National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER DETERRENCE: IMPLICATION FOR CANADA AND ITS ALLIES

Maj Alfred Lai

JCSP 43 DL

Exercise *Solo Flight*

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 43 AD

Exercice *Solo Flight*

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 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CYBER DETERRENCE: IMPLICATION FOR CANADA AND ITS ALLIES

Maj Alfred Lai

Word Count: 3026

Compte de mots: 3026

CYBER DETERRENCE: IMPLICATION FOR CANADA AND ITS ALLIES

Introduction

With an estimated 63.01 Internet users per 100 inhabitants, Canada ranks the 9th most connected countries in the world.[1] As a major economic power, a member of G7, much of Canada's day to day activities including economic and military operations are heavily dependent on the Internet and other communications based on the same physical computer network systems. The Internet was not designed with security in mind at the beginning, rapid development over the last several decades have increased and compounded security vulnerabilities. This leaves Canada being exposed to a great number of Cyber threats from different vectors pursuing their political, military and criminal ends. These include nation states, the so called rogue states, non-state entities as well as individuals. As part of defending Canada and ensuring security for Canadians against these threat vectors the concept of "Cyber Deterrence", preventing Cyber-attacks before they materialized, has attracted much attention. The Cyberspace and its constituent technologies have the inherent characteristics of due use nature. Cyber threats against Canada consist of a spectrum of vectors that straddles the military and non-military nature and at times a combination of both to different degrees. To deter against such threats, Canada requires a comprehensive Cyber deterrence strategy.

This paper argues that traditional military deterrence concepts are inadequate for Cyber deterrence. In order to deter against a spectrum of Cyber threats Canada, as a medium power but

[1] Canadian Journal of Communication http://www.cjc-online.ca/index.php/journal/article/view/1656/1794

with vast amount of assets to protect, must adopt a holistic integrated Cyber deterrence strategy. Canada should adopt a "Whole-of-Nation" form of the "Active Cyber Defence" concept as a foundation. Based on this foundation, different deterrence postures should be tailored toward specific category of threats. On the international political and military levels, Canada should act in conjunction with allies to deter potential adversaries. Similarly, at the domestic level, to deter criminal, terrorist and miscreant activities in the Cyber Domain, through law and order agencies , and education of the public in order to safeguard Canada's defence and security.

Cyber Security Strategy

Under the current Canada's *Cyber Security Strategy*[2] , the Government of Canada has identified seven government departments and agencies that have key roles in Cyber security. These are 1) Public Safety Canada (PSC) that leads the coordination in the efforts to protect critical infrastructures; 2) Shared Services Canada (SSC) provides and protects government information infrastructures; 3) Canadian Security Intelligence Service (CSIS) collects information, assesses threats, produce intelligence and advises the government of the threats to the security of Canada; 4) Communications Security Establishment (CSE) provides foreign signals intelligence from the global information infrastructure; 5) Royal Canadian Mounted Police (RCMP) conducts and coordinates criminal intelligence, crime prevention and investigation of Cybercrimes; 6) Canadian Radio-television and Telecommunication Commission (CRTC) whose mandate include enforcement of legal compliance of Cyber

[2] Government of Canada, "*Canada's Cyber Security Strategy - For a stronger and more prosperous Canada*", © Her Majesty the Queen in Right of Canada, 2010, ISBN: 978-1-100-16934-7

technologies; and 7) Department of national Defence/ Canadian Armed Forces (DND/CAF) with mandate to conduct GoC authorized military missions in the Cyber Domain and contribute to joint security efforts with allied military organizations. Note that this "Whole-of-Government" construct is protective in nature and does not presence a clear deterrence posture. Provincial, local authorities, private sector entities and individual citizens contribute to the collective Cyber security of Canada by protecting their own perimeters.

