National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# GROWTH INDUSTRY: AN EXAMINATION OF NON-STATE ACTORS IN THE CYBER DOMAIN

Maj P.J. Kelly

## JCSP 40

## Exercise *Solo Flight*

**Disclaimer**



## PCEMI 40

## Exercice *Solo Flight*

**Avertissement**



Canada

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

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

# GROWTH INDUSTRY: AN EXAMINATION OF NON-STATE ACTORS IN THE CYBER DOMAIN

Maj P.J. Kelly



Word Count: 3673

Compte de mots: 3673

# GROWTH INDUSTRY: AN EXAMINATION OF NON-STATE ACTORS IN THE CYBER DOMAIN

> *States are more likely to receive blame for cyber acts of terror than are the non-state actors frequently responsible for this genre of criminal activity.*
>
> Michael N. Schmitt and Liis Vihul – Proxy Wars in Cyberspace[1]

## INTRODUCTION

We live in a world that is growing increasingly dependent on the internet and various forms of networked systems. This is true for individuals, corporations and governments alike. As society's dependence on technology increases, so does the threat from the cyber domain. Exposure to new risks has led to an increase in cyber incidents. Cyber incidents can result from both deliberate actions and unintentional events. Due to increased threat, there has been a heightened level of attention placed on cyber-attacks. These attacks include gaining unauthorized access to digital systems for the purposes of gaining access to sensitive information, corrupting data and/or disrupting operations. Additionally, execution of an attack does not necessarily require access to systems, such as is the case with a denial-of-service attack. The threat is wide in nature: almost anyone who has a network connection may execute a cyber-attack; this includes individuals, like-minded groups, corporations and even governments.[2] The impacts of these attacks may be quite varied. Examples include financial crime, identity theft, fraud, disruption of communication systems, etc.

---

[1] Michael N.Schmitt and Liis Vihul, "Proxy Wars in Cyberspace - The Evolving International Law of Attribution." Last Accessed May 19, 2015. http://www.fletchersecurity.org/#!schmitt-and-vihul/cyhm.

[2] U.S. Securities and Exchange Commission. "CF Disclosure Guidance: Topic No. 2 Cybersecurity." Last Accessed May 19, 2015. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

This paper will focus on the role and impacts of non-state actors within the cyber domain, it will examine the various forms of non-state actors, their motivations and the potential impacts that these actors can have on the cyber domain when aligned with nation states. To accomplish this, we will first review terminology associated with the cyber domain. Next, we will briefly review some well-known cyber-attacks. Then, we will examine the various types of non-state actors in the cyber domain and their potential impacts. Following this, we will examine the widespread nature of social media use and its impact on modern conflict. Finally, we will look at some of the current legal challenges that arise when dealing with actions occurring within cyberspace.

**TERMINOLOGY**

In media as well as various other sources, there are many references to cyber warfare. To provide context for the reader, here is a list of definitions for the most commonly used related terms:

Cyberspace: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, Telecommunications networks, computer systems and embedded processors and controllers"[3]

Cyber-attack: "Operations employing the hostile use of cyberspace capabilities, by nation states or non-state actors acting on their behalf, to cause damage, destruction, or casualties in order to achieve military or political goals."[4]

[3] United States Department of Defense. *Joint Publication 1-02 - Department of Defense Dictionary of Military and Associated Terms.* (Washington: Department of Defense, 2015), 58.

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

Cybersecurity: "Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack."[5]

## BRIEF HISTORY OF CYBER WARFARE

When comparing the age of other known forms of warfare with cyber warfare, the latter is in its infancy. One of the first known examples of malicious activity was the Morris Worm. Reported on November 2nd 1988, it was a piece of malware. Designed by Robert Morris to attack other systems, its intent was to determine how big the Internet actually was at the time. The worm had no payload – it simply propagated from system to system. This first piece of malware essentially crashed the internet: at the time, it affected 6000 of 60,000 systems on the internet.[6]

Fast forward to 2007 when government networks in Estonia suffered denial-of-service attacks. These attacks were in retaliation of the Estonian government's removal of a Soviet war memorial. The attacks targeted multiple government websites, banks, universities, and newspapers. They lasted for three weeks and ended when Estonia took the step of blocking all international network traffic.[7] The International Affairs Review from George Washington University states:

> It is now known that the attackers who waged cyber warfare on Estonia acted on their own initiative, primarily as a form of political protest. These "hacktivists" turned out to be a combination of experienced hackers who would contract out their own botnets or write their own malicious programs, and "script kids" who were, by and large, individual novice

[5] Merriam-Webster. "Dictionary - Cybersecurity." Last Accessed May 19, 2015, http://www.merriam-webster.com/dictionary/cybersecurity.

