National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CANADIAN CYBER SECURITY FROM AN OFFENSIVE AND DEFENSIVE POINT OF VIEW

Lieutenant-Commander R.D. Leyte

JCSP 40	PCEMI 40
Exercise *Solo Flight*	**Exercice *Solo Flight***
Disclaimer	**Avertissement**
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.	Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 40 – PCEMI 40
2013 – 2014

CF 549 SOLO FLIGHT - 12 MAY 2014

CANADIAN CYBER SECURITY FROM AN OFFENSIVE AND DEFENSIVE POINT OF VIEW

By/Par LCdr/Capc R.D. Leyte

"This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

"La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale."

Word Count: 3295

[1] Department of National Defence, A-AP-005-000/AP-004, Leadership in the Canadian Forces: Conceptual Foundations (Ottawa: DND Canada, 2005), 50

[2] Ibid., 50

What is of supreme importance in war is to attack the enemy's strategy.

- Sun Tsu, The Art of War.

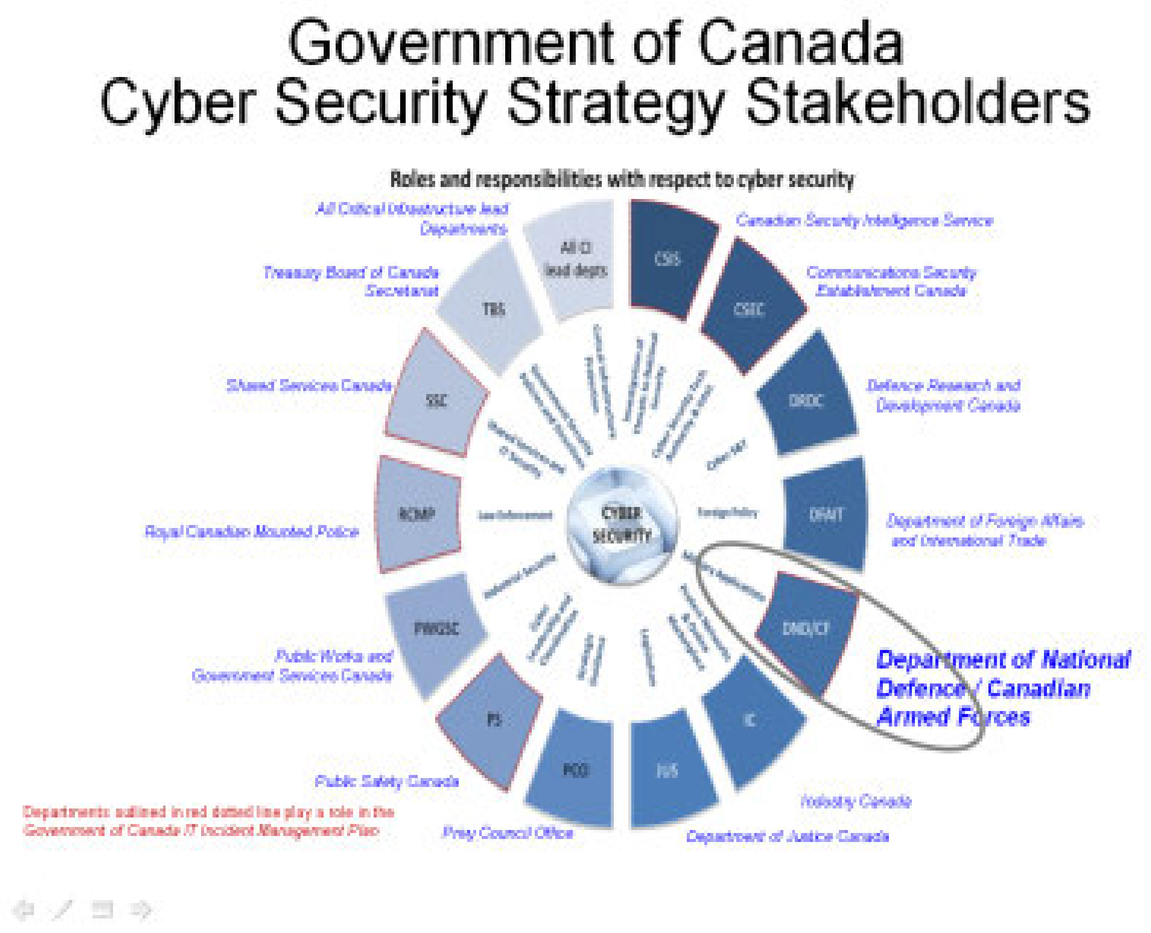
CANADIAN CYBER SECURITY FROM AN OFFENSIVE AND DEFENSIVE POINT OF VIEW

The creation of the internet has led to great advances in communications and information technology; these advances have led to an unprecedented pace of change which still proceeds today at an exponential rate. The entire world now has become reliant on communication networks and information technologies environment which has become known as Cyberspace. This cyberspace as described in Canada's Cyber Security Strategy is "the electronic world created by interconnected networks of information technology and the information on those networks."[1] The Government of Canada has assigned Public Safety Canada as the lead for cyber security and implementation of Canada's national strategy on cyber security in the cyber environment. The cyber environment is described as "the interdependent networks of information technology structures, including the internet, telecommunications networks, computer systems, embedded processors and controllers, as well as the software and data that reside within them."[2] Canada is a trading nation in a highly globalized world that relies on a market economy; Canada's prosperity and security rely on international stability, our economic success is essentially dependent on secure global communications and networks that are open and accessible to all. This paper will address Canada's approach to cyber security,

[1] Government of Canada, Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada, Canada: 2010, 2.

