The Significance of Cyberspace in Canadian Security Policy

Miron Lakomy

The phenomenon of cyber-terrorism, cyber-espionage, or even the first examples of using cyberspace to conduct military operations has convinced decision-makers that new solutions to security challenges need to be implemented. Cyber-attacks in Estonia and Georgia, multiple incidents in the United States and the Stuxnet worm attack proved that computer networks have became a theatre of rivalry, not only between states but also between non-state actors (such as terrorist groups or criminal organisations). Therefore, there is a rising need to investigate how different governments react to cyber threats. This article deploys the example of Canadian approaches to securing cyberspace in terms of its policy direction and the international solutions that may be discerned.

Keywords: Cyber-security, Stuxnet, security policy, Canada, cyber-terrorism

Introduction

Traditional definitions of national and international security in the post-Cold War era are increasingly becoming outdated. The mainstream definitions of security adopted by Renouvin, Duroselle, Wright and Osgood, and many others, were based on the concepts of national interest, survival and the absence of fear. Such traditional approaches to security problems after the Cold War are obsolete. Zięba claimed that after 1989, a definition of security should include not only the military and political dimensions, but also economic, social, cultural,

ideological or even ecological. However, none of the canonical definitions included the rising importance of computer networks. On the verge of the 21st century, even such a broad approach to security was insufficient. The rapid development of information and communications technology (ICT) surprised states and they lost control over this process. In 1995 there were only about 15 million internet users. Five years later, there were 361 million, and 10 years later about 2 billion.[1] This process was accompanied by rising malicious activity on the internet. It led to new kinds of challenges for the security of states; neither regulated by national nor international laws.[2] Cyber-threats were unrecognised by most states until the first decade of the 21st century. The phenomenon of cyber terrorism, cyber espionage, or even the first examples of using cyberspace to conduct military operations finally convinced decision-makers that new solutions needed to be implemented. Cyber-attacks in Estonia and Georgia, multiple incidents in the US or the Stuxnet worm attack proved that computer networks have become a theatre of rivalry, not only between states but also between non-state actors. Therefore, there is a rising need to investigate how different governments react to cyber threats.

This article presents the significance of cyberspace in Canadian security policy. There are several reasons why Canada's case is interesting. First, Ottawa is strongly involved in global security efforts, especially through military operations like in Afghanistan. This increases threats to Canada via acts of terrorism, including cyber-terrorism. Canada is also a neighbour and a key strategic and economic partner of the US; a popular target of cyber-attacks. Multidimensional cooperation between Canada and the US may encourage governments and non-state actors to use cyberspace against Canada. Its high-tech industry, advanced military technologies and well-developed economy also make Canada a convenient target of cyber-terrorism or cyber-espionage. Furthermore, thanks to outdated juridical practices, it is one of the most popular places to undertake cyber-criminal activity.[3] Finally, despite such challenges, Canada was relatively late to adopt its first official cyber-security strategy. This document was presented in October 2010 when most European and Asian countries had their long-term plans already well-established and implemented. These issues beg several questions:

What are the main challenges to Canadian cyber-security?

What measures are deployed by Ottawa to counter cyber-threats?

What shortcomings have retarded Canada's cyber-security strategy?
What is the overall significance of cyberspace in Canada's security policy?

Cyberspace as a Challenge to National Security

To answer such questions, it is necessary to understand which challenges to national security stem from cyberspace in more general terms and define its very meaning. The first recorded use of the term cyberspace was by science-fiction writer William Gibson who understood this concept as a 'consensual hallucination,' which was the matrix. In his book *Neuromancer*, he used the word cyberspace to depict the world of digital networks, being a theatre of war, not between states but between corporations.[4] In the 1990s, other definitions were generated; for instance, Hildreth characterised cyberspace as 'the total interconnectedness of human beings through computers and telecommunication without regard to physical geography.'[5] However, it should be noted that the "cyber" prefix is derived from the word cybernetics and has a general meaning of 'through the use of computers.'[6]

