CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Canada and Cyber

by John Adams

July, 2016

2016 POLICY REVIEW SERIES

Canada and Cyber

by John Adams

CGAI Fellow
July, 2016

This essay is one in a series commissioned by Canadian Global Affairs Institute in the context of defence, security and assistance reviews by the Trudeau Government. The views expressed are those of the author and not CGAI. As a Canada Revenue Agency approved charitable organization, CGAI has no 'views' but rather acts as a platform and forum for intelligent discussion of Canadian global affairs policy.

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1600, 530 – 8th Avenue S.W., Calgary, AB T2P 3S8
www.cgai.ca

ISBN: 978-1-927573-69-3

We cannot fight new wars with old weapons
- Vinoba Bhave

Computers and information systems have become a fundamental part of Canadian life. Day-to-day activities, commerce and statecraft have gone digital. The associated information technology (IT) underpins nearly all aspects of today's society. It enables much of our commercial and industrial activity, supports our military and national security operations and is essential to everyday social activities.

A vast amount of data is constantly in motion and an astronomical quantity is being stored in cyberspace. Furthermore, owing to market incentives, innovation in functionality is outpacing innovation in security. Additionally, neither the public nor the private sector has been successful at fully implementing existing best known security practices. Consequently, data is vulnerable whether it is in motion or at rest.

What is cyberspace? According to Daniel Kuehl, "[c]yberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum (EMS) to create, store, modify, exchange, and exploit information via inter-connected information and communication technology-based systems and their associated infrastructures."[1]

There are several characteristics of cyberspace worthy of note:

- The cost of entry into cyberspace is cheap.
- For the time being, offence is easier than defence in cyberspace.
- Defence of IT systems and networks relies on vulnerable protocols and open architectures and the prevailing defence philosophy emphasizes threat detection not elimination of the vulnerabilities.[2]
- Exploits occur at great speed, putting defences under great pressure, as an attacker has to be successful only once, whereas the defender has to be successful all the time.
- Range is no longer an issue, since exploitations can occur from anywhere in the world.[3]
- The attribution of exploits is particularly difficult, which complicates possible responses.[4]
- Modern society's overwhelming reliance on cyberspace is providing any exploiter a target-rich environment, resulting in great pressure on the defender.[5]

People with expertise in software programming and manipulation concentrate their actions on exploiting the intricacies of computer networks and terrorize IT systems as follows:

- *Hacktivism*: an exploitation motivated by political activism that often involves defacing a website for the explicit purpose of publicly shaming the target.[6]

- *Cyber Crime*: a criminal offence involving a computer as the object of the crime (hacking, phishing, spamming), or as the tool used to commit a material component of the offence (child pornography, hate crimes, computer fraud).[7]

- *Cyber Espionage*: an exploitation to access covert information of national interest belonging to others.[8]

- *Cyber Terrorism*: the systematic threat or use of violence, often across national borders, to attain a political goal or communicate a political message through fear or intimidation of non-combatant persons or the general public.[9]

- *Cyber War*: disrupting or destroying information and communications systems with the intent of causing catastrophic damage and destruction of critical infrastructure, in the same league as bombs and bullets.[10]

Facebook

The term *cyber attack* is an umbrella term often used to include all of the exploitations above. The word 'attack' carries a lot of baggage with it. Generally it implies destruction of material and/or people and it could be construed to be an act of war. Consequently, the term cyber attack would be more accurately used to describe only those exploitations in support of cyber war.

Another term for such exploitations is *network warfare operations*. The term *cyber exploitations* is the more accurate umbrella term for all other exploitations enumerated above.

The government of Canada has responded to cyber exploitations with its Cyber Security Strategy.[11] Published in 2010, the strategy is noteworthy for the fact that it limits itself to strengthening the government's capability to detect, deter and defend against cyber attacks while deploying cyber technology to advance Canada's economic and national security interests. It did not militarize cyber security, it was limited to specifying that the Canadian Armed Forces were to strengthen their capacity to defend their own networks, work with other government departments to identify threats to their networks and possible responses, and continue to exchange information about cyber best practices with allied militaries.

