National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# THE LAWLESSNESS OF CYBERSPACE: DO WE NEED AN INTERNET SHERIFF?

Maj R.F.J. Dias

## 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*

# THE LAWLESSNESS OF CYBERSPACE: DO WE NEED AN INTERNET SHERIFF?

Maj R.F.J. Dias



Word Count: 4672

Compte de mots: 4672

## INTRODUCTION

When the first series of interconnected computer networks were first turned on, little did the creators know that within a few decades, over half of the world's population would share in their creation and find themselves so dependent on what would become the World Wide Web. Not expecting that their little research network would ever grow beyond the confines of research and academia, the forefathers of the Internet never considered to impart rules of governance or guidelines on the use and care of the system. Placing ownership and regulations would have been counter to what they were trying to achieve, which was an open system to allow for the free flow of thoughts and ideas for the betterment of the discipline.

Today however, the world is a very different place, with a generation now in their teens that do not know life before smartphones and social media, and when over 3 billion people are connected via this ever-morphing creature which within it carries our lives. Be those personal family memories, identities, financial information and national security postures. The day will come when the security and survivability of this "creature" may come into question. Although the world is more interconnected than ever before, it is also fragmented in thought and ideology, which in time of crisis our "creature" may falter.

Rosenzweig's statement on "How does a fractured international community respond to the phenomenon of the Internet" is of critical concern when discussing governance framework at the international level.[1] This becomes all the more relevant when considering the development of domestic and international security policy regarding the use and securing of cyberspace.

This paper will demonstrate the contemporary use of the cyber domain as a medium through which states extend their national power and where non-state actors thrive in the chaotic

[1] Paul Rosenzweig. "The International Governance Framework for Cybersecurity." *Canada-United States Law Journal* 37, no. 2 (2012). 405.

nature of unregulated cyberspace. Throughout this piece the question, "Do we need an Internet Sheriff?" to regulate and to protect the cyber domain will be explored.

The paper will analyze of current examples of state actors utilizing cyberspace as an extension of its national power exerting its state influence across its population and to other states with relative impunity. Through this review, we will note the role of civil society and non-state actors which work with, and at times against, the state. After having reviewed examples of cyber activities by both state and non-state actors, we will finally consider what international mechanisms currently exist which may be able to answer the challenge of being the ultimate "cyber cop".

**TERMINOLOGY**

To begin discussing anything related to cyber, it is important to use the correct lexicon, and define some terms often used in this domain. As practitioners in our own disciplines, we use the tools available to us in the cyber domain daily often at times using terms interchangeably, without the full understanding of its meaning. Even those who operate, manage, and support these highly complex systems, confess to stumble with using the correct terms. Therefore I offer the following key terms to assist in our discussion of the subject.

*Cyberspace* has been described as the "global, virtual, [information and communications technology] based environment, including the Internet, which directly or indirectly interconnects systems, networks, and other infrastructures critical to the needs of society".[2]

Demonstrating the challenges of defining many cyber related terms, the literature does not find consensus in definition for the term *cyberattack*. One article suggests that a cyberattack is the employment of "cyberspace capabilities, by nation-states or non-state actors acting on [the

[2] Johan Sigholm. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (2013). 6.

state's behalf], to cause damage, destruction or casualties in order to achieve military or political goals".[3] In another article, the disruption of a portion of a nation's economy could be considered a cyberattack, while the stealing of data through intrusion would not constitute an attack.[4]

The military, in attempting to achieve precision even in terminology has to refer back to Clausewitz's criteria of what qualifies as an act of war when defining *cyberwarfare*. According to Clausewitz, an act of war must be violent or have the potential for violence; must be physical to "compel the enemy to accept the attacker's will"; and have a political goal in mind.[5] However, according to Thomas Rid, "no known cyberattack has met all three of those criteria", thus we have yet to see a cyberwar. [6]

In the late 1990s, the concept of cyberwar was seen as the exploitation of knowledge to maintain a battlefield advantage. Targeting those command and control information systems which modern militaries had grown so dependent upon would disrupt and cripple the ability to fight.[7]

Conversely, academics and policy makers began to discuss cyberwar in "terms of attacking infrastructure – a kind of information age [analogous] to strategic bombing" but more recently comparing it to irregular warfare, akin to special operations.[8] The analogy of cyberwarfare compared to special operations and the criteria for what constitutes an act of war will become useful in the analysis of later examples in this section.