[2] Ron, Deibert, Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace, Calgary: Canadian Defense and Foreign Affairs Institute, 2012, 1.

in relation to our allies and discuss how Canada requires a comprehensive approach from whole-of-government (WoG) and all stakeholders to meet the cyber and internet security requirements of the future.


Government of Canada
Cyber Security Strategy Stakeholders
Roles and responsibilities with respect to cyber security
All Critical Infrastructure lead Departments
All CI lead depts
Canadian Security Intelligence Service
CSIS
Treasury Board of Canada Secretariat
TBS
Communications Security Establishment Canada
CSEC
Shared Services Canada
SSC
Defence Research and Development Canada
DRDC
Royal Canadian Mounted Police
RCMP
Law Enforcement
CYBER SECURITY
Foreign Policy
DFAIT
Department of Foreign Affairs and International Trade
Public Works and Government Services Canada
PWGSC
DND/CF
Department of National Defence / Canadian Armed Forces
Public Safety Canada
PS
PCO
JUS
IC
Industry Canada
Departments outlined in red dotted line play a role in the Government of Canada IT Incident Management Plan
Privy Council Office
Department of Justice Canada

Defining and Framing Cyber Security

Canada as a country and Canadians as a connected population are extremely dependent on cyber space for their day-to-day conduct of their lives. Government and businesses are highly reliant on the internet and advanced mobile technologies to keep the economy of Canada moving forward toward a successful future. Therefore, the importance of understanding cyber space and defining how to secure our investment in the internet is essential to maintaining a prosperous economy. Tremendous advances in innovative communications and information technology have had an extraordinary influence on how our lives are lived today and have made our culture heavily dependent on information technologies and cyber infrastructure. Our dependence is very apparent in all aspects of our lives because so much of our physical infrastructure is coordinated and controlled through cyber space as the medium in which it operates. All facets of our lives are affected, form transportation controls, energy distribution, banking and communications systems, to government organizations like national defense, treasury board and taxation; are all controlled and coordinated through computer infrastructure and information networks.