Even though the term had not yet entered the parlance of security, the first cyber-threats occurred in the 1960s and 1970s. However, these were no more than simple acts of cyber-crime such as basic data theft. The first time cyberspace was used for national security purposes, was likely undertaken by the US Central Intelligence Agency in 1982. The CIA installed a so called "logic bomb" in the Canadian industrial programme which was stolen by Soviet spies and used to control pipeline systems in Siberia. The "logic bomb" caused an overload resulting in a huge explosion.[7] It was not the only example of cyberspace activity in the 1980s. A couple of years later, NATO used the programme *PROMIS* to hack servers located behind the Iron Curtain. These acts demonstrated the potential there was in computer networks. [8]

Initially cyber threats were connected mostly with the activity of home-grown hobbyists, so-called "script kiddies," creating the first world-wide malware attacks and committing rather simple hacking attempts. They were behind the rise of wide-spread viruses such as *Boza, Michelangelo, Melissa,* and *I love you*.[9] Over time, this phenomenon evolved as individual hackers organised into groups. Among others, they were responsible for the first serious acts of cyber-terrorism in South-East Asia, where groups of hackers threatened to attack the Indonesian banking systems as a reaction to the crisis in Eastern Timor.[10]

The breakthrough however came in the 1990s and Richard A. Clarke noted that 'as Internet usage grew, so did intelligence agencies' interest in it.[11] American, Chinese, and Russian governments were the first to pioneer the true potential of cyberspace. In March 1998, Russian hackers initiated operation *Moonlight Blaze* against American military, business and scientific networks. For the next two years, they hacked multiple servers belonging to universities, research institutes, corporations, as well as the Pentagon, the Department of Energy, and NASA. As US officials admitted, the Russians managed to obtain information about American missile targeting systems. It was the first massive, well-planned attack against the US in cyberspace. This experience helped convince US decision-makers about the rising significance of the Internet regarding national security. In 2003 Chinese hackers, under the operation *Titan Rain*, conducted another well-coordinated attack against American military and scientific servers, obtaining information concerning the *Joint Strike Fighter* programme.[12] At the same time, Russian and Chinese programmers began targeting West European servers; they were seeking new technologies, business, military, political, and private information.[13]

In 2006-2007 another milestone was reached. First, in 2006 Israel conducted operation *Orchard* against an alleged Syrian nuclear facility. The mission successfully undermined Damascus' attempt to become a nuclear power as Israeli fighter jets operated over hostile airspace thanks to the computer virus *Suter*, which infected Syrian antiaircraft defence systems and prevented Israeli aircraft from appearing on Syrian radars. This was the first time that cyberspace was used to conduct a tactical military operation and demonstrated that computer networks could open completely new possibilities for both defensive and offensive military efforts.[14]

Second, in April 2007, a political crisis erupted between Russia and Estonia, caused by Tallinn's plans to remove the *Bronze Soldier* statue, which commemorated the liberation of Estonia by the Soviet army. The Russians reacted with a diplomatic protest and a massive cyber-attack.[15] Multiple websites and servers belonging to the government and private companies were blocked and overwhelmed. Hackers attacked the websites of the President of Estonia, government, ministries, political parties, and media consortiums. Furthermore, Estonian e-banking services were attacked and produced a serious blow to the national financial system. Even telecommunication networks suffered multiple

incidents and malfunctioned. The Russians used a relatively simple method of attack called Distributed Denial of Service (DDoS), thanks to the huge botnet they disposed. The incidents in Estonia were regarded as the first cyber war, since computer networks were used to paralyse the critical infrastructure of a nation-state. Similar methods were used by the Russians one year later during the conflict in Georgia, when cyberspace became the fifth domain of war. On 07 August 2008, when war broke out, Russia reacted with armed force and the Internet. Using the same methods as in Estonia, Russian programmers successfully paralysed key elements of the Georgian critical ICT infrastructure. The main Internet and telecommunication services were blocked, along with government and private companies' websites. Georgia was largely deprived of the ability to present its position to the international public.