---

[3] *Ibid*.

[4] James Joyner. "Competing Transatlantic Visions of Cybersecurity." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-182. Washington: Georgetown University Press, 2012. 160.

[5] Thomas Rid. "*Cyberwar and Peace: Hacking Can Reduce Real-World Violence*." *Foreign Affairs* 92, no. 6 (2013). 78.

[6] *Ibid*.

[7] John Arquilla. "The Computer Mouse That Roared: Cyberwar in the Twenty-First Century." *Brown Journal of World Affairs.* 18, no.1 (2011). 42.

[8] *Ibid*.

The following two terms are proposed due to their prevalence in modern discourse in the halls of academia and policymakers and relevant to the analysis in this paper. Although not exclusive to the post 9/11 world, *cyberterrorism* has become a term which engenders fear and intimidation. Michael Vatis is quoted describing cyberterrorism as "computer-to-computer attacks intended to cause significant damage in order to coerce or intimidate a government or civilian population."[9]

*Cyber-espionage* can be defined as "the use of cyberspace by governments to illicitly procure classified information"[10] while *cyber-sabotage* can affect "business processes without interfering with physical industrial processes, remaining nonviolent" but having costly consequences.[11] *Cyber-sabotage* ultimate "purpose is to gain political, economic, commercial or military advantage over a perceive threat actor".[12]

Finally, *cybercrime* may involve many of the above terms in one form or another, but for now, many nations' police forces address cybercrime within the bounds of their criminal code and national jurisprudence, legislation and other legal and policy instruments.[13] This is a salient point to our discussion as we demonstrate the need for an international body in dealing with cybercrime. Further examples will be identified in later sections. The terms and definitions stated above are by no means all inclusive, but help define the lexicon to be used and which have been considered to be most relevant in this discussion.

**STATE ACTORS**

---

[9] Victor Platt. "Still the fire-proof house? An analysis of Canada's cyber security strategy." *International Journal* 67, no. 1 (2011). 156.

[10] *Ibid*.

[11] Thomas Rid. "*Cyberwar and Peace: Hacking Can Reduce Real-World Violence*." *Foreign Affairs* 92, no. 6 (2013). 83.

[12] Government of Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa, 2010. 5.

[13] Royal Canadian Mounted Police. *Royal Canadian Mounted Police Cybercrime Strategy.* Ottawa, 2015. 19.

Originally intended as a means to share information, research and enhance academia, the Internet and the cyber domain has been used to further advance political agendas over the last decade just as much as any other form of soft or hard power. As another tool in a state's toolbox of power, cyberspace has become a preferred method to exert power and influence on both the international stage and domestic political arena. One can say that in essence, "cyberspace as become militarized".[14]

The literature on the matter consistently refers to the same group of states - Russia, China, and USA. When providing examples of states which are considered to be most capable of state funded and/or sanctioned cyber activities towards another state. Along the spectrum of cyber capabilities, these states are referred to as "advanced persistent threats (APT)".[15] Whether for the purpose of espionage, sabotage, theft or coercion, state actors have utilized cyberspace to exceptional effect.

**Russia**

The first example of state funded or state sanctioned cyber activities would be Russia's effective use of cyber towards its neighbours – Estonia, Georgia, and Ukraine. In 2007, after "Estonian authorities decided to move a Soviet-era memorial" to the outskirts of the city, pro-Russian Estonians launched violent riots in the nation's capital of Tallinn followed by cyberattacks.[16] During a three week period, "cyber-savvy Russian nationalists" conducted coordinated distributed denial of service (DDoS) attacks that crashed and disrupted Estonia's networks, "hijack[ing] up to 85,000 computers", using the computers to conduct the DDoS.[17]

---

[14] Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. MIT Press, 2010. 5.

