environment or risk being overtaken by it.

Bibliography

Arquilla, John and David Ronfeldt. *Cyberwar is Coming!* Washington, D.C.: RAND, 1993. http://www.rand.org/pubs/reprints/RP223.html

Arwood, Sam, Robert Mills, and Richard Raines. "Operational Art and Strategy in Cyberspace."Academic Conferences International Limited, Apr 2010, 2010.

Australia. Office of the Attorney- General for the Government of Australia. *Cyber Security Strategy.* Barton ACT: Commonwealth of Australia, 2009.

Bartholomees, J. Jr. "Appendix II, Guidelines for Strategy Formulation." In *U.S. Army War College Guide to National Security Issues, Vol. II: National Security Policy and Strategy. 3rd ed.,* edited by J. Boone Bartholomees, Jr. Carlisle , PA: Strategic Studies Institute: U.S. Army War College, June 2008.

Canada. Department of National Defence. *CAF Cyber Operations Primer.* Ottawa: Canada, 2014

Canada. Department of Public Safety. *Canada's Cyber Security Strategy.* Ottawa: Canada Communication Group, 2010.

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

Canada. Department of Public Safety. *Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security.* Ottawa: Canada Communication Group, 2012

Canada. Privy Council Office. *Securing an Open Society: Canada's National Security Policy,* Ottawa: Canada Communication Group, 2004.

Campen, Alan D. "Apathy and Incompetence Trump Terrorism in Cyberspace." *Signal* 59, no. 5 (Jan 2005, 2005): 43-46.

Deibert, Ronald J. "Toward Distributed Security and Stewardship on Cyberspace." In *Black Code: Inside the Battle for Cyberspace.* Toronto: MCClelland and Stewart, 2013.

Denning, Dorothy. "Cyberwarriors: Activists and Terrorists Turn to Cyberspace." *Harvard International Review* 23, no. 2 (Summer 2001, 2001): 70-75.

European Union. High Representative Of The European Union For Foreign Affairs And Security Policy. *Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions*

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels: European Commission, 2013.

Gunneriusson, Håkan and Rain Ottis. "Cyberspace from the Hybrid Threat Perspective."Academic Conferences International Limited, Jul 2013.

Joyner, James. "Competing Transatlantic Visions of Cybersecurity." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* edited by Derek S. Reveron, Washington: Georgetown University Press, 2012.

Liaropoulos, Andrew. "Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction?" Academic Conferences International Limited, 2013.

Ottis, Rain and Peeter Lorents. "Cyberspace: Definitions and Implications," The Proceedings of the 5th International Conference on Information Warfare and Security, 8-9 April 2010: 267-269. http://books.google.ca/books?hl=en&lr=&id=nmMHBAAAQBAJ&oi=fnd&pg=PA267&dq=definition+cyber+conflict&ots=G17ttpYPTI&sig=Jnf_bb0EldOKLE3udecVHamdtRE#v=onepage&q=definition%20cyber%20conflict&f=false

Platt, Victor. "Still the fire-proof house? An analysis of Canada's cyber security strategy." *International Journal 67,* no. 1 (Winter 2011/2012): 155-167. http://search.proquest.com/docview/1018566910?accountid=9867.

Reinbach, Andrew. "CYBER TERRORISM Strikes could as Easily be Perpetrated for Kicks by a Kid as by a Terrorist Once Trained by the CIA in Afghanistan, Whose Intent is to Harm America by Attacking its Lifeblood." *American Banker,* Sep 8, 1997, 1997.

Rid, Thomas. "Cyberwar Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (February 2012): http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939.

Rid, Thomas. "Cyberwar and Peace: Hacking Can Reduce Real-World Violence." *Foreign Affairs* 92, no. 6 (November/December 2013): 77-87. http://search.ebscohost.com/login.aspx?direct=tru&db=a9h&AN=91542532&site=ehost-live.

United Kingdom. Minister for the Cabinet Office and Paymaster General. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World.* Whitehall, London: Cabinet Office, 2011.

United States. Executive Office of the President of the United States. *The National Strategy to Secure Cyberspace.* Washington, DC: U.S. Government Printing Office, 2003.

United Sates. Executive Office of the President of the United States. *The International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World.* Washington, DC: U.S. Governemnt Printing Office, 2011.

Wasserman, Elizabeth. "Top Cybercop Richard A. Clarke, the Special Adviser to the President for Cyberspace Security, on the Threat of Cyberterrorism, Weapons of Mass Disruption, C-3PO, and the Power of 14-Year-Old Hackers." *Yahoo! Internet Life* 8, no. 2 (Feb 1, 2002, 2002): 1-78.