This realization that cyber space affects us all on a daily basis makes us realize that cyber security also affects the daily conduct of all of our lives. The convenience that communications networks and information technology gives us also makes Canada and Canadians susceptible to attack and vulnerable to compromise. As cyber space grows and encompasses more and more of our daily activities, so does our susceptibility to a cyber-attack. It is important to define exactly what constitutes cyber-attack, so that measures can be taken to defend against them and protect our cyber networks and communications infrastructure. Cyber attacks as defined in Canada’s Cyber Security Strategy “include unintentional and unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electric information and/or the electronic and physical infrastructure used to process, communicate and/or store that information."[3] This definition aids government agencies in assessing whether an attack has happened or is under way and correlates "the severity of the cyber-attack to determine the appropriate level of response and/or mitigation measures: i.e., cyber security."[4] In essence this is why cyber space needs to be understood and seriously contemplated utilizing a comprehensive approach not just by government and military but by private sector and business, so that all computer networks and information infrastructure remains secure from cyber-attack. It is clear that the benefits enabled by cyberspace and advanced information technology are tremendous and will continue as long as they outweigh the risks involved with cyber and information security and that all stakeholders need to better understand and manage their involvement in cyber space. In securitization of cyberspace, what needs to be realized is "the major difference between kinetic (real world) and non-kinetic (virtual world) warfare methodology is the weapons vs. the software programs they use."[5] As in the fight for the Stanley Cup or any high level competition, it has to be understood that the best defense is a good offense, so to be able to defend a team must know how to attack and how they will be attacked, to provide the best defense against attack. Cyber-attacks are increasing at an exponential rate, as we rely more and more on cyberspace as the environment to conduct both business and personal affairs. As the attackers adapt, improvise and overcome the cyber security defenses; so must the defense of our cyber environment be bolstered to deal with these attacks at every level in cyber space, such as cyber-crime, cyber espionage and cyber warfare. Government cyber

[3] Government of Canada, Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada, Canada: 2010, 3.

[4] *Ibid*., 3.

[5] Steve Winterfeld and Jason Andress. The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice, Waltham: Syngress, 2013, 3.

security initiatives, business and commercial cyber practices and policies, law enforcement and legal jurisdiction with regards to cyber law, and national defense cyber policy and procedures; all need to be coordinated and synchronized to ensure cyber space is accessible, safe and secure for Canada and all Canadians.

Information and Cyber Security Threats

There is a definite correlation to the information that we wish to protect and the types of cyber threats which threaten the security of our information technology and communications network infrastructure. The issue of information security in cyberspace is paramount to cyber security, as the security of the information that any organization or individual retains is the key factor to success and critical to effectiveness and trust in the system. Wherever and how the information is stored is relevant to its security but also to personal privacy, business opportunity, commercial in confidence, national security and to prevent risk and possible damage or destruction to computer networks and communications infrastructure. Therefore, the defining principles to information security are, "confidentiality, integrity, availability, authentication and non-repudiation (trusted assurance),"[6] and all of which apply to cyber security. These principles require strict adherence in information and cyber security, otherwise cyber threats can affect the validity of the information and its trusted utilization in the information system and cyber network, causing cyber insecurity in the Canadian populace.

Cyberspace can be exploited in a countless number of ways and methods with the use of either hardware or software; this is done by attackers exploiting vulnerabilities and

[6] SANS Institute. Information Warfare: Cyber Warfare is the Future Warfare, GIAC Repository, 2004, 5.

faults within the computer, the network and/or the programming software (the code). The Canadian Cyber Security Strategy identifies that cyber-crimes are the majority of the cyber threats for three main reasons; “the increasing number of users…are creating a growing baseline of potential targets,”[7] the unprecedented expansion in “the ways in which we communicate and share information online,”[8] and the fact that cyber-crimes are “rarely disclosed to the public,”[9] which leads to a false sense of information security. In the Strategy, it correlates the increase in cyber-attacks to four main factors; “inexpensive attack tools, which are easy to use (basic skills can cause significant damage), effective (minor attacks can cause extensive damage), and of low risk (attackers can evade detection and prosecution).”[10] Presently, cyber-crimes are mostly economic based attacks because cyber-crime pays, but the hackers training, techniques and procedures (TTPs) can be exploited to conduct cyber-crime, cyber-espionage and cyber warfare.

The evolution of the cyber threat is expanding the types of cyber-attacks that can be anticipated, and each one is unique in their rationale and objectives, in accordance with the *Strategy* they are categorized into three groups, “state sponsored cyber espionage and military activities, terrorist use of the internet and cyber-crime.” [11] Cyber security is undergoing a paradigm shift that will be adaptable and varying in its context that will not be from one single structured approach and will need to be dealt with both defensively and offensively by utilizing cyber strategic, tactical measures and counter-measures at all levels. The challenges to cyber security are numerous and related to the iniquitousness of

[7] Ron, Deibert, Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace, Calgary: Canadian Defense and Foreign Affairs Institute, 2012, 11.