[15] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 5.

[16] Thomas Rid. "*Cyberwar and Peace: Hacking Can Reduce Real-World Violence*." *Foreign Affairs* 92, no. 6 (2013). 79.

[17] *Ibid*.

These attacks targeted the Estonia's communication infrastructure, mobile phone networks, newspaper outlets, banks, and government web sites including those of key government leaders, hampering Estonia's "ability to carry out administrative functions".[18]

This attack on Estonia's national institutions became known as "Web War One" and the first known case of a state attacking another state through cyberspace, and the first attack towards a NATO member.[19] From this action, Estonia learned some valuable lessons regarding how the nation had been so "wired" across all facets of its society, and has developed new methods for defence and NATO has established the Cooperative Cyber Defence Centre of Excellence in Tallinn.[20]

Russia having had the experience in how to instigate a small cyber conflict turned its eye to another former Soviet republic which was requesting member status within NATO. Post-communist Georgia's foreign policy had seen shifts toward Western ideals since the late 1990s and had requested membership within NATO. In early 2008 at the Bucharest Summit, NATO had declared that Georgia "will become a member" at some point in the future. During the summer of the same year, "Georgia was subject to an extensive, coordinated cyberattack" prior to the "Russian land invasion and air attack".[21]

With precision and severity, the cyberattacks saw the defacement of public websites and barrages of DDoS effectively shutting down the Georgian communication systems, rendering the Georgian defences blind and paralyzed to the oncoming Russian invasion. The attacks targeted

---

[18] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 10.

[19] James Joyner. "Competing Transatlantic Visions of Cybersecurity." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-182. Washington: Georgetown University Press, 2012. 161.

[20] James Joyner. "Competing Transatlantic Visions of Cybersecurity." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-182. Washington: Georgetown University Press, 2012. 161.

[21] *Ibid.*

national institutions and infrastructure similarly to the Estonia attacks the year prior, severing the Georgian government from its citizens. A key differentiation between the attacks on Estonia and those against Georgia was that in 2008, the world saw for the first time coordinated use of cyberattacks with conventional military operations as a form of "hybrid warfare". NATO stated that these attacks demonstrated the "potential to become a major component of conventional warfare".[22] This should now be expected to be the new normal.

The final example of the effective use of cyber in conjunction with the use of military hard power was observed be during Russia's annexation of Ukraine's Crimean Peninsula. In the days leading to the Russian occupation of Crimea, Ukrainian networks had been infected by a complex and pervasive virus affecting key government networks in Kiev.[23] In this case and that of the attacks on Georgia, the ability to point a finger to the exact culprit or culprits has become more of a challenge. These cyberattacks were perpetrated in such a way, that it eluded tracing its origins, but some evidence points to the "Russian Foreign Military Intelligence agency (the GRU) and the Federal Security Service (the FSB)", along with the effective use of intermediaries in the attempt to cover Russian involvement.[24] Less known attacks having targeted Lithuania, Kyrgyzstan, Kazakhstan, the UK, and the US happened without the ability to conclusively point to the Russian government's involvement in these attacks, whether directly or indirectly.[25] The ability to definitively identify those responsible for cyberattacks is of great importance when considering creating an international body with the mandate of capturing and prosecuting those responsible for said attacks.

---

[22] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 11.

[23] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. Cybersecurity Challenges for Canada and the United States. Fraser Institute, 2015. 11.

[24] James Joyner. "Competing Transatlantic Visions of Cybersecurity." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-182. Washington: Georgetown University Press, 2012. 162.

[25] Alexander Klimburg. "Mobilising Cyber Power." *Survival* 53, no. 1 (2011). 49.