Finally, the vast potential of cyberspace was demonstrated through Israel's alleged creation and deployment of the *Stuxnet* virus designed to paralyze Iran's nuclear weapons programme. As many IT scientists noted, *Stuxnet* was the most advanced malicious programme ever created and its complexity initially prevented experts from understanding even its basic functions. It targeted industrial systems in both the Bushehr and Natanz nuclear power plants, interrupted communications between systems, disrupted inputs and calculations and generally undermined both plants in terms of their technological framework. Gerwitz argued that *Stuxnet* opened a new era of cyber-warfare and suggested that this new type of cyber-weapon had a similar meaning for international security as the bombing of Hiroshima and Nagasaki.[16]

In some ways, *Stuxnet* has acted as a punctuation mark for a variety of tactics deployed in cyberspace which add it its international appeal. For instance, cyber-operations retain, low operating costs, transcend national political boundaries without having to expose operatives to risks and they increase the potential and scope of propaganda activities. At the same time, there is an absence of strategic intelligence and warning systems that may offset such attacks while difficulties with international cooperation to deal with such issues persist.[17]

At present, cyber-threats may be classified into three groups:

Cyber-terrorism: a politically motivated attack or threat of attack against computers, systems or networks to intimidate or force groups or governments to meet specific demands;

Cyber-espionage: to extract classified information from systems or

networks;

Cyber-War-fighting: to use aspects of cyberspace to conduct military operations.[18]

The conducting of any of these may be considered as an act of cyber-war. And others add to such an understanding: Clarke sees it as 'actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption,[19] while Yagil presented it as a military operation that causes damage or changes to information and communication systems of the enemy.[22] As early as 1995 Warden included cyberspace as the fifth domain of armed conflict (next to air, sea, land and outer space);[21] a point confirmed by US Deputy Secretary of Defence General William J. Lynn, who said that 'as a doctrinal matter, the Pentagon has formally recognised cyberspace as a new domain in warfare.'[22]

Of course, such a definition depends on how war is understood. This work accepts the logic of Gelven's approach which holds war to be 'an actual, widespread and deliberate armed conflict between political communities, motivated by a sharp disagreement over governance,'[23] though concludes that Gelven has little to offer in terms of understanding post-Cold war conflict. Cyber-warfare is extraterritorial, typically clandestine and often involves unidentifiable patterns and consequences. In short, understand cyber-war entails an entire rethink of war itself; its laws, conventions and implications.

Consider Ellis' depiction of the challenges to international law posed by such technological explosions. He suggested that the

> prospects of new technological attacks may pose problems for international law because law is inherently conservative. Technological change may enable new activities that do not fit within existing legal categories, or may reveal contradictions among existing legal principles.[24]

Indeed, cyberspace may pressure international law in three ways: Firstly, the damage caused by cyber-attacks is fundamentally different than the physical damage produced traditional warfare. The extraction or manipulation of computer data may result in intangible damage, such as disrupting government activities. Secondly, the features of electronic signals, which may be projected around the world with impunity, crossing different geographical regions and allowing different entities to affect the network challenges the inherent laws of sovereignty; in cyberspace they are ill-defined and difficult to execute.

Finally, it is difficult to distinguish between cyber-attacks against military and civilian targets and damage caused by cyber-attacks may also skirt human rights.[25]

Cyber-warfare challenges the security policies of all industrial states and the lack of a clear international mechanism to coordinate responses has increased the need for independent actions to be undertaken in a spinoff of an arms race. In short, each state is forced to develop its own plan of action with or without its allies.