The Cyber Domain and Cyberspace

The Canadian Armed Forces (CAF) is the only CoG department that has the mandate to conduct military actions on behalf of Canada. It has defined Cyber Space as the 5th war fighting domain[3]. CAF Doctrine[4] proposes that the "Cyber Domain" represents all factors that influence operations in "Cyber Space". These include human users and users groups, infrastructures and all activities relating to and affecting "Cyber Space" similar to the Maritime, Land, Air and Space Domains[5] where the CAF operates. On the other hand, "Cyber Space" represents an element of the "Cyber Domain" as the medium in or through which Cyber operations are conducted, analogues to the ocean, land, air and space. This medium, however, is entirely created by human – an artificial terrain. The "Cyber Space" consists of interdependent systems of networks built on information technology (IT) structures including the Internet, public and proprietary computer

[3] CAF Chief of Forces Development, "Integrated Capstone Concept" 20 October, 2009 P. 28

[4] Government of Canada, "*Canadian Armed Forces Joint Doctrine Note, Cyber Operations*", JDN 2017-02, Joint Doctrine Branch, Canadian Forces Warfare Centre, © Her Majesty the Queen in Right of Canada, 2010

networks, telecommunication networks, computer systems, embedded processor and controllers as well as the data created, resided and transmitted within[6].

Characteristics of Cyberspace

The Cyberspace is shared by actors whose utilize it for all form of activities that both benefits and detrimental to society. To promote beneficial use of Cyberspace and to prevent its use as a platform for nefarious purposes such as conducting "cyber-attacks" for various purposes, users must be informed of and understood the consequences of misuse of this domain – hence the necessity of Cyber Deterrence. The Cyber Domain has a set of characteristics that presents unique challenges which have direct impact on implementing traditional concept of deterrence. These attributes includes,

1. The Cyber Domain is both pervasive and transnational without respect for national borders. It enables both global and local operations. Physical distance has no impact in Cyber operations.
2. Operation in the Cyber Domain can produce asymmetric effects. It is offensive biased; the Cyber Domain favours the attacker then the defender. Small actors with access to the appropriate technologies and skills set can act against much larger adversaries or entities. Equally, with a small amount of investment nation states can act against near peer adversaries achieving effects out of all proportion. The Cyber Domain harbours a large array of potential adversaries to deter against.

---

[5] Ibid P.2-1
[6] Ibid

3. The technologies that aggregate to form the Cyber Domain provide Cyber actors with easy anonymity, and thus provide deniability; that makes attribution of responsibility almost impossible. When deterrence fails, it is difficult to prove and act against perpetrators.
4. The effects of Cyber activities can be instantaneous and affecting multiple locations. On the other hand, time taken to investigate and to identify origins of offensive operations can be lengthy. Equally, the time and efforts required gathering intelligence, weapon development and readiness for offensive operations also takes time. The immediacy of retaliation as deterrence is reduced.
5. Cyber weapons are versatile. Cyber operations can be used across a full range and phases of military operations. From exerting influence to certain types of destructive actions within in or external to the Cyber Domain are possible. Similarly,
6. The Cyber Domain is highly connected and complex, Cyber operations can cause unintentional cascading effects. The complexity renders the second and third order effects unpredictable and creation of collateral damages highly likely.
7. With it trans-border nature, dual military and civilian use of the constituent technologies and able to achieving certain military effects without the application of kinetic combat military power, the Cyber Domain contains a lot of legal gray areas in term of the application of international law and the Law of Armed Conflict (LOAC).
8. Most importantly, the Cyber Domain as a warfighting domain cannot delivery decisive military actions. Cyber operations have proven to be able to excerpt influence, provide a mean for reconnaissance and espionage for information gathering, disruption of communications and civic functions and provided certain destructive effects. However, Cyber operations will always serve as an enabler for kinetic military operations. Only the application of physical combat power can destroy the adversaries and occupancy their territories in order to forces one's will for a desirable end-state.