The Department of National Defence and the Canadian Armed Forces were also to work with allies to develop the policy and legal framework for military aspects of cyber security, complementing international outreach efforts of Global Affairs Canada. It is noteworthy that cyber attacks were not on the table. Some may have despaired of this approach believing the best defence to be a good offence. There are several reasons why a more aggressive approach would have been ill-advised in 2010 in that cyber defence was the focus and the concept of cyber war had not yet sufficiently matured:

- By militarizing relatively low-level cyber threats, governments risk desensitizing the citizenry thereby creating a type of 'moral hazard,' which makes ordinary people and companies less likely to take responsibility for protecting themselves. That is exactly the opposite of the sort of behaviour a responsible government should want to encourage.

- Furthermore, one risks negating other "longer-term and more sustainable efforts"[12] to address the new challenges that cyber brings to security systems.

- Finally, one risks creating the impression that one is in a constant state of war where cyber is concerned, but with little evidence of damage or impact on citizens personally which might thereby engender cynicism and complacency.

What has changed since 2010 such that Canada should revisit its 2010 cyber strategy? To answer that question let us return to our discussion of cyberspace.

Many consider cyberspace to be the newest and most important addition to the global commons, which comprises four domains: maritime, air, space and now cyber. Cyberspace is now used by a quarter of the world's population and that number continues to expand. It has "become the centre of gravity for the globalized world, and for nations, the centre of gravity for all aspects of national activity, to include economic, financial, diplomatic, and other transactions including military operations."[13]

In essence digitization is now so pervasive that cyberspace is indispensable for transportation systems, electrical transmission grids, weapons systems, command and control systems, *inter alia*. It is, therefore, a very real concern that successful cyber attacks within cyberspace would have disastrous effects on the ability of states to function. Consequently, cyberspace has become an emerging theatre of operations and all states must be capable of operating therein. According to Fred Schreier, "[s]uccessful exploitation of this domain through network warfare operations could allow an opponent to dominate or hold at risk any or all of the global commons."[14] Harking back to the characteristics of cyberspace highlighted earlier, it is a domain where the classic restraints of distance, space, time and investment are reduced, sometimes dramatically, both for us and for potential enemies.

Power based on information resources is not new; cyber power is.[15] As Kuehl defines it, "[c]yberpower is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[16] Franklin Kramer defines it as "the use, threatened use, or effect by the knowledge of its potential use, of disruptive cyber attack capabilities by a state."[17] And Schreier argues that,

> The key strategic attribute of cyber power is the ability in peace and war to manipulate the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment.[18]

Cyber power capabilities challenge the strategist to integrate those capabilities with other elements and instruments of power. And this requires the crafting of a cyber strategy, which is "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational realms, to achieve or support the achievement of objectives across the elements of national power."[19] To develop a national strategy for cyberspace, therefore, is simultaneously to create cyber resources and procedures that can contribute to the achievement of specific national security objectives. Cyber war means disrupting or destroying information and communications systems with the intent of threatening a state's sovereignty. It also means trying to know everything about an adversary while keeping the adversary from knowing much about oneself.[20]

There are three forms of what have been called *computer network operations*:

- *Computer Network Attack*: operations designed to disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers or networks themselves.

- *Computer Network Exploitation*: retrieving intelligence-grade data and information from enemy computers by information and communications technology (ICT).