Canadian security environment

Canada has not been spared the trials associated to security in cyber-space. However, analysis of policy in this domain must be preceded by a short depiction of Canada's wider security environment. Canada's security is largely based on its NATO membership, geopolitical position and its terminally close relationship to the US. This latter additive predates NATO and is based on geographical proximity combined with integrated infrastructures (re: power grids), economic interdependence and similar perceptions of international problems.[26] Despite such advantages, Canada still feels acute security challenges; made all the more acute since the 11 September 2001 terrorist in the neighbouring US. In fact, Canada recognised five challenges produced by states or sub-state groups:

- International terrorism is currently considered the most potent threat to Canada's national security. The 9/11 attacks, the bombings in Madrid, London, and Bali forced a major shift in Canadian security policy since al Qaeda recognises it as among its main enemies a point accentuated by Canada's role in the counter-terrorism coalition spearheaded by the US in the aftermath of 11 September.[27]
- The proliferation of weapons of mass destruction, to other states and terrorist organisations, is viewed by Canada as representing its second main challenge.
- Failed or failing states, perceived as a factor for spreading instability and providing fertile recruitment grounds for terrorist and organised crime.
- Foreign espionage serves the fourth area of concern.
- Organised crime supporting the trafficking of people, narcotics and weapons.[28]

To meet such challenges, Canada's National Security Policy (CNSP) listed three main goals: 1. protecting Canada and Canadians at home and abroad, 2. ensuring that Canada is not a source of threats for its allies and 3. contributing to international security. The third goal is especially interesting, as Canada is perceived as one of the most active nations when it comes to global security efforts. However, as Bland and Maloney note, the Canadian operational approach in the international environment is usually rather more reactive than adaptive.[29] To develop more complex and corresponding approaches to current challenges, the document listed multiple measures. Among others, it decided: to establish an Integrated Threat Assessment Centre, analysing all threat-related information,[30] to establish a National Security Advisory Council composed of security experts, to create a Cross-Cultural Roundtable on Security,[31] and to enhance Canada's security intelligence capacity and emergency planning programmes. It also promised increased Canadian participation in the activities enhancing the international security environment.[32] For all these units, Canada remains vulnerable to breaches of its cyber-security. .

Significance of Cyberspace in Canadian Security Policy

The Canadian cyber security policy

Libicki once noted that 'the denser the electronics the more that cyberspace pervades real space, the more dependent real life becomes on the correct functioning of cyberspace.'[33] Canada is, at the moment, one of the most wired states in the world and nearly all governmental and business services are Internet-based. As stated above, cyber security challenges are strongly related to the level of ICT development. On one hand, the widespread use of the Internet is beneficial, for regular citizens, business and the public sector. Alternatively, the wide use of the Internet causes a higher risk of serious cyber incidents, as the Estonian example revealed. In 2007, 87% of Canadian business and 74% of households used the Internet and online sales were estimated at $62.7 billion (CDN). A year later, almost 60% of personal tax filings were electronic and in 2009, 67% of Canadians banked online. And, the federal government offers about 130 online services including business, family support, cultural, health, financial benefits, taxes, environmental, and career opportunities, showing just how important computer networks have become for Canada.

Despite the rising dependence on ICT's and the Internet, Canadian officials underestimated the importance of cyberspace and related issue were only seriously addressed in the 2004 CNSP which noted:

> The August 2003 electrical blackout that affected Ontario and eight US states demonstrated how dependent we are on critical infrastructure and how vulnerable we are to accidents or deliberate attacks on our cyber and physical security. Cyber-attacks are a growing concern that have the potential to impact on a wide range of critical infrastructure that is connected through computer networks [...] Cyber-security is at the forefront of the trans-border challenges to Canada's critical infrastructure. The threat of cyber-attacks is real, and the consequences of such attacks can be severe.[34]

According to Gagnon, Canadian perceptions of cyber-threats were similar to the US.[35] However, Canadian counter-measures were insufficient compared to Russian and the US. Ottawa simply did not allocate sufficient resources to catch-up to most other developed countries. Despite multiple, mostly scientific, voices to create a proper cyber-security strategy, such did not materialise for another six years—even after the Estonian and Georgian cyber-wars.