[6] Larry Seltzer, "The Morris Worm: Internet malware turns 25." Last Accessed 19 May 2015, http://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/

[7] Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security" Last Accessed 19 May 2015, http://www.iar-gwu.org/node/65

> hackers who attacked Estonian target sites by following "how-to" guides found on various hacker websites.[8]

Here lies an important distinction: these attacks were orchestrated not by a nation state, but by non-state actors who acted upon their own initiative. The actions of these types of actors are the subject of this paper.

In July 2010, Stuxnet was discovered. It was a piece of malware that replicated through Microsoft Windows operating system as it sought out an application known as Siemens Step7. This application provides control for various forms of equipment; in its final step it compromised the Programmable Logic Controllers (PLC) allowing access to monitor and sometimes control the industrial systems – which were, in turn, controlled by these devices.[9] Stuxnet is reported to have attacked Iranian uranium enrichment centrifuges, which delivered a crippling blow to Iran's nuclear capability.[10]

In January 2011, a cyber-attack originating from China infiltrated several key government agencies: Defence Research and Development Canada, Department of Finance, the Treasury Board. The intent of the attack was to gain access to key government systems to access classified information. Greg Weston for CBC news reported, "any such attack would have some connection to the government in China, which is also known for producing so-called 'patriotic hackers' devoted to targeting institutions or governments perceived as threatening to the government at home."[11] This

---

[8] *Ibid*.

[9] David Kushner, "IEEE Spectrum - The Real Story of Stuxnet." Last Accessed May 19, 2015. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[10] Kaspersky Lab. "Press Release, First Victims of the Stuxnet Worm Revealed." Last Accessed 19 May 2015, http://usa.kaspersky.com/about-us/press-center/press-releases/first-victims-stuxnet-worm-revealed-kaspersky-lab-reports.

[11] Greg Weston, "CBC News - Politics - Foreign hackers attack Canadian governement." Last Accessed May 19, 2015. http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618.

is yet another example where attribution of the source of the attack is unclear; it appears to have been carried out by non-state actors in the interest of their governments.

## TYPES OF NON STATE ACTORS

In his paper, *Non-state Actors in Cyberspace Operations*, Johan Sigholm makes a very relevant statement concerning the characteristics of cyberspace:

> Its asymmetric nature, the lack of attribution, the low cost of entry, the legal ambiguity, and its role as an efficient medium for protest, crime, espionage and military aggression, makes it an attractive domain for nation-states as well as non-state actors in cyber conflict.[12]

In the brief history of cyber warfare outlined above we have seen several instances where the actions and motivations of non-state actors have aligned with the interests of nation states and had very negative consequences for the intended targets.

Various non-state actors such as malware authors, hacktivists, script kiddies and patriot hackers have already been mentioned. This section will outline more of the various forms of non-state actors in cyberspace and provide some details regarding their methods, motivations and potential targets. This paper will discuss them in order of increasing complexity.

The most prolific actor within cyberspace is the ***Ordinary Citizen***. The vast majority of *Ordinary Citizens* use the Internet for legitimate purposes: surfing the web, using online services for business, entertainment and educational purposes. The actions of *Ordinary Citizens* are typically passive; most lack the knowledge or intent to act maliciously within the cyber domain. The primary reason that *Ordinary Citizens* are important to distinguish is that various other actors target their systems in order to

[12] Sigholm, "Non-State Actors…" 1.

leverage their computing power for malicious acts. A single piece of malicious software commonly known as malware could potentially leverage the power of millions of *Ordinary Citizens'* computer systems to flood a network with traffic to overwhelm a specific recipient causing a denial-of-service attack.