[8] *Ibid*., 11.

[9] *Ibid*., 12.

[10] Government of Canada, Canada’s Cyber Security Strategy: For a Stronger and More Prosperous Canada, Canada: 2010, 5.

[11] *Ibid*., 5.

cyberspace, in which there are no boundaries in the physical realm, no direct contact or line to cross or physical presence required which makes detection difficult and at times impossible. This makes computer and network systems security fundamental in the cyber security realm.

The Plan and Future Focus

To combat the cyber threat, the Canadian government has constructed a plan to meet the challenges of securing Canadian interests and protecting them from future cyber threats. The plan is based on Canada's Cyber Security Strategy 2010 which has been built on three fundamental principles for cyber security which are "securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online."[12] These principles are to ensure that the Canadian government endeavors to persevere and maintain the trust of the Canadian populace in their ability to secure information and services while defending our national interests and protecting national security in cyberspace. Also, the principles enables government at all levels and the private sector to work together to reinforce critical cyber infrastructure and information communications systems and to enhance cyber security through government sponsored initiatives and related programs. Furthermore, governmental cyber security information dissemination will provide Canadian cyberspace and internet users the protection required to combat cyber threats and enable a legal framework to have cybercrime dealt with accordingly. Although the fact that Canada finally has a strategy that will enhance the government's ability to react to cybercrime in

[12] *Ibid*., 7.

the cyberspace realm, it is still not a panacea to protect Canadians against all cyber threats.

Canada as part of the greater cyber global community will require international cooperation and partnership in alliances in order to ensure that cyberspace security can be a trusted environment and that Canada is viewed as a trusted cyber global partner. Canada's leading economic and security partners, the United States, The United Kingdom, and Australia have all published their own strategies for the securitization of cyberspace and highlighted the importance of international collaboration to effect a safe and secure cyber environment. Their strategies are similar in context and content to ours, reflecting similar principles, priorities, policies and procedures.

The US Department of Defence (DoD) Strategy for Operating in Cyberspace (2011) states that, "DoD will employ an active cyber defense capability to prevent intrusions onto networks and systems,…DoD will operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on networks."[13] Similarly, in the United Kingdom in September 2013, the Secretary of State for Defence publically acknowledged that the UK is developing an offensive cyber capability to "strike back in cyberspace against enemies who attack us."[14] The Ministry of Defence (MoD) is creating a Joint Cyber Reserve Unit that will conduct operations in cyberspace for both defensive and offensive purposes. The UK's updated Cyber Security Strategy (2011) indicates that the MoD's Defence Cyber Operations Group (DCOG) will include a Joint Cyber Unit (hosted by GCHQ), that will "develop new tactics, techniques and plans

[13] US Government, The Comprehensive National Cybersecurity Initiative, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

[14] Government of Canada, Director General Cyber, Sharepoint web site, Ally engagement.

to deliver military effects through operations in cyberspace."[15] The MoD has recently stood up a new Global Operations and Security Control Centre to focus on cyber defence for the armed forces. A second Joint Cyber Unit embedded at this centre will "develop and use a range of new techniques, including proactive measures, to disrupt threats to our information security."[16] Australia in stride in January 2013, as part of its National Security Strategy, announced that an Australian Cyber Security Centre would be created and would develop "sophisticated capabilities to maximise Australia's strategic capacity and reach in cyberspace, giving the Government the ability to detect, deter and deny offshore malicious cyber actors targeting Australia."[17] All of our four strategies are complimentary with regards to cyber security and strengthens our shared goal to enhance global cyber security, but to ensure continued freedom of movement in cyberspace these strategies must be continually updated to maintain pace with evolving cyber threats.