Theory of Deterrence

In order to create credible deterrence against Cyber threat vectors against Canada, a clear understanding what constitutes deterrence is required. Effective deterrence stems from the cognitive level of the adversary's belief that the costs out weights the benefit of action[7]. To instill this belief, a deterrence strategy must be have the capability – the means to influence behaviour; credibility – instilling believability; and communication - of the right message[8]. Traditional deterrence exists in three forms, 1) deterrence by retaliation; 2) deterrence by denial; and 3) deterrence by entanglement[9]. These three traditional deterrence options could conceivably apply to some extend in the Cyber Domain. However, due to the characteristics of the Cyber Domain as discussed above, no single option could provide a complete solution.

The first option, deterrence by retaliation, requires timely and accurate information to identify the perpetrator responsible. If attribution if possible, the nature and scale of retaliation, by Cyber and/or other means, will need to be proportional. Current technology developments have not yet able to achieve retaliations by pure Cyber means with such accuracy without creating collateral damages thus lack the capacity for effective deterrence. The second option of deterrence by denial where majority of current defensive postures adopted by the public and private sector as well as individuals depends on perimeter defences. Such postures are routinely defeated by intruders lacking both capability and credibility for effective deterrence. The third option of deterrence by entangle based upon the high connectivity and complexity in the Cyber Domain. It applies mainly to strategic level inter-state adversarial Cyber contentions based on the

---

[7] Jasper S. "*Strategic Cyber Deterrence – The Active Cyber Defence Option*", Rowman & Littlefield, Maryland 2017 P.9

[8] Ibid P. 209

[9] Ibid P. 13

assumption that second and third order effects of any Cyber action might backfire on the perpetrator. This option is less effective against perpetrator states that are low on Cyber connectivity and ineffective against small non-state actors or individuals. This lack of credibility to instill believability and a clear mean to communicate the possible consequence of a Cyber-attack makes this option ineffective as a deterrence.

Threat Landscape of Canada

According to *Cyber Security Strategy,* the threat landscape of Canada can be described in three broad categories, 1) State sponsored Cyber espionage and military activities – well resources and persistent threat to gain political, economic, commercial and military advantages. They are typically designed to sabotage infrastructures, communications, illegally obtain data and information. In wartime to support kinetic military operations; 2) Terrorist use of the Internet – primarily use to support recruitment, fund raising, and propaganda purposes. Though less capable then their state sponsored counterpart, it is increasing likely that terrorist group are developing the capabilities to conduct Cyber operations; and 3) Cybercrime – organized crime increasingly purse traditional crime a few examples include identity theft, money laundering and extortion[10].

These three broad categories are not clearly demarcated. More often, threats are consisted of overlapping elements from these categories forming a spectrum of different threat vectors. For example, state sponsored terrorist activities may employ criminal "Hacking-as-a-Service" to

[10] Reference 2 P.5

conduct Cyber operations in order to maintain deniability. Furthermore, due to the asymmetric characterises of the Cyber Domain, Hacktivists as well as individuals also post significant threats that need to be countered. In order for Cyber Deterrence is to be effective, it has to be specifically tailored according to each type of threat vectors.

In order to provide tailored Cyber Deterrence against a spectrum of threat vectors, each type of threat vector need to be categorized. In most public discourses, the term "cyber-attack" is applied to any adversarial actions conducted within the Cyber Domain. The spectrum of activities described as cyber-attacks ranges from defacing and altering of web-pages for propaganda, installation of spyware on personal computers to steal passwords and other personal data, denial of service (DoS), massive data breaches for ransom, state espionage activities to sabotage through Cyber operations that caused physical damages. These adversarial actions can be carried out by non-state actors such as a single hacker, hacktivists promoting a cause, criminal groups for financial gains, terrorist organizations, as well as by nation states. Often nation states level common espionage conducted against each other through the Cyber Domain are often described as "Cyber Warfare" and when discovered such action are described as a "Cyber-attack". However, an attack has a specific meaning in terms of LOAC[11]. Currently, there is no clear defined threshold indicating where a disruptive (offensive) Cyber operation against a state has risen to the level of an armed attacked – an act of war. Recent attempts have tried to correct this confusion by defining Cyber-attacks, Cyber espionages and other unauthorized entry for illegal purposes through operations in the Cyber Domain. Such clear definition would help to formulate appropriate deterrence posture without undue escalation.