The next actor is referred to as ***Script Kiddies***. These actors are not technologically sophisticated and they rely on tools written by more experienced individuals. They generally are motivated by bragging rights from gaining access and defacing various websites. Some refer to their actions of defacing websites as being the Graffiti artists of the Internet.[13]

***Hacktivists*** is a term used to describe a wide array of actors. The Oxford dictionary defines *Hacktivist* as "A person who gains unauthorized access to computer files or networks in order to further social or political ends."[14] *Hacktivism* is generally a means to reach underlying political, military of commercial goals. *Hacktivist* groups are comprised of many forms of activists ranging from script kiddies to sophisticated Black Hat Hackers. Probably the best-known collection of *Hacktivists* today is the collective Anonymous, whose methods range from website defacements, redirects, and denial-of-service attacks. [15] Currently the Anonymous collective is focusing their efforts on hindering ISIS and their supporters. They have vowed to attack social media accounts that ISIS uses extensively to spread their message to the rest of the world. Heather Saul

[13] Greg Harvey, "Sitepoint - Website Defacers - the Graffiti Artists of the Internet." Last Accessed May 19, 2015. http://www.sitepoint.com/graffiti-artists-internet/./

[14] Oxford Dictionary, "British & World English > Hacktivist." Last Accessed 19 May 2015, http://www.oxforddictionaries.com/definition/english/hacktivist.

[15] David Kushner, "The New Yorker - The Masked Avengers, How Anonymous incited online vigilantism from Tunisia to Ferguson." Last Accessed 19 May 2015, http://www.newyorker.com/magazine/2014/09/08/masked-avengers.

reporting for The Independent states, “More than 1,500 Twitter and Facebook accounts have been taken off line since the hacktivists launched their fight against ISIS supporters.”[16]

When most people think of hostile actions in cyberspace, they think of hackers. Webster’s Dictionary defines a hacker as “a person who secretly gets access to a computer system in order to get information, cause damage, etc.”[17] However, the term hacker is a very broad term. Hackers are broken into four categories based on their motivations.

The first is the ***Black Hat Hacker*** whose motives are for personal financial gain or other malicious reasons. Their targets are decided based on their motivations, they use their knowledge of computer systems to infiltrate networks and gain access to information or cause damage which will benefit their cause. An example of their activities would be to break into databases to steal credit card information, either to use personally or to sell the information for profit.

The second type of hacker is the ***White Hat Hacker***, essentially the polar opposite to the Black Hat Hacker. Their motivations are driven by a desire to improve security of computer systems and they generally have high moral standards when compared to the general population. Governments or security consulting corporations generally employ these types of hackers to expose vulnerabilities in their systems so that they may be updated before they are exploited.

---

[16] Heather Saul, "Operation Isis: Anonymous takes down Twitter and Facebook accounts associated with extremist group", Last Accessed 19 May 2015, http://www.independent.co.uk/life-style/gadgets-and-tech/operation-isis-anonymous-vows-to-take-down-accounts-and-associated-with-extremist-group-10035199.html

[17] Merriam-Webster. "Dictionary - Hacker." Last Accessed May 19, 2015, http://www.merriam-webster.com/dictionary/hacker.

These hackers' names are derived from old western movies. In those films the good guys wore white cowboy hats where the bad guys wore black.[18]

The next type of hacker is the ***Grey Hat Hacker***. As implied by the color, grey, these hackers generally fall into the category of a white hat, but can dabble in the black hat side of things when something affects them personally – usually in retaliation to an event or an attack on something on which that they had previously worked.

Finally, we are left with the ***Patriot Hacker***. These hackers are motivated to support the interests of their nation state. Three nations are known to have large Patriot Hacker communities: China, Russia and Syria. Some of the well-known groups in China are the 'Honker union' and the 'Red Hacker Alliance.'[19] In Russia, the 'Nashi Youth' are believed to have been involved in the aforementioned attacks on Estonia in 2007. In Syria, the well-known group that goes by the name of the 'Syrian Electronic Army' has recently attacked several Western news networks, defacing their websites in order to display messages and to take these sites offline temporarily. The CBC was one of the targets of this group and their site was hacked in November 2014.[20]

---

[18] Techopedia, "Black Hat Hacker", Last Accessed 19 May 2015, http://www.techopedia.com/definition/26342/black-hat-hacker

[19] Scott Henderson, "Beijing's Rising Hacker Stars… How Does Mother China React?" *IO Sphere* (Fall 2008), 25-30.