Also, Canada will need to further its international cyber security interests by enhancing cyberspace relationship building with our key strategic alliances like, NATO, the UN, and the G8. Canada is a signatory of the "Council of Europe's Convention on Cybercrime and is preparing legislation to permit ratification of this treaty."[18] This and other similar initiatives with our international and economic global partners will assist in building an international cyber security legal framework that will provide governance and an increased layered cyber defense. Canadian government, including the Department of National Defence (DND) and Communications Security Establishment Canada (CSEC), working in conjunction with NATO and our key allies in the Five Eyes (ABCANZ)

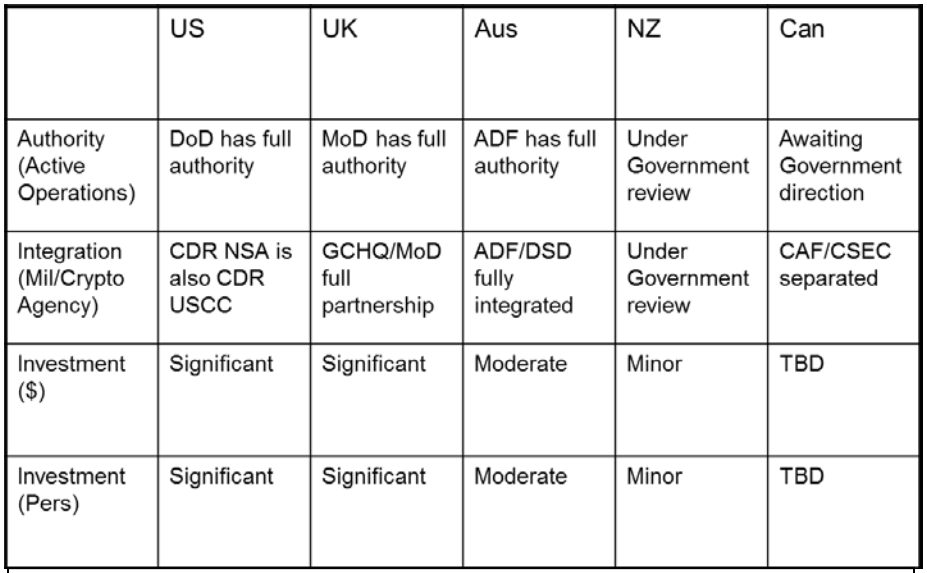
[15] *Ibid.*

[16] *Ibid.*

[17] *Ibid.*

[18] Government of Canada, Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada, Canada: 2010, 8.

partnership give Canada access to shared intelligence, the ability track and trace cyber threats, and challenge cyber technological challenges; that would not be available otherwise nor would it be financially feasible to develop this capability by ourselves.



	US	UK	Aus	NZ	Can
Authority (Active Operations)	DoD has full authority	MoD has full authority	ADF has full authority	Under Government review	Awaiting Government direction
Integration (Mil/Crypto Agency)	CDR NSA is also CDR USCC	GCHQ/MoD full partnership	ADF/DSD fully integrated	Under Government review	CAF/CSEC separated
Investment ($)	Significant	Significant	Moderate	Minor	TBD
Investment (Pers)	Significant	Significant	Moderate	Minor	TBD

ABCANZ – key ally engagement in cyber security from DG Cyber website.

Globally, the laws and obligations that govern cyberspace and the cyber interactions of state and non-states are still in flux and presently lack legal legitimacy. Therefore, the Canadian Government is entrusted with securing the Canadian cyber environment and providing protection of our information and the systems that contain it. To achieve the cyber integrity for the Canadian government, public and private sector clear roles, responsibilities and duties need to be assigned and delineated. As Public Safety Canada has the lead, they have defined which agencies develop, hold and deliver the services and capabilities required for the securitization of cyberspace, utilizing a comprehensive approach for the implementation of the strategy, leveraging government and all stakeholders' abilities to implement the tenets of the security strategy. The key government departments that are directly involved and have inherent capabilities to affect the securitization of cyberspace are Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), the Treasury Board Secretariat (TBS), Department of Foreign Affairs and International Trade (DFAIT), Department of National Defence (DND), and the Communications Security Establishment (CSEC). Most important in the offensive and defensive capabilities to be provided in the relationships between these organizations and how they interact to provide mutual beneficial support to each other, in particular the relationship between CSEC and DND.

