National Defence | Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

A CYBER STRATEGY BASED ON COUNTERINSURGENCY PRINCIPLES

Maj G.B. Parisien

JCSP 42

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 42

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 42 – PCEMI 42
2015 – 2016

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

A CYBER STRATEGY BASED ON COUNTERINSURGENCY PRINCIPLES

Maj G.B. Parisien

Word Count: 3299

Compte de mots: 3299

A Cyber Strategy Based on Counterinsurgency Principles

Introduction

As the cyber environment continues to evolve and develop and our understanding of this environment matures it is evident that our society is reliant on the services that are dependent upon an available and reliable cyber environment. It is also increasingly apparent that there exists significant opportunity for criminal and malicious activity that can cause great harm to a nation that is reliant on this environment. Canada, like most advanced nations has spent considerable resource to include a cybersecurity component to their national security policy. In these efforts Canada has developed a cyber-strategy focused on defending Canadians and Canadian interests within this contested space. However, in the development of this strategy little consideration was placed on the nature of the threat vectors and lessons we have learned from similar experiences in the past. This paper will argue that the most common threat vector within the cyber environment displays characteristics of a classical insurgent force and that a cyber-strategy based on counterinsurgency principles needs to be adopted in order to effectively deal with these threats. This paper will be divided into two main sections, the first section will discuss Canada's current cyber strategy and its development as well as discussing the current threat vectors in the cyber environment and the second section will demonstrate how a cyber-policy based on counterinsurgency principles can address the threat vectors identified.

Canada's Cyber Strategy and Threat Vectors

In 2004 the government of Canada produced a national security policy, this policy centred on three interests: protect Canada and Canadians at home and abroad, ensuring Canada is

not a base for threats to our allies and contributing to international security.[1] In the area of cyber emergency planning and management this policy committed to the development of two key initiatives. The first indicates "the Government will increase its capacity to predict and prevent cyber-security attacks against its networks"[2] indicating a required increase in intelligence gathering and sharing with likeminded nations as well as the development of a cyber-incident response capability. The second indicates "a national task force, with public and private representation, will be established to develop a National Cybersecurity Strategy"[3] indicating that a consolidated whole of government approach will be used to protect Canadian interests against cyber threats. In 2010 the government released Canada's Cyber Security Strategy. This strategy is centred on three pillars: securing government systems, partnering to secure vital cyber systems outside the federal government and helping Canadians to be secure online.[4] This policy identifies that the RCMP will coordinate with the Canadian Cyber Incident Response Centre through the establishment of a Cyber Crime Fusion Centre in a law enforcement capacity. While this policy does address the need to educate Canadians on how to be safe while navigating the cyber environment and outline privacy laws, it does little to address how they intend to contain non-state actors that utilise the cyber environment within Canada or the internal threat of cyber. This policy while a good start in creating an atmosphere of understanding the importance to take action within the Cyber environment and sets a groundwork for "defensive measures" it does not layout the role that the Canadian Armed Forces is to play in the Cyber environment nor does is lay the groundwork for how Canada intends to shape the cyber environment in Canada.

---

[1] Canada. Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Privy Council Office,[2004]).
[2] Ibid, xi.
[3] Ibid, xi.
[4] Canada. Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: Govt. of Canada,[2010]).

An examination of the threat vectors within the cyber environment reveals that the most frequent source of threat comes from non-state actors rather than foreign governments. To be clear this is not to say that state sponsored cyber action is not a threat but rather to suggest that they are not currently the only or even the greatest threat. Given the low cost of entry into waging war within the cyber environment and the relative anonymity, the use of the cyber domain affords an attractive option to non-state actors that would otherwise not be able to compete in a conventional way. Gabriella Coleman in her book, *Hacker, Hoaxer, Whistleblower, Spy: the Many Faces of Anonymous,* gives an in-depth overview of Anonymous as an organisation, she describes the organisation as one with little formal structure that is vastly complex. So complex in fact that she describes it as "an infinite machine operating a tight recursive loop wherein mazes generated maze generating mazes."[5] Anonymous is but the most widely publicised network of actors within the cyber environment but serve as a useful target for analysis for the purpose of this paper and displays typical characteristics of the most common threat vectors. Parmy Olson, in her book *We are Anonymous,* describes the organisation as a global cyber insurgency "hell-bent on attacking enemies of free information".[6] Brian Kelly in his article, *Investing in a centralized cybersecurity infrastructure: why "hacktivism" can and should influence cybersecurity reform*, supports the notion that Anonymous has "a very loose and decentralized command structure that operates on ideas rather than directives."[7] Similar descriptions have been used to describe the structure of the Taliban insurgency in Afghanistan and ISIS in Iraq. John Mills asserts in his paper, *Counterinsurgency in Cyberspace,* that:

---

[5] Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (New York: Verso, 2014), 9.
[6] Parmy Olson, *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (New York, NY: Little, Brown and Co, 2012), 3.
[7] Brian B. Kelly, "Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" can and should Influence Cybersecurity Reform," *Boston University Law Review* 92, no. 5 (2012), 1678.

> these threat vectors cannot be dealt with through conventional means. A creative counterinsurgency strategy and mindset must be followed to deter and eliminate these insidious elements. Successful tenets of counterinsurgency must be updated and applied in the world of cyber.[8]

To date Canada has determined to accept that cyber is a new environment within which it must operate much like the Air, Sea and Land environments, yet it has only developed strategy for conventional defence to this point. If as articulated above there exist actors within this environment who do not conform to conventional actions that are not susceptible to conventional strategies then an unconventional strategy needs to be applied. It has been argued that the most common threat vector displays principles akin to insurgent forces; as such one can take lessons from counterinsurgency strategies and apply them within the cyber environment. The next section will discuss some of the counterinsurgency principles that can be applied to these threat vectors in a cyber-environment.

Counterinsurgency Principles Applied to a Cyber Strategy

Debate exists over whether the cyber environment can truly be classified as a domain like the land, sea and air environments, A paper written by Dr. Mitchell and LCol McGuffin lays out this debate rather succinctly; it focuses is on the lack of dimensional aspect in the cyber environment which for the discussion in this paper is irrelevant. Mitchell and McGuffin's paper does concede that "force and influence can be projected through Cyberspace"[9] it is this notion that allows us to discuss how to influence the actors within the cyber environment. John Mills lays out a four pillar cyber strategy that considers tenants of counterinsurgency, it consists of: inducing the cyber insurgents to turn on themselves, creating a unified, total-government action in cyberspace, establishing cyber hygiene and establishing a cyber-counterinsurgency training

[8] John R. Mills, "Counterinsurgency in Cyberspace," *Georgetown Journal of International Affairs* (2011), 158.
[9] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal* 69, no. 3 (2014), 411.

and technology pipeline.[10] In an effort to expand upon these ideas this section will draw links between the four pillars of Mills proposed cyber counterinsurgent strategy and the 28 Articles of a counterinsurgent strategy that David Kilcullen has proposed in his book *Counterinsurgency* and which have been successfully adopted into the counterinsurgency strategy of the United States Department of Defense. This section will also briefly explore the clear, build, hold strategy proposed by David Fidier.

This first pillar of Mills cyber strategy identifies the need to induce the cyber insurgents to turn on themselves.[11] Mills indicates the need to create wedges between competing actors in the cyber environment. In this way the focus of the actors is turned partially towards each other pitting their strengths against each other and away from their original objectives. Kilcullen's article 23 describes the need to practice armed civil affairs, which espouses the same principles; the needs to attack the links between insurgent groups and drive a wedge between them and the society.[12] Successful counterinsurgency operations around the world including Canada's experience in Afghanistan have seen success when they are able to "exploit gaps and seams among factions struggling to be the dominant element of the insurgency."[13] Not only does this reduce the level of cooperation and thus the risk of simultaneous attack but also reduces their collective influence on society as a result of mixed messaging. The applications of this principle in the cyber environment has been demonstrated through the concept of "Bug Bounties", through this concept rewards are offered for incriminating information of individuals or groups whom are in possession of computer code that can be used to commit a cybercrime (Malware). The successes of these programs are linked to the dual benefit to the individual whom claims the

[10] Mills, *Counterinsurgency in Cyberspace*, 157-162
[11] Ibid, 158.
[12] David Kilcullen, "Three Pillars of Counterinsurgency" (Remarks delivered at the U.S. Government Counterinsurgency Conference, Washington D.C., 2006), 43.
[13] Mills, *Counterinsurgency in Cyberspace*, 158.