[20] CBC News, "Syrian Electronic Army claims hack of news sites, including CBC.", Last Accessed 19 May 2015, http://www.cbc.ca/news/technology/syrian-electronic-army-claims-hack-of-news-sites-including-cbc-1.2851962


**Figure 1 - Image of CBC website hacked by the SEA**

Corporations are another non-state actor that commit various actions within cyberspace; their motivations are almost always are profit driven. They will conduct operations in cyberspace in order to gain a competitive advantage, sometimes in line with the national interests of nation states. At times, they will enlist the services of various hacker groups, either Black Hat or Patriot hackers based on the type of operation they are conducting. Their methods certainly vary and are hard to trace. Corporations can conduct a wide range of activities to infiltrate competitors and gain confidential information. The largest example of this in Canada is the case of telecom giant, Nortel Networks, infiltrated by Chinese based hackers; this resulted in the theft of confidential information and led to the eventual demise of the company.[21] From discussions with former Nortel employees, Chinese telecommunications giant Huawei directly benefitted from these efforts as their products are rumoured to be extremely similar to former Nortel

[21] Siobhan Gorman, "Chinese Hackers Suspected In Long-Term Nortel Breach", Last Accessed 19 May 2015, http://www.wsj.com/articles/SB10001424052970203363504577187502201577054

technology. Brian Shields, a former security advisor for Nortel was quoted by the CBC, stating:

> It was on behalf of Huawei and ZTE and other Chinese companies that could have used this information to compete against us in the marketplace. How can you survive when you have a competitor basically right there knowing all your moves, what you're doing, what you see as the future products?[22]

This incident is also having a further effect on the Canadian Government's efforts to consolidate the Department of National Defence (DND) operations in the National Capital Region to the former Nortel Campus. In 2013, the Ottawa Citizen reported of the possibility of electronic eavesdropping devices being present from the former compromise of Nortel Networks.[23] No listening devices have been found; however, the court of public opinion makes the move to the Nortel campus unappealing for many.

We have looked at various forms of non-state actors, from ordinary citizens, to hackers with varying interests, to corporations who are motivated by financial gain. We have seen instances where actions of certain non-state groups have had direct impacts against other nations, either through direct attacks against infrastructure such as in Estonia, or through the gathering of confidential information, as evidenced by Chinese based attacks against the Canadian government and Canadian industry, in the example of Nortel Networks where thousands lost their jobs and pensions.

---

[22] Laura Payton, "Former Nortel exec warns against working with Huawei", Last Accessed 19 May 2015, http://www.cbc.ca/news/politics/former-nortel-exec-warns-against-working-with-huawei-1.1137006

[23] David Pugliese, "Delays in move to former Nortel campus cost DND millions", Last Accessed 19 May 2015, http://ottawacitizen.com/news/politics/delays-in-move-to-former-nortel-campus-costs-dnd-millions

**SOCIAL MEDIA**

The next section of this paper will focus on the emerging world of Social Media. In an increasingly interconnected world, people have greater potential for exposure to online influences. To examine this phenomenon further, we will look at how ISIS uses social media – such as Facebook and Twitter – to spread its message globally. Social media helps ISIS gain support for their cause, recruit new members, inspire vulnerable members of Western society to become radicalized, and conduct lone wolf attacks.. Michelle Zillo for CTV News quoted Defense Minister Jason Kenney as saying, "Very typically it happens online, these are what in other times you might have called social misfits, kids that often don't fit in. And sometimes but not always, they come from families where there have been problems."[24] A recent example of Canada's efforts to minimize this threat was the interception of 10 youths attempting to travel to join ISIS from Montreal on May 15th.

J.M Berger and Jonathon Morgan have conducted some interesting research on the use of Twitter by ISIS. Their paper entitled *The ISIS Twitter Census* makes some very interesting and relevant observations:

> Best estimate of total number of overt ISIS supported accounts on Twitter: 46,000, Maximum estimate of ISIS supporter accounts onTwitter: 90,000, Average number of tweets per day per user: 7.3 over lifetime of account, 15.5 of last 200 tweets by user … Most common month accounts were created: September 2014.[25]

[24] Michelle Zilio, "Most young Canadian ISIS recruits targeted online: Jason Kenney", Last Accessed 24 May 2015, http://www.ctvnews.ca/politics/most-young-canadian-isis-recruits-targeted-online-jason-kenney-1.2388452

[25] J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census." The Brookings Project on U.S. Relations with the Islamic World - Analysis Paper No. 20, (2015): p. 9.