DND role as stated by BGen Loos (2012 Director General Cyber) and in accordance with the Cyber Security Strategy is clear in that they are "responsible to protect DND information and networks and to contribute to WoG effort in characterizing the threat and sharing information on what is going on in the cyber environment."[19] Their role is complementary to CSEC cyberspace mandate, on which the relationship is being built and further strengthened for future operations. CSEC mandate as stated by John Forster, Chief CSEC, to the Standing Senate Committee on National Security and Defence, is a three part mission, "to collect foreign signals intelligence, to provide advice, guidance and services to protect electronic information and information infrastructure, and provide technical and operational assistance to federal law enforcement and security partners."[20] This relationship is similar to the US construct where Cyber Command encompasses National Security Agency (NSA) and DoD capabilities to address cyber security and cyber warfare issues for the US government but

[19] Parliament of Canada, Proceedings of the Standing Senate Committee on National Security and Defence; Issue 10 - Evidence - Meeting of November 5, 2012. 3.

[20] *Ibid.*, 8.

has not been formally instituted into government policy as seen with our America counter-parts. Ultimately, both systems are meant to strengthen cyber security of governmental regulated cyber systems and infrastructure, enhance cyber security awareness and deconstruct barriers to information distribution and cooperation between government departments and trusted global partners.

Canadian Cyber Security Way Ahead

Canada and the entire world have grown to become thoroughly dependant on the utilization of cyberspace, advanced communications technologies and information communications infrastructure. Although the 2010 Canadian Cyber Strategy was the first real step in the plan to securitization of cyberspace by defining an architecture for the framework to be placed and identifying Canada's first principles in regards to determining the way ahead, much work still needs to be done to ensure continued success into the future of cyber security. Cyber security itself needs to be an educational process for all Canadians who utilize cyberspace, as the strategy applies to everyone who uses the benefits of cyberspace in their day to day conduct of their lives, therefore cyber security will require a combined effort of government, public and private sector to achieve implementation of the principles.

For Canada a comprehensive approach to cyber security is required by all stakeholders, all Canadians, with a whole-of-government implementation process to ensure that cyberspace is an open and available resource for all to utilize. The Chief of CSEC stated this at the 2013 GTEC on *Cyber Security and Government of Canada*, in his closing remarks, “It is a team sport — it will take all of us, IT practitioners in government and industry, working together to ensure we can safely have an agile government, that is open, collaborative mobile – and relatively secure!"[21]

[21] CSE's Chief John Forster delivered a keynote address at GTEC 2013, entitled Cyber Security and the Government of Canada. http://www.cse-cst.gc.ca/gtec/speech-2013-10-09-eng html

Bibliography

Books

Burns, Nicholas, and Jonathon Price. Securing Cyberspace: A New Domain for National Security, Washington: The Aspen Institute, 2012.

Demchak, Chris C. Wars of Disruption and Resilience: Cybered Conflict. Power, and National Security, Athens: University of Georgia Press, 2011.

Harrison Dinniss, Heather. Cyber Warfare and the Laws of War, New York: Cambridge University Press, 2012.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. Cyberpower and National Security, Washington: National Defense University Press, 2009.

Libicki, Martin C. Crisis and Escalation in Cyberspace, Santa Monica: RAND Corporation, 2012.

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

Articles

Canada, Government of. Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada, Canada: 2010.

Canada, Government of. CSE's Chief John Forster delivered a keynote address at GTEC 2013, entitled Cyber Security and the Government of Canada. http://www.cse-cst.gc.ca/gtec/speech-2013-10-09-eng.html

Canada, Parliament of. Proceedings of the Standing Senate Committee on National Security and Defence; Issue 10 - Evidence - Meeting of November 5, 2012. http://www.parl.gc.ca/content/sen/committee/411%5CSECD/10EV-49784-e.HTM

Deibert, Ron. Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace, Calgary: Canadian Defense and Foreign Affairs Institute, 2012.

Government, US., The Comprehensive National Cybersecurity Initiative, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Gray, Colin S. Making Strategic Sense of Cyber Power: Why the Sky is Not Falling, Carlisle Barracks: US Army War College Press, 2013.

SANS Institute. Information Warfare: Cyber Warfare is the Future Warfare, GIAC Repository, 2004.

Web

Canada, Government of., Director General Cyber, Sharepoint web site, Ally engagement