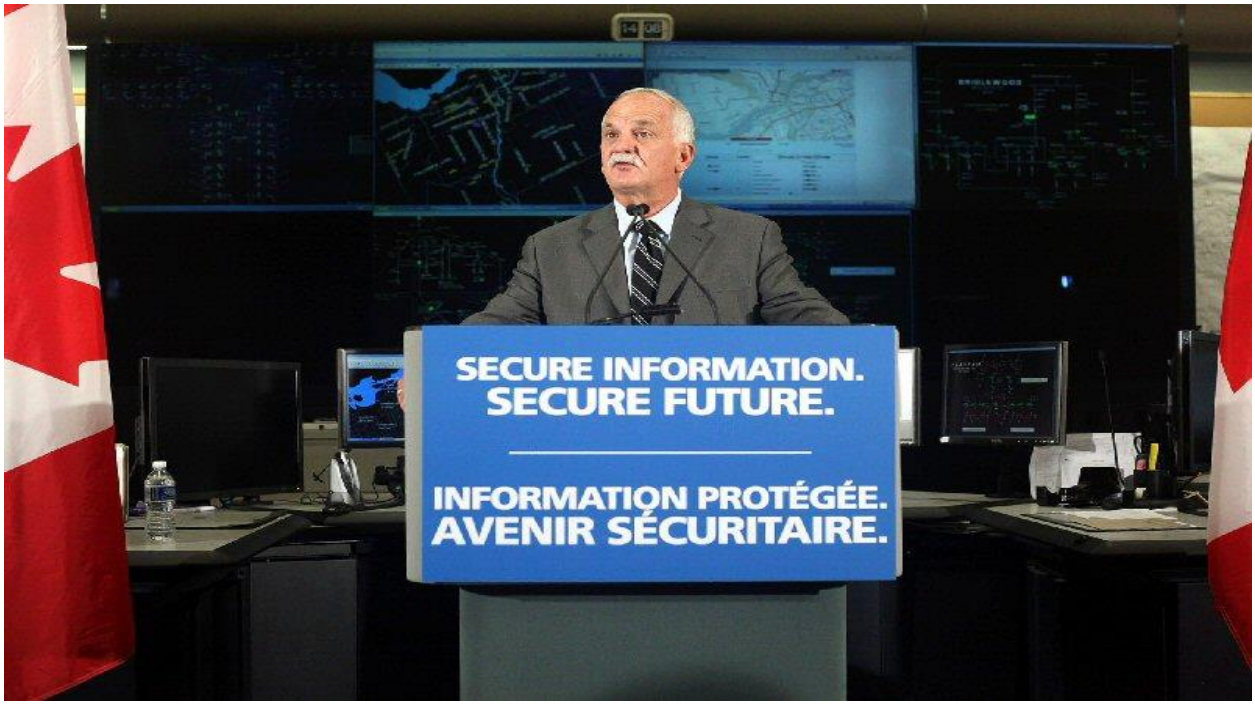
- *Computer Network Defence*: all measures necessary to protect your own ICT and infrastructures from hostile computer network attack and computer network exploitation.[21]

Computer network attack is still in its infancy, but its importance has increased immensely since 2010 and it will certainly increase considerably in the coming years.[22] Some people think that cyber war will sooner or later replace kinetic war. More frequently, cyber war is presented as a new kind of war that is cheaper, cleaner and less risky for an attacker than other forms of armed conflict. In either case, the Canadian Armed Forces have a responsibility not only to protect their own systems but they also need to have the authority to direct offensive action, in the form of cyber attacks, if that is what it takes to blunt an ongoing catastrophic attack on critical infrastructure at home. It would be neglectful beyond belief to leave the Canadian Armed Forces without access to offensive cyber capabilities and the requisite authority to attack a foreign adversary who is causing catastrophic damage to Canada's critical infrastructure through cyber war. Only then will the Canadian Armed Forces be relevant in future conflicts. This high priority responsibility and authority must be highlighted in the upcoming Defence Policy Review thereby ensuring that it is adequately resourced forthwith.

In that regard, it is noteworthy that in spite of days of contentious debate on the floor of the US Congress over the 2015 *National Defence Authorization Act*, there was a rare bipartisan consensus concerning cyber and it was fully funded.[23]

Also worthy of note is the fact that in April 2015, the United States released a new Cyber Security Strategy. Among other things, for the first time, it explicitly discusses the circumstances (see catastrophic attack above) under which cyber war could be used against an attacker.[24] This is why asking the Department of National Defence and the Canadian Armed Forces to work on

the policy/legal framework in 2010 was wise – *why* and *when* is easily as important as *how*, and actually harder to nail down. Not least of the policy questions is how/where capabilities should be developed and how/when accessed. If that's not clear, drumming up funding for weaponry development could be wasteful at best and disruptive/dangerous at worst. That work must be finalized, if it hasn't been already, as part of the Defence Review. It will be an essential component to an update of Canada's 2010 Cyber Security Strategy, which will be an indispensable complement to the Defence Policy Review.



Marketwire Photo/Public Safety Canada

The clarification of Canada's approach to cyber as highlighted above, within the Defence Review, in combination with the updated Cyber Security Strategy, would form the basis for Canada/US discussions regarding a CANUS Cyber Accord. Borders do not inhibit network warfare operations. Furthermore, elements of Canada's critical infrastructure, currently vulnerable to cyber attack, are shared. Accordingly, such an accord makes eminent sense and would deepen Canada-US defence cooperation.