"pelt" as it were. Firstly the financial reward is evident but secondly the elimination of a potential competitor within the cyber environment is often equally or more rewarding. As the number of hackers for hire increase so does the competition for jobs therefore it is in the best interest of the entrepreneurial hacker to turn in their competition and steal their contracts. Through these same principles a number of large firms are offering similar bounties but rather than requiring hackers to turn on each other they offer an opportunity to potential hackers by challenging them to find vulnerabilities in their security defences offering financial incentive if they can identify them. In this manner they are driving a wedge between the would-be hacker, a potential employer and their intent to exploit a weakness. The hacker receives financial compensation while contributing to the security of the company rather that bringing it down, the hacker still gets a payday and does not incur the associated risk of criminal activity. A 2010 article by Jeremiah Grossman indicated that Google and Mozilla where the first two companies to introduce such programs into corporate practice; he further indicated that Facebook, PayPal and Microsoft amongst others had similar programs without financial compensation at the time.[14] Since the writing of that article in 2010 however, all of these companies and most major tech firms now employ this tactic as a part of their cyber security strategy. The US DOD established a program entitled HackerOne which uses a similar bounty program to identify security vulnerabilities; exploiting the talent of the hacker industry. [15] In this manner a shaping of the cyber environment is possible by either removing players that have been "snitched on" or by turning hackers into pseudo employees rather than enemies.

---

[14] Jeremiah, Grossman. *Bug Bounty Programs Comes to Website Security: What do they Mean?* [Bug Bounty Programs comes to Website Security: What do they mean?] 2010. http://blog.jeremiahgrossman.com/2010/12/bug-bounty-programs-comes-to-website.html

[15] Department of Defense, "Department of Defense Launches Bug Bounty Program on HackerOne." *Politics & Government Business* (2016), 26.

The second pillar of Mills cyber strategy is a unified, total-government action plan in cyberspace.[16] Mills highlights the need for federal government to establish a cooperative action plan that considers the interests of all departments as well as the industrial and commercial interests that the nation's economy relies upon if developing its Cyber strategy. Kilcullen's article 13 describes the need in a counterinsurgency environment to build trusted networks.[17] This is the "hearts and minds" part of the counterinsurgency strategy and is built upon a foundation of trust and communication. Kilcullen describe the two parts as ""hearts" meaning persuading people their best interests are served by your success; "minds" means convincing them that you can protect them, and that resisting you is pointless."[18] In this same way the federal government needs to create a willingness for interdepartmental and corporate cooperation to tackle the task of creating a strategy and framework for sharing that looks beyond corporate differences and interdepartmental disputes to address the common security risk. Mills describes how in response to the cyber-attack in Estonia, the US responded in 2007 to ensure it shored up its cyber strategy through unprecedented cooperation. "Departments and Agencies with little vested interest in cooperating across title lines came together and cooperated to produce NS/HSP-54/23, commonly known as the Comprehensive National Cybersecurity Initiative."[19] In much the same way as the military cannot defeat an insurgency on its own but relies upon the economic, political, intelligence and diplomatic powers of a country as well. The cyber environment must leverage these sources of power also, it is only through a unified Whole of Government approach that a cyber-insurgency can be dealt with efficiently. Cooperation must exist between the executive and legislative branches of the government to ensure that policy and

[16] Mills, *Counterinsurgency in Cyberspace*, 159.
[17] Kilcullen, *Three Pillars of Counterinsurgency*, 37.
[18] Ibid, 37.
[19] Mills, *Counterinsurgency in Cyberspace*, 159.

law are complimentary and provide rules within the corporate and service industry to support the national strategy. The ability to regulate internet service providers, minimum security standards for business and personal conduct on the internet are also key to an affective cyber strategy.