---

[11] Reference 4 P. 3-8

An Alternative Strategy

From the above analysis, it is clear the traditional deterrence strategies are inadequate in providing the necessary tailored deterrence effects when facing the contemporary Cyber Threat spectrum. A viable alternative deterrence strategy may be found in adopting the "Active Cyber Defence" concept for the Canadian situation. Active Cyber Defense (ACD) is defined as "an organization's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities within their cyber defense ecosystem".[12] Since static perimeter defences such as hardening networks and systems through preventive control are no longer effective, ACD combines internal systemic resilience to defeat malicious Cyber activities after a network intrusion and tailored disruption capacity to repulse the intruder. Based on an integrated and automated common framework, ACD deploys reactive activities to stop or limit damage through detective controls and remedial actions. The reactive activities employed in ACD are based on three active defence concepts: detection, deception and termination, through automated means. Through the use of artificial intelligence (AI), systems supporting the ACD strategy are about to react to any intrusion in Cyberspace relevant timeframe. The ACD strategy encourage adversary's restraint by shaping perception of the costs and the benefits of any given Cyber-attack in a scale large enough to deter multiple malicious actors of different nature.

Effectiveness of the ACD strategy can be seen by the result published by Dr. Ian Levy, Technical Director of the United Kingdom's (U.K.) National Cyber Security Centre (NCSC)[13]. In 2016, the Government of the U.K. launched the new National Cyber Security Strategy. A part

---

[12] Denning D.E. & Strewser B.J. "*Active Cyber Defense: Applying Air Defense to the Cyber Domain*" http://carnegieendowment.org/2017/10/16/active-cyber-defense-applying-air-defense-to-cyber-domain-pub-73416

[13] Dr. Levy I. "*Active Cyber Defence – One Year On*", UK National Cyber Security Centre, 5th February, 2108 https://www.ncsc.gov.uk/information/active-cyber-defence-one-year

of this strategy is to set up the NCSC as part of Government Communication Head Quarter (GCHQ) with a mandate to purse the radical actions required to better protect their U.K.'s interests in Cyberspace. A key strand in this new approach is the NCSC's ACD programme. The ACD programme's intend is to tackle the high-volume commodity attacks that affect people's everyday lives, rather than the highly sophisticated and targeted attacks. The reported named *Active Cyber Defence - One Year On*, categorize a series of successes achieved in the year since the deployment of the ACD strategy. For example, in 2017, 121,479 unique phishing sites across 20,763 attack groups physically hosted in the UK were taken down[14]. As a consequence, the median availability of a phishing site physically hosted in the UK reduced from 26 hours to 3 hours, again giving them much less time to do harm. 76.8% of those were down in 24 hours, up from 47.3% before we started takedowns. Over the year 2017, the month-by-month volume of each of compromised website has fallen, suggesting that criminals hosting fewer of their malicious sites in UK infrastructure. The ACD strategy made conducting malicious activities in Cyberspace based in the U.K., in this case Cyber Crime, unprofitable and risky. The Cyber criminals understood the message that the costs out weights the benefit generated by their malicious actions. They ceased their operations; the ACD strategy thus achieved the desired deterrent effect. The U.K. results demonstrated the ACD strategy meets capacity, credibility and communication requirements to be selected as an option to achieve deterrence within the Cyber Domain.

Albeit applied against commodity Cybercrime level within the national boundary of the U.K., the ADC strategy can equally be deployed against non-state actors and terrorist use of the

---

[14] Ibid P. 1

Internet. The parameters and limitations of the ADC strategy have yet to be fully explored. The technologies, technique, tactics and procedure can be scale up to provide deterrence against state sponsored Cyber espionage and military activities. However, due to the characteristic of the Cyber Domain, further research in the direction of legality within the international legal framework and the ethics of extra-boundary and trans-boundary long distance deployment of the ADC strategy is required.