**The United States of America**

In keeping with the theme of state actors who are known as being an advanced persistent threat, the United States has long been a leader in this area. Notwithstanding, the US technological prowess, it does not however make them immune to cyberattack as we will see later in this section. The example however most used by academics and cyber security practitioners relates to the United States' use of a cyberattack as a way for it to exert its national will, through a joint venture with Israel against Iran.

In the case of the famous *Stuxnet* worm, the US along with Israel had long been concerned with Iran's nuclear program. Here covert action would be used where diplomatic discussion seemed ineffective. In 2006, the George W. Bush administration authorized the joint cyber operation with Israel with the original intent to cause physical damage to Iranian centrifuges with a view to stopping or slowing down the Iranian nuclear program. Creating malfunctions with machinery and providing false readings as to the true status of equipment, the *Stuxnet* worm created the conditions for the most successful example of cyber-sabotage which would erode Iran's own confidence in their experts and ultimately in their own program.[26] After exposing the worm to the Iranian networks for over a period of 17 months, the worm functioned as intended, burning out 20% of Iran's centrifuges, hundreds of system-critical computers and setting back Iran's nuclear program several months. As noted by Bush's CIA director, this became the first time a major cyberattack was "used to effect physical destruction".[27]

This surreptitious coercive tactic worked for a short while. Once the Iranians realized that the failings of the nuclear program was not due to their lack of understanding and expertise, Iran

---

[26] Thomas Rid. "*Cyberwar and Peace: Hacking Can Reduce Real-World Violence*." *Foreign Affairs* 92, no. 6 (2013). 82.

[27] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 12.

quickly recovered and they too retaliated with its own cyberattack. In 2012, Iran launched its own virus targeting a Saudi oil company, and Qatari natural gas company "effectively destroy[ing all data on over] 30,000 company computers" replacing the data with a "burning American flag" causing the most destructive attack that the private sector had seen.[28] In this case, Iran responded indirectly to the US attack via its allies in the region signalling that "Iran [was] not a weak state incapable of threatening valuable interests in cyberspace.[29]

As mentioned previously, the US is not immune to hostile cyber activities either. In 2008, an infected flash drive was used on a US military laptop at a base in the Middle East. The malicious code spread across the US Central Command networks on both classified and unclassified systems, transferring data to foreign servers. This breach became the impetus for the creation of the US Cyber Command, and a revamp of the US cybersecurity protocols. It was the "most significant breach of US military computers ever".[30]

**China**

The final state actor which has demonstrated capacity and willingness to use the cyber domain as an extension of its foreign policy is China. China has for some time, focused its cyber activities on espionage "in order to bridge technological gaps" with a view to gaining an advantage in support of their national economic development.[31] China is the "top intruder into government and private-sector networks in Canada and the United States".[32] The Chinese has realized the importance of information dominance in a highly technological world, and has

---

[28] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 12.

[29] *Ibid*.

[30] James Joyner. "Competing Transatlantic Visions of Cybersecurity." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-182. Washington: Georgetown University Press, 2012. 162.

[31] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 12.

[32] *Ibid.*, 16.

responded by standing up a special cyber unit under the People's Liberation Army (PLA), which has been attributed to many cyber exploits.[33]

China's cyber exploitation has been focused along two main lines of effort: the targeted state's government departments and their corporate and financial sectors. The Chinese have very effectively been able to conduct cyber exploitation and the gathering of intelligence from foreign ministries and state departments, defence and finance departments, and national research. The information acquired gives the Chinese an informational advantage when discussing issues of state, trade negotiations and with the ability to bring products to market ahead of its competitors. Furthermore the theft of state and industrial secrets poses a grave risk to the affected nation's national security and defence apparatus and further erodes any trust with China in future state to state negotiations.[34]

A Chinese example of intellectual property theft which would likely affect national security was the breach of government contractor networks where information regarding the Joint Strike Fighter and the Boeing C-17 Globemaster project resided. In addition, the networks of Defence Research and Development Canada along with Canada's Finance Department and National Research Council had also been breached with data being stolen.[35] The costs of such breaches are significant, not only in monetary value, but also reputation. Replacement of infected machines and hard drives can be done quickly, but the damage in reputation and trust will take much longer to recoup.