The third pillar in Mills cyber strategy is establishing cyber hygiene.[20] Mills indicates that there is a minimum standard for cyber security that all persons and corporations need to adhere to in order to ensure personal and corporate security. Kilcullen's article 16 describes the need to practice deterrent patrolling.[21] In this regard it is suggested that a counterinsurgency force must not only be prepared to encounter an adversary, but must interact with the society to ensure that they are isolated from the adversary and are prepared to resist influence by the insurgents. Mills draws parallels to the notion of establishing a road block where a counterinsurgency force can inspect those attempting to pass to ensure they are not members of the insurgency, are not carrying supplies for them knowingly or unknowingly and are aware of the dangers in the area. In much the same way Mills proposes that proper cyber hygiene is like a roadblock where cyber users are required to possess the necessary protective measures perhaps in the form of up to date virus definitions on their network and firewalls to ensure known threat vectors do not have access to influence cyber users. A proper identification system that is mandatory of users within a cyber-environment would greatly assist in controlling the environment and eliminate the ability to "spoof" firewalls into believing an actor is someone else. This notion is difficult to enforce on the wider internet due to privacy laws but within government and corporate networks, closed networks with unique identification and password controls are now becoming the norm but some open networks still exist that jeopardise the networks of all other networks which then connect to them. The elimination of those open networks with the requirement for secured shared trust

[20] Ibid, 160.
[21] David Kilcullen, *Counterinsurgency* (Oxford: Oxford University Press, 2010), 39.

relationships, with minimum standards for antivirus definition and identification are the cornerstone for cyber hygiene and minimize the opportunity for hackers to hide in your vehicle as you pass checkpoints.

The fourth pillar in Mills cyber strategy is establishing the cyber counterinsurgency training and technology pipeline.[22] Education and training are essential to ensure that those whom will be responsible for executing a nation's cyber strategy have the necessary skills to be proficient but also so that education institutions remain current with this ever changing dynamic environment. Kilcullen's art 28 describes the need to keep the initiative.[23] Forcing your adversary to respond to your actions rather than the contrary where you find yourself reacting to his actions. This marks arguably the greatest gap in Canada's current cyber strategy which is very reactive in nature and relies on intelligence gathering from anecdotal evidence of cyber-attacks that have already been executed and adapting systems to close exposed weaknesses. The proposed approach concentrates on research and development to create an environment that changes faster than potential adversaries have the ability to exploit. A proper education and training system needs to extend beyond postgraduate education which is the mainstay of current education training; but focus at institutionalising cyber security within secondary school and undergraduate programs. Thereby exposing potential future cyber warriors to their future career environment at an earlier age and developing an industry of research and naturalising a career path. Mills draws comparisons to the boom of the Aerospace industry in the 1950s and 1960s the US created interest around this new field of education, institutions created new engineering fields to support government programs as a result the US has maintained the lead in this field ever since. To date the cyber industry in the US and Canada in particular has not created the

[22] Mills, *Counterinsurgency in Cyberspace*, 161.
[23] Kilcullen, *Counterinsurgency*, 48.

necessary education and training environment nor the eventual career fields to stimulate the interest and research in this environment to as great an extent as is possible and frankly required to keep pace with other global actors.

A more simplified cyber strategy is is proposed by David Fidier in his article *Is IT Time for a Counterinsurgency Approach to the Cyber War against ISIS?* Fidier proposes using the clear, hold and build principles of a basic counterinsurgency strategy in the development of a cyber-strategy to combat ISIS in the cyber environment.

Fidier proposes that the clear principle can be applied by reducing the "footprint" of ISIS in the cyber environment.[24] Fidier argues that social media providers actions to counter the messaging that ISIS attempts on their services is an example of challenging the "ground" that ISIS is attempting to hold in this non dimensional environment. By working with service providers to be vigilant in removing ISIS propaganda, they are effectively driving a wedge between them and the society they are attempting to influence in much the same manner as clearing operations are conducted in the real world.

Fidier proposes the hold objective "involves steps to bring online voices from communities adversely affected by ISIS violence and ideology."[25] Fidier argues that it is important to project a counterinsurgency narrative in the cyber medium to take the initiative in shaping greater opinion and by using primary source experiences develop an atmosphere where ISIS ideology is rejected. He further draws parallels to COIN successes where we have learned that "holding the line against the return of insurgent influence works best when communities

[24] David Fidier, "Is it Time for a Counterinsurgency Approach to the Cyber War Against ISIS?" *Defence One* (March 12, 2015), May 8 2016.
[25] Ibid.

with the most at stake populate the front lines."[26] By using social media to put the narrative of the negative effects of ISSI on front page news the intent is to create a resistance to future influence activities within vulnerable communities.