In the Canadian context, an alternative Cyber Deterrence strategy should developed by adopting the ACD strategy as the foundation. A trusted information sharing (TIS) framework should be constructed for the seven GoC departments and agencies that have key roles in Cyber security to share situation awareness and Cyber threat information collected under each of their respective mandates in Cyber relevant timeframe in order to apply appropriate and effective countermeasures. Building upon this foundation, Cyber Deterrence based on the ACD strategy could be made more robust by expanding into a "Whole-of-Nation" effort. The TIS framework should be expanded to include other GoC departments, provincial and territorial governments, major municipal governments and law enforcement agencies, as well as critical industries in the private sector on a "need-to-share" basis. As evident from the successes of the U.K. model, a Canadian "whole-of-Nation" effort could scale up and provide similar successes within Canada in providing Cyber Deterrence against commodity Cybercrime, non-state actors, and terrorist as well as Hacktivists and individuals that post Cyber threat within Canada.

At the international political and strategic military level, the ACD strategy scaled up from the domestic foundation could provide Canada a credible Cyber Deterrence against state sponsored Cyber espionage and military activities. Working with allies with different Cyber

Security posture in peace time could expose Canada to the possibility of becoming collateral victim in conflicts that Canada is not involved in. However, in war time working closely with allies would enhance the effectiveness of Cyber Deterrence within the context of collective defence. Nevertheless, working closely with like-minded allies would benefit Canada through ex-change of ideas, coordinating research and development, sharing of experience as well as sharing technologies, tactics, technique and procedures. Indeed, the report *Active Cyber Defence - One Year On*, published by NCDC actively encourage foreign government collaboration.

Conclusion

The Cyber Domain, the 5th warfighting domain and its constituent part the Cyberspace is a new environment. Unlike other domains of war it is an entirely artificial environment and is still evolving. Due to the characteristics of the Cyber Domain, traditional theories of deterrence based on are not adequate. An alternative viable form of deterrence is found in the Active Cyber Defence strategy.

Canada being a highly connected country with a vast amount of assets to protect must build upon Active Cyber Deterrence strategy as a foundation to secure its interest. This strategy has proven to be successful and could be scale up for deployment within Canada in "Whole-of-Country" approach incorporating different levels of government as well as the private sector. Canada must also collaborate closely with allied counties to form a credible Cyber Deterrence in the context of collective defence.

Bibliography

CAF Chief of Forces Development, "*Integrated Capstone Concept*" 20 October, 2009

D Cyber FD, CAF Joint Publication JDN 2017-02 Promulgated Draft, "*Cyber Operations*", 2017

Jasper S. "*Strategic Cyber Deterrence – The Active Cyber Defence Option*", Rowman & Littlefield, Maryland 2017

HQ, Department of the Army, FM 3-38, "*Cyber Electromagnetic Activities*", February 2014

Mandiant Report APT1, "*Exposing One of China's Cyber Espionage Unit*", 2013

Blackwell, James. "Deterrence at the Operational Level of War." *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 30-52.

Freedman, Lawrence. "The meaning of deterrence." In *Deterrence*. Cambridge: Polity Press, 2004. P: 26-42.

Carr J, "*Inside Cyber Warfare*" 2nd Edition , O Reilly, 2014

DOD, Defense Science Board, "*Task Force on Cyber Deterrence*", February 2017

Wilson R. "*Sun Tzu and the Art of Cyber War*", Defense AT&L. January-February 2018

Lai A.C.W. Maj, "*Rules of Engagement of Military Cyber Operation in International Legal Framework*", M.Sc. Dissertation, 2014.

Ghionis A.A., "The Limits of Deterrence by Punishment", University of Sussex

Hua J & Bapna S., "How Can We Deter Cyber Terrorism?", Information Security Journal: A Global Perspective, 21: 102-114, 2012