What gives China an advantage in conducting cyber operations in addition to its specialized PLA cyber unit, is China's "close relationship between the central government and

---

[33] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 13.

[34] *Ibid*., 12.

[35] *Ibid*., 14.

many state-owned enterprises".[36] This brings significant resources to China's cyber operations, blending state capacity and state funded capacity, unmatched in the world. Although most of China's activities have been more in the collection of information and intelligence, this has created intended or unintended economic consequences in the private sector. Such example is the fall of the former Canadian tech giant – Nortel. Nortel officials blame a Chinese state-owned telecommunications company for hacking into Nortel and stealing vast amounts of intellectual property over nearly a decade, effectively undermining any of Nortel's competitive edge in bringing new products to market.[37] The same Chinese company has been suspected by the US for placing listening devices and "backdoors" into one of the United States' wireless networks, adding further suspicion of China's true intentions.

The discussion thus far has demonstrated the effective use of cyber operations in gathering intelligence or intellectual property, delaying progress of national capital programs, or as a show of "virtual" force towards another state or its own population as a means to an end. What happens when non-state actors leverage the anonymity and interconnected nature of cyberspace to advance their own political or ideological cause?

**NON-STATE ACTORS**

In this section, the discussion will delve into the analysis of non-state actors in cyberspace through determining the motivation and likely desired outcomes of cyber activities and how they exist in a seemingly lawless domain. For the purpose of this discussion, the numerous and varied non-state actors have been grouped by what motivates them to conduct cyber operations.

---

[36] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 14.

[37] *Ibid.*, 15.

The first group will be motivated by financial gains and tend to act similarly in there cyber activities focussing on use of malware for fraud and identity theft, denial of service attacks, blackmail and extortion. Organized crime has gone high tech and has fully exploited what the cyber domain provides – anonymity and reach. The cybercriminal would not be much different than that of its counterpart in the "real world". Motivated ultimately by financial gain, the cybercriminal can enjoy anonymity and a seemingly borderless "territory" to run their criminal organization. Additionally, the internet offers access to like-minded organizations and easy "entry to market" making cyberspace an ideal forum for organized crime to flourish.[38] Furthermore, with the relative immature status of cyber law enforcement, and the ever increasing use of cyberspace to commit crimes such as identity theft, child pornography, extortion and human trafficking,[39] the net is full of criminals who are more driven by financial gains than political ideologies.

Grouped with organized crime are corporations as non-state actors predominantly due to their motivation for profit and market share. Most corporations would not normally conduct any illegal activity for fear of economic sanctions or prosecution. However if these companies do conduct illegal cyber activities, it is likely on the request of a state – either through contract or state sanction. [40] Intelligence agencies often use corporate fronts to cover any clandestine activities and we have seen the Chinese example of companies acting on behalf of the state in the previous section.

The last non-state actor which could be placed in this group due to their financial motivation is the "insider threat". These are people who have legitimate reasons to have access to

[38] Johan Sigholm. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (2013). 19.

[39] *Ibid*., 20.

[40] *Ibid*., 21.

networks, which would normally be considered trusted agents, but for some reason are now disloyal to their employer, possibly a disgruntled former employee who has a grievance or someone willing to betray their country for financial gains.[41] Handling insider threats are more challenging to contend with because of the legitimate access the individual would normally have for their daily work and who are knowingly compromising critical infrastructure or stealing data. The ease, in which data can be retrieved and transported via removable media, has made it possible for people like Edward Snowden and Jeffrey Delisle to steal thousands of classified documents. [42]

The example of Snowden and Delisle's were considered insider threats but more motivated by ideological and political reasons and not specifically financially motivated. These two cases tie into the second group of non-state actors worthy of discussion. Those who are politically motivated or have a desire for social change, consider themselves as *Hacktivists*. This grouping consists of insider threats, hacktivists and cyber terrorists who are mainly motivated by some ideological desire for social change.