One of their deductions was that the month that most Twitter accounts were created directly correlated with the timeframe that ISIS used Twitter to distribute graphic images and videos of the beheadings of hostages.[26] Another interesting statistic they presented is ISIS' widespread use of smartphones to spread their message via Twitter. This further reinforces the notion that the world is interconnected to the point that the religious fundamentalism of ISIS is now available at your fingertips, on your smartphone.

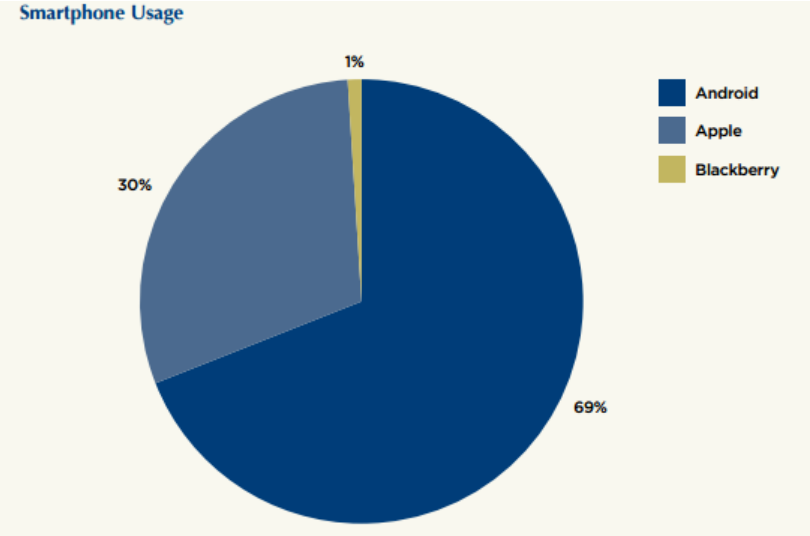


**Figure 2 - Smartphone usage among ISIS supporters**[27]

We live in an interconnected world where social media has provided a new tool for groups to spread their messages globally. We have also seen other groups such as Anonymous take actions against groups such as ISIS that are using social media; they attempt to expose them and disrupt their activities. Analysis of the use of social media is also one of the methods that law enforcement such as the RCMP, CSIS and CBSA use to monitor support for these groups domestically.

[26] *Ibid*, p.19.
[27] *Ibid*, p 26.

## LEGAL IMPACTS

As cyberspace has evolved rapidly over the last 25 years, the cyber community and international legal system are both working to keep pace. The United States government published their International Strategy for Cyberspace in May 2011, wherein they state:

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace.[28]

The consensus is that there does not need to be a completely new set of laws developed to govern cyberspace. Existing laws that cover international conflict may serve as the basis for this new form of conflict as many of the underlying principles are similar, such as use of force, proportionality of response and the right to self-defence. NATO has published the Tallinn Manual which consists of the agreed upon rules agreed to by experts in the field, it cites appropriate references to existing international laws and provides explanations on how they are to be applied in the cyber context.[29]

Our previous examples of actions by non-state actors provide evidence that there are two general challenges faced when dealing with operations in the cyber domain. Attribution – essentially, proving who committed the action, and Proportionality – the appropriate response.

Attribution appears to be the most difficult problem when dealing with cyber operations, as Schmitt references the Koh Speech in his article The Koh Speech and the

---

[28] US Government, International Strategy for Cyberspace (Washington: The White House, 2011): p. 9.

[29] Michael Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard Law International Journal* 54: p. 15.

Tallinn Manual Juxtaposed, it states, "How do we address the problem of attribution in cyberspace? Unresolved."[30] The single word answer, unresolved, is the crux of the problem. Attribution will be unresolved until there is sufficient proof that an individual or group has committed an action; however, there are limited legal avenues available to pursue. As we have seen in previous examples, the operations that have been conducted by Patriot Hackers have met little public or legal response; the burden of proof in such cases is quite difficult, as those who commit these actions are very diligent in covering their tracks.