Fidier proposes that the build objective seeks to create a stable cyber environment, one in which ISIS would not have the ability to influence society through its use. Unlike the hold where the objective is to build resilience among the population in the build principle you are attempting to build resiliency in the cyber environment to deny the adversary access to the medium. Fidier draws parallels from the build objective to the role that the cyber environment should play in the development of political, economic and social development of a typical counterinsurgency strategy.

This section has demonstrated how the principles of counterinsurgency operations can be applied to the development of a cyber-strategy. A national cyber-strategy that adopts either the four pillars proposed by Mills and supported by Kilcullen's articles on counter insurgency or a simple clear, hold, build strategy proposed by Fidier are examples of how a national cyber security strategy can shape the cyber environment to ensure that an unconventional adversary is not able to use this medium to influence and disrupt society.

Conclusion

The development of a national security policy in Canada demonstrated Canada's commitment to a recognized essential resource. It is now time however, to step back and re-examine the threat vectors as they exist today in order to ensure that our strategy is focused on addressing not only state actors but also non state and criminal actors. This paper has proven that

[26] Ibid.

the most common threat vector within the cyber environment displays characteristics of a classical insurgent force and that a cyber-strategy based on counterinsurgency principles needs to be adopted in order to effectively deal with these threats. It has been demonstrated that David Kilcullen's articles on counterinsurgency conduct are applicable in large part to the cyber environment and that Canada should adopt a cybersecurity strategy aimed at addressing non-conventional actors. This policy should be based on John Mills's four pillars: inducing the cyber insurgents to turn on themselves, creating a unified, total-government action in cyberspace, establishing cyber hygiene and establishing a cyber-counterinsurgency training and technology pipeline[27] or on Fidier simple clear, hold, build principles.[28] Furthermore, it has been demonstrated that the current cyber strategy is extremely reactive in nature and to be useful a cyber-strategy needs to shape the environment, maintain the initiative and adapt to the extremely complex and dynamic environment.

[27] Mills, *Counterinsurgency in Cyberspace*, 157-162
[28] Fidier, *Is it Time for a Counterinsurgency Approach to the Cyber War Against ISIS?*, May 8 2016

BIBLIOGRAPHY

British-North American Committee. *Cyber Attack: A Risk Management Primer for CEOs and Directors*. London [England]: British North-American Committee, 2007.

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

Canada. Public Safety Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa: Govt. of Canada, 2010.

Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York: Verso, 2014.

Department of Defense. "Department of Defense Launches Bug Bounty Program on HackerOne." *Politics & Government Business* (2016): 26.

Fidier, David. "Is it Time for a Counterinsurgency Approach to the Cyber War Against ISIS?" *Defence One* (March 12, 2015, : May 8 2016.

Grossman, Jeremiah. *Bug Bounty Programs Comes to Website Security: What do they Mean?* [Bug Bounty Programs comes to Website Security: What do they mean?] 2010. http://blog.jeremiahgrossman.com/2010/12/bug-bounty-programs-comes-to-website.html.

Ingimundarson, Joel M.. *Canada's Cybersecurity Strategy: Between Cyber Warriors and Cyber Moderates?*. Toronto, Ont: Canadian Forces College, 2015.

Kelly, Brian B. "Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" can and should Influence Cybersecurity Reform." *Boston University Law Review* 92, no. 5 (2012): 1663.

Kilcullen, David. *Counterinsurgency*. Oxford: Oxford University Press, 2010.

———. "Three Pillars of Counterinsurgency." Remarks delivered at the U.S. Government Counterinsurgency Conference, Washington D.C., .

Martin, Paul Edwin Charles. "Cyber Warfare Schools of Thought: Bridging the epistemological/ontological Divide."Canadian Forces College, 2015.

McGuffin, Chris and Paul Mitchell. "On Domains: Cyber and the Practice of Warfare." *International Journal* 69, no. 3 (2014): 394-412.

Mills, John R. "Counterinsurgency in Cyberspace." *Georgetown Journal of International Affairs* (2011): 157-162.

Olson, Parmy. *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York, NY: Little, Brown and Co, 2012.

Rosenzweig, Paul. *Lessons of WikiLeaks: The U.S. Needs a Counterinsurgency Strategy for Cyberspace*: The Heritage Foundation, 2011.

Gignac, Tamara. "Canada Caught in Internet Paradox; Cybersecurity Strategy Outdated." *Calgary Herald,* 2013.

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