The *hacktivist* will use cyberspace resources such as cyber-sabotage, denial of service, site defacement, and site re-directs as a means to express support to an ideology or political agenda and/or demonstrate in protest. The group "Anonymous" has often acted as a hacktivist non-state actor, predominantly against what it deemed repressive regimes and internet censorship, "carrying out acts of civil disobedience" in cyberspace. [43]

---

[41] Johan Sigholm. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (2013). 17.

[42] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 17.

[43] Johan Sigholm. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (2013). 14.

Cyberterrorists on the other hand are extreme in their ideology and are willing to use violence indiscriminately to achieve their goals. Terrorists are continuing to incorporate cyber operations in their doctrine, and using the Internet for recruiting and other propaganda tools. Terrorists now use the internet and social media to convey their message and provide "how-to" videos in conducting terrorist activities including launching cyberattacks on western governments.[44] Groups like Al-Qaeda and ISIL have been very effective in exploiting the use of social media to carry out their information operations campaign.

In defending national cyber infrastructure and by extension defending national sovereignty, how does a nation reconcile its mandate to protect its national interests and private citizens while not disregarding its citizens' individual privacy and civil liberties? To shed some like in this area, we turn to the last group of non-state actors which can be collectively labeled under civil society. These are groups who through investigative techniques and cyber-sleuthing are able to "call-out" elements of government which they feel are not being truthful or being held to account for their actions specifically as it relates to control over the Internet and censorship.[45] During their daily conduct, these "watch groups" provide the balance expected in western liberal democracies. Generally, these non-state actor groups conduct cyber activities which divulge questionable behaviours of public officials such as tax evasion from the more recent Panama Papers to more socially embarrassing Ashley Madison data breach bringing unwanted attention to the government. Conversely, some of these actors' methods are at times questioned when the issue of national security arises such as the *WikiLeaks* site or the Edward Snowden case.

---

[44] Government of Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa, 2010. 5.

[45] Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. MIT Press, 2010. 11.

The three aspects of a nation's cyber power includes: coordination of operational domestic policy, coherency of policy through international legal frameworks, and cooperation of non-state cyber actors. [46] For western liberal democracies, the most important aspect is the cooperation with civil society in applying a 'whole of nation' approach to security policy including cyber security.[47] It has been suggested that Canada has a "strong civil society" with expertise in cyber security which should be leveraged in creating a framework to deal with cyber threats. Organizations and "think-tanks" such as CyberTRAX and CitizenLab are well known internationally to be able to support in this type of endeavour. [48]

**INTERNATIONAL GOVERNANCE FRAMEWORK**

In this final section, the discussion turns towards considerations for international governance, policies, standards, and ability to police and prosecute offenders of hostile or illegal cyber activities. The examples throughout this paper showcase international states use and sometimes misuse of cyberspace without any concern for repercussion, other than possible forms of retaliatory cyberattacks, but otherwise states and non-state actors go about their cyber activities without a care. A few aspects of cyberspace which appeals to those who would want to use it for illegal purpose, is its relative anonymity, and global interconnectedness. The level of connectivity allows actors to have cyber effects on a global scale, without unnecessarily exposing themselves to authorities. What makes the internet so useful also makes it a challenge to protect.

The responsibility for the protection of society from violence and attack still resides with the state. Despite the societal nature of the Internet, the State does not abdicate the inherent

---

[46] Alexander Klimburg. "Mobilising Cyber Power." *Survival* 53, no. 1 (2011). 43.

[47] Government of Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa, 2010. 12.