The other major challenge is the proportionality of the response. Once an action has been attributed to a person or group, what is the appropriate response? This concept is no different whether applied to the cyber domain or conventional military operations. The rule of proportionality for cyber operations expressed in rule 51 – Proportionality of the Tallinn manual – states,

> A cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited.[31]

The key issues in dealing with operations in cyberspace are the issues of attribution, actually proving that someone has committed the action and the proportionality of the response. Nation states will continue to struggle with these issues for some time to come.

---

[30] *Ibid*, p.34

[31] Michael Schmitt, *The Tallinn Manual on International Law Applicable to Cyber Warfare*. (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013): p. 159.

## CONCLUSION

The world of cyberspace is relatively new in comparison to other known arenas of conflict. It is a world that is expanding exponentially. In the last twenty-five years, the evolution of technology and networks has enabled global access from the palm of your hand, in the form of a smartphone. The number of devices connected to the Internet is growing to a point that society will soon exceed the number of available network addresses that were available when the internet was created. To illustrate this point, CBC News technology reporter Peter Armstrong stated,

> IP addresses are like the internet's phone numbers. Under the web's current system, there are billions of them – 4.3 billion to be exact. But as more of us do more and more online, those addresses are being gobbled up. And soon, very soon that supply will run out.[32]

This rapid expansion has created opportunity for criminal, military and terrorist uses. This paper has shown through examples that there are various actors involved in cyberspace and for the most part, they are not acting on behalf of a nation state. Nation states are very cognisant of the threat that cyberspace provides. Cyberspace is a very accessible medium where the cost of entry is relatively low. The purchase of computer systems and a reliable network connection is a much lower cost than a conventional military force, and arguably can impose similar effects when directed at a nation's economy, industry or infrastructure. We have not seen direct state-to-state cyber conflict as of yet and probably will not in the near future. We have seen that states have a preference to allow non-state actors to act on their behalf in order to maintain deniability

[32] Peter Armstrong, "The internet's IP addresses are running out: Can IPv6 save the day?" Last Accessed May 19, 2015. http://www.cbc.ca/news/technology/the-internet-s-ip-addresses-are-running-out-can-ipv6-save-the-day-1.3074428.

and to leverage one of the well-known weaknesses in prosecuting cyber operations, attribution.

China and Russia are known to tolerate, if not sponsor, such non-state actors in the form of Patriot Hacker groups. As China and Russia are both permanent members of the UN Security Council, any changes to international laws or operations directed at pursuing non-state actors will probably be vetoed. Experts in the field have widely discussed the application of international law. NATO has produced the Tallinn Manual that serves as the basis of understanding on how existing international laws may be applied to actions in cyberspace.

Non-state actors continue to be the primary operators in cyberspace. Their motivations range from personal gain to aligning with the interests of their chosen nation state. The impacts have ranged from the interruption of government services such as in in Estonia, the downfall of leaders of industry such as the infiltration of Nortel, and the destruction of infrastructure such as the Stuxnet attacks in Iran. Considering the scale and damage of these known cyber-attacks, they have similarities to terrorist activities, they are conducted by groups or networks which are hard to locate, hard to predict, and more importantly, hard to trace back to their original source.

The number of actors in cyberspace will increase for the foreseeable future. As the world becomes ever dependant on technology, the potential for return on investment in cyber capabilities will increase. In simple terms, cyberspace is a growth industry and will be for some time, both in the conduct of cyber-attacks and conversely the efforts invested in cybersecurity.

## BIBLIOGRAPHY

Armstrong, Peter. *The internet's IP addresses are running out: Can IPv6 save the day?* May 15, 2015. http://www.cbc.ca/news/technology/the-internet-s-ip-addresses-are-running-out-can-ipv6-save-the-day-1.3074428 (accessed May 19, 2015).

Berger, J. M., and Jonathon Morgan. *The ISIS Twitter Census.* Analysis paper, The Brookings Project on U.S. Relations with the Islamic World, 2015.

CBC News. *Syrian Electronic Army claims hack of news sites, including CBC.* November 27, 2014. http://www.cbc.ca/news/technology/syrian-electronic-army-claims-hack-of-news-sites-including-cbc-1.2851962 (accessed May 19, 2015).

Gorman, Siobhan. *Chinese Hackers Suspected In Long-Term Nortel Breach.* Feburary 12, 2013. http://www.wsj.com/articles/SB10001424052970203363504577187502201577054 (accessed May 19, 2015).