Finally, to highlight the priority that the United States is placing on this matter, there is draft legislation before Congress which seeks to improve the Pentagon's defence procurement process for cyber warfare technologies by including these technologies within the Secretary of Defense's Rapid Acquisition Authority.[25]

In conclusion, the time for the government of Canada, the Department of National Defence and the Canadian Armed Forces to close the shortfall in the authority to engage in cyber war is now, and the perfect vehicle is the Liberal government's recently announced Defence Review to be done in lockstep with an update of Canada's Cyber Security Strategy.

[1] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr and Larry K. Wentz (eds), *Cyberpower and National Security*, Washington D.C., National Defence University Press, Potomac Books, 2009.
[2] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About it*, New York, Ecco, 2010, pp. 103-149.
[3] Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in Kramer, Starr and Wentz (eds), *Cyberpower and National Security*, Washington D.C., National Defence University Press, Potomac Books, 2009.
[4] Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*, New York, Oxford University Press, 2009.
[5] Clarke and Knake, *Cyber War*, pp. 170-175.
[6] "Hacktivism," Technopedia, available at www.techopedia.com/definition/2410/hactivism.
[7] Global Affairs Canada, "What is Cyber Crime?" available at http://www.international.gc.ca/crime/cyber_crime-criminalite.aspx?lang=eng
[8] "Definition of Cyber Espionage," PC Magazine, available at ww.pcmag.com/encyclopedia/term/64376/cyber.espionage
[9] FBI definition quoted by Margaret Rouse in a blog, 2010, available at searchsecurity.techtarget.com/definition/cyberterrorism
[10] "New Cyberwar Victims American Business," *Vanity Fair*, July 2013.
[11] Minister of Public Safety, "Canada's Cyber Security Strategy," 2010, available at www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx#fn12
[12] Mary Ellen O'Connell, "Cyber Security Without Cyber War," *Journal of Conflict and Security Law*, Vol. 17, No. 2 (2012), pp. 187-209, available at jcsl.oxfordjournals.org/content/17/2/187.full.
[13] Fred Schreier, "On Cyberwarfare," DCAF Horizon 2015, Working Paper No. 7, available at http://www.dcaf/content/download/67316/1025687/file/on Cyberwarfare-Schreier.pdf, p. 13.
[14] *Ibid*., p. 13.
[15] Joseph S. Nye, *Cyber Power*, Cambridge, Harvard Kennedy School, Belfer Centre for Science and International Affairs, May 2010, p. 3.
[16] Kuehl, "From Cyberspace to Cyberpower," in Kramer, Starr and Wentz (eds), *Cyberpower and National Security*, p. 38.
[17] Franklin D. Kramer, "Cyberpower and National Security," in Kramer, Starr and Wentz (eds), *Cyberpower and National Security*, p. 48.
[18] Schreier, "On Cyberwarfare," p. 18.
[19] Kuehl, "From Cyberspace to Cyberpower," in Kramer, Starr and Wentz (eds), *Cyberpower and National Security*, p. 39.
[20] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica, Rand Corporation, 2001.
[21] NATO, "Allied Joint Doctrine for Information Operations," NATO Allied Joint Publication (AJP) 3.10,23 November 2009.
[22] "Cyberwar: War in the Fifth Domain," *The Economist*, 1 July 2010, available at www.economist.com/node/16478792
[23] See Cory Bennett, "House's Defense Bill Fully Funds Cyber," *The Hill*, 15 May 2015, available at hill.com/policy/cybersecurity/242235-house-passed-defence-budget-fully- funds-cyber.
[24] "Pentagon Announces New Cyberwarfare Strategy," The New York Times, 24 April 2015.
[25] Jeremy Seth Davis, "Draft bill seeks to improve U.S. military cyber warfare capabilities," *SC Magazine*, 8 February 2016, available at www.scmagazine.com/draft-bill-seeks-to-improve-us-military-cyber- warfare-capabilities/article/471965/

About the Author

Major-General John Adams (Ret'd) joined the Canadian Army in 1960 and served until 1996. He took on many roles, from command of 1 Combat Engineer Regiment CFB Chilliwack, to Command of The Special Service Force and CFB Petawawa. John was a former Chief of the Communications Security Establishment Canada and Associate Deputy Minister of National Defence. He is a Fellow with the Canadian Global Affairs Institute.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States) or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the International Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to the Institute.