[48] Victor Platt. "Still the fire-proof house? An analysis of Canada's cyber security strategy." *International Journal* 67, no. 1 (2011). 166.

responsibility to protect, but to do so without infringing on individual freedoms is the challenge.[49] It is also in this realm, that civil society and state actors have a role in striking a balance between liberty and security.

In discussing governance, existing Internet governance structures are set up to deal with technical standards such as domain names, numbering and naming conventions, technical standards, and the best use practices, ensuring the Internet "superhighway" keeps rolling freely. However, since "nobody actually owns or operates the Internet itself", the rules of the "road" are set by an open community of designers, engineers, and operators. [50] These governance organizations have been established for a while but take decisions by rough consensus and have no enforcement function at all. The open nature of the Internet has been its survival thus far; however as sovereign states begin to crack down on internet traffic within its own borders, it clashes with the original design of the internet for the free flow of information.

One school of thought is to allow sovereign states to have more control of the Internet within their borders and increase security according to their needs. This could be justifiable in the wake of limiting the spread of hate and violence such as extreme ideologies and child pornography, within one's borders, and have the ability to prosecute and punish in accordance with state laws, including those who facilitate such activities.[51]

The other side of the debate would see a more open and distributed security posture across the Internet and a strategy based on liberal democratic principles with consideration for the need to share knowledge and communicate. The concept of distributed security states,

---

[49] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 24.

[50] Paul Rosenzweig. "The International Governance Framework for Cybersecurity." *Canada-United States Law Journal* 37, no. 2 (2012). 410.

[51] Paul Rosenzweig. "The International Governance Framework for Cybersecurity." *Canada-United States Law Journal* 37, no. 2 (2012). 413.

citizens, governments and the private sector all have "roles to play in securing and governing cyberspace, but none to the exclusion or pre-eminence of the others".[52] This school of thought is very much supported by Deibert, in which he states that "civic networks need to be at the forefront of security solutions that preserve cyberspace as an open commons of information, and that protect privacy and support freedom of speech".[53]

Perhaps the answer sees a hybrid solution based on existing international bodies and treaties such as the United Nations. Even Russia and China have advocated for an "international treaty to govern conflict in cyberspace" – a kind of "Cyberspace Geneva Convention".[54] In addition to a treaty, the ability to prosecute and penalise those who commit illegal cyber activities is paramount, for without teeth, a convention or treaty is worthless. Perhaps consideration should be given then to what role the International Court of Justice may play for state actors, or perhaps criminalizing certain cyber activities like the "creation and selling of malicious software" which would allow for law enforcement to apprehend and prosecute theses cyber criminals.[55]

The very nature of the Internet was founded on open and distributed networks, functioning in the absence of centralized control which morphed from an organism-like creature – ever evolving to what it is today. With security concerns and crime being the new reality on the Internet, "securitization of cyberspace may be inevitable, but what forms it takes is not."[56]

**CONCLUSION**

---

[52] Ronald J. Deibert. *Black code: Inside the battle for cyberspace*. Signal, 2013. 239.

[53] *Ibid.*, 237.

[54] Paul Rosenzweig. "The International Governance Framework for Cybersecurity." *Canada-United States Law Journal* 37, no. 2 (2012). 414.

[55] James Joyner. "Competing Transatlantic Visions of Cybersecurity." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-182. Washington: Georgetown University Press, 2012. 165.

[56] Ronald J. Deibert. *Black code: Inside the battle for cyberspace*. Signal, 2013. 241.

Throughout this paper, examples were discussion of contemporary uses of cyberspace to further advance a state's power base. We have also seen the role of non-state actors in that projection of state power and in some case for their own individual gains – whether financial or ideological. Additionally, this paper introduced the role of civil society in cyberspace and how vital its role is in establishing a domestic security policy based on the principles of a liberal democracy and open dialogue.

Finally, we introduced the argument as to whether the Internet should be securitized or not and by whom – sovereign states or international bodies? We also determined that current United Nations organizations could be mandated to prosecute those found culpable of hostile or illegal cyber activities.