In April 2010, Bradbury asked

> where is Canada's cyber security strategy? [...] Cyber-crime is becoming an increasingly pervasive problem that affects people across the globe. For example, losses from online crime more than doubled in the US last year, according to the latest figures from the Internet Crime Complaint Centre (IC3), which is operated by the FBI south of the border [...] As cyber-criminals continue to exploit vulnerable victims online, governments should surely be stepping in to do something about it, and yet Canada seems to be trailing significantly. The Canadian Government has long promised a cyber-security strategy to protect its citizens.[36]

It did not take long for Bradbury to be vindicated; in January 2011 Chinese hackers gained access to the Finance and Treasury Board, the Finance Department and the Defence Research and Development Canada networks, which forced the government to curtail the use of the Internet.[37] Then, in June the same year, a group called LulzCraft hacked the website of the Conservative Party of Canada, where they

placed information concerning the hospitalisation of PM Stephen Harper, causing acute confusion.[38] This runs against the backdrop that Canada has suffered from a major boom in cyber-crime, in particular phishing. About 1.7 million Canadian citizens were victims of identity thefts in 2008, which caused a loss of about $2 billion (CDN); 86% of Canadian companies were harmed by cyber-attacks in 2009.[39] According to Glenny, Canada is also the sixth most popular country among hackers to host servers running malicious programmes.[40] These threats were summarised by the Minister of Public Safety, Peter Van Loan, who noted at the beginning of 2010 that 'we don't have a day go by when there isn't some effort by someone somewhere in the world to breach government systems.'[41]

Canada's answer was the adoption of its Cyber Security Strategy (CCSS) on 03 October 2010.

The CCSS presented several basic definitions and information concerning Canadian cyber security of value to this work. For instance, Cyberspace was defined as

> where the electronic world created by the interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship.[42]

The Strategy also defined cyber-attacks, as

> unintentional or unauthorised access, use, manipulation, interruption, or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information.[43]

The CCSS also made a firm declaration tha

> Our success in cyberspace is one of our greatest national assets. Protecting this success means protecting our cyber systems against malicious misuse and other destructive attacks [...] Cyber security affects us all, in part because even attackers with only basic skills have the potential to cause real harm.'

The CCSS also underscored the main challenges for Canadian cyber security. Legislators admitted that there are multiple ways to undertake harmful activity on the Internet, like exploiting vulnerabilities in security systems or using malicious software such as trojans, viruses and backdoors. The Canadian Strategy formulated similar assessments of cyber threats like Rand Corporation in the mid-1990s.[44] According

to this act, cyber-attacks are considered as inexpensive, easy to use, effective and low risk.

On this basis, the Strategy distinguished three main types of cyber-threats:

State sponsored espionage and military activities;

Cyber-terrorism to recruit and conduct basic cyber-attacks;

Cyber-crime in the areas of: identity theft, extortion and or money laundering. Some criminal groups are engaged in trade with credit/debit card numbers, logins, and passwords or even malicious software.

Such a threat perception is standard among most developed states. But such a simple classification of challenges is not enough. By comparison, the US Computer Emergency Readiness Team recognises a wider group of cyber-threats, from national governments' cyberwarfare programmes, cyber-espionage, cyber-terrorism, industrial spies, and organised crime groups, to hacktivists, bot-networks operators, phishers, spammers, and malware authors.[45] A narrow perception of the risks by the CCSS may be problematic. Canada's strategy is focused on the manifestations of malicious activity but omits its roots notably, the existence of bot-networks.[46]

The CCSS also identified several counter-measures such as: securing government systems' – understood as defence of Canadian "cyber-sovereignty" – security, and economic interests; partnering to secure vital cyber-systems outside the federal government and assisting Canadian citizens to be secure online. The main goal included strengthening cyber-systems and critical infrastructure sectors, supporting economic growth, and