Harvey, Greg. *Sitepoint - Website Defacers - the Graffiti Artists of the Internet.* January 15, 2003. http://www.sitepoint.com/graffiti-artists-internet/ (accessed May 19, 2015).

Henderson, Scott. "Beijing's Rising Hacker Stars… How does Mother China React?" *IOSphere - The Professional Journal of Joint Information Operations*, Fall 2008: 25-30.

Kaspersky Lab. *Press Release, First Victims of the Stuxnet Worm Revealed.* November 11, 2014. http://usa.kaspersky.com/about-us/press-center/press-releases/first-victims-stuxnet-worm-revealed-kaspersky-lab-reports (accessed May 2015, 2015).

Kushner, David. *IEEE Spectrum - The Real Story of Stuxnet.* Feburary 26, 2013. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (accessed May 19, 2015).

—. *The New Yorker - The Masked Avengers, How Anonymous incited online vigilantism from Tunisia to Ferguson.* September 8, 2014. http://www.newyorker.com/magazine/2014/09/08/masked-avengers (accessed May 19, 2015).

Merriam-Webster. *Dictionary - Cybersecurity.* 2015. http://www.merriam-webster.com/dictionary/cybersecurity (accessed May 19, 2015).

—. *Dictionary - Hacker.* 2015. http://www.merriam-webster.com/dictionary/hacker (accessed May 19, 2015).

Oxford Dictionary. *British & World English > Hacktivist.* http://www.oxforddictionaries.com/definition/english/hacktivist (accessed May 19, 2015).

Payton, Laura. *Former Nortel exec warns against working with Huawei.* October 11, 2012. http://www.cbc.ca/news/politics/former-nortel-exec-warns-against-working-with-huawei-1.1137006 (accessed May 19, 2015).

Pugliese, David. *Delays in move to former Nortel campus cost DND millions.* August 22, 2014. http://ottawacitizen.com/news/politics/delays-in-move-to-former-nortel-campus-costs-dnd-millions (accessed May 19, 2015).

Richards, Jason. *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security.* http://www.iar-gwu.org/node/65 (accessed May 19, 2015).

Saul, Heather. *Operation Isis: Anonymous takes down Twitter and Facebook accounts associated with extremist group.* Feburary 10, 2015. http://www.independent.co.uk/life-style/gadgets-and-tech/operation-isis-anonymous-vows-to-take-down-accounts-and-associated-with-extremist-group-10035199.html (accessed May 19, 2015).

Schmitt, Michael. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard Law International Journal* 54 (December 2014): 13-37.

Schmitt, Michael N., and Liis Vihul. *Proxy Wars in Cyberspace - The Evolving Internation Law of Attribution.* May 22, 2014. http://www.fletchersecurity.org/#!schmitt-and-vihul/cyhm (accessed May 19, 2015).

Schmitt, Michael. *The Tallinn Manual on International Law Applicable to Cyber Warfare.* Talinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013.

Seltzer, Larry. *The Morris Worm: Internet malware turns 25.* November 2, 2013. http://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/ (accessed May 19, 2015).

Sigholm, Johan. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* (National Defence University, Finnish Society of Military Sciences) 4, no. 1 (2013): 1-37.

Techopedia. *Black Hat Hacker.* 2015. http://www.techopedia.com/definition/26342/black-hat-hacker (accessed May 19, 2015).

U.S. Securities and Exchange Commission. *CF Disclosure Guidance: Topic No. 2 Cybersecurity.* October 13, 2011.

https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (accessed May 19, 2015).

United States Department of Defense. *Joint Publication 1-02 - Department of DefenseDictionary of Military and Associated Terms.* Washington: Department of Defense, 2015.

US Government. *International Strategy for Cyberspace.* Washington: The White House, 2011.

Weston, Greg. *CBC News - Politics - Foreign hackers attack Canadian governement.* Feburary 16, 2011. http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618 (accessed May 19, 2015).

Zilio, Michelle. *Most young Canadian ISIS recruits targeted online: Jason Kenney.* May 24, 2015. http://www.ctvnews.ca/politics/most-young-canadian-isis-recruits-targeted-online-jason-kenney-1.2388452 (accessed May 24, 2014).