It appears then that we already have an Internet Sheriff; we just can't seem to come to a consensus to the Cyber Cop's terms of reference and exact job description, but we know he should be walking the international cyber beat. The need for vigilance, governance and security in the exponential expansion of cyber will necessitate more discussion, specifically those who design, engineer, maintain, monitor and protect the networks. Furthermore, we must remain cognisant that the use of cyberspace was meant to be a tool for communicating and sharing openly of ideas and thoughts to be shared by humanity. It is our job to be good stewards of this capability and ensure it continues for further generations.

**BIBLIOGRAPHY**

Arquilla, John. "The Computer Mouse That Roared: Cyberwar in the Twenty-First Century." *Brown Journal of World Affairs.* 18, no.1 (2011): 39-48.

BBC World News – Latin America – "Panama Papers affair widens as database goes online" – last accessed 09 May 2016. http://www.bbc.com/news/world-latin-america-36249982

Betz, David, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-power*. The International Institute for Strategic Studies, 2011.

Caulkins, Bruce D. *Proactive self defense in cyberspace*. Army War College Strategic Studies Institute, 2009.

CNN Politics. "Chinese cyber espionage group caught hacking defense, industrial base" – last accessed 09 May 2016. http://www.cnn.com/2015/08/05/politics/cyber-espionage-campaign-chinese/

Deibert, Ronald J. *Black code: Inside the battle for cyberspace*. Signal, 2013.

Deibert, Ronald J. "My conversation with Edward Snowden" – last accessed 09 May 2016. http://deibert.citizenlab.org/

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. MIT Press, 2010.

Geist, Michael. "Cyberlaw 2.0." In *Boston College Law Review*. 44 (2002): 323.

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why The Sky is Not Falling*. Army War College Strategic Studies Institute, 2013.

Gansler, Jacques S. *Democracy's arsenal: Creating a twenty-first-century defense industry*. MIT Press, 2011.

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

International Consortium of Investigative Journalists – last accessed 09 May 2016. https://panamapapers.icij.org/

International Telecommunication Union – last accessed 09 May 2016. http://www.itu.int/en/Pages/default.aspx

Joyner, James. "Competing Transatlantic Visions of Cybersecurity." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-182. Washington: Georgetown University Press, 2012.

Klimburg, Alexander. "Mobilising Cyber Power." *Survival* 53, no. 1 (2011): 41-60.

Levin, Avner, Paul Goodrick, and Daria Ilkina. "Securing cyberspace: a comparative review of strategies worldwide." In *The 2014 IT Canadian Conference*. 2013.

Mazanec, Brian M., and Bradley A. Thayer. *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace*. Palgrave Macmillan, 2014.

Moens, Alexander, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015.

NATO Cooperative Cyber Defence Centre of Excellence – last accessed 09 May 2016 https://ccdcoe.org/un.html

Parliament of Canada. "The Standing Senate Committee on National Security and Defence, Ottawa, 05 November 2012". Last accessed 06 May 2016. http://www.parl.gc.ca/content/sen/committee/411%5CSECD/49784-e.HTM

Platt, Victor. "Still the fire-proof house? An analysis of Canada's cyber security strategy." *International Journal* 67, no. 1 (2011): 155-167.

Rid, Thomas. "*Cyberwar and Peace: Hacking Can Reduce Real-World Violence*." *Foreign Affairs* 92, no. 6 (2013): 77-87.

Rosenzweig, Paul. "The International Governance Framework for Cybersecurity." *Canada-United States Law Journal* 37, no. 2 (2012): 405-432.

Royal Canadian Mounted Police. *Royal Canadian Mounted Police Cybercrime Strategy*. Ottawa, 2015.

Sigholm, Johan. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (2013).

United Nations Office on Drugs and Crime – last accessed 09 May 2016. https://www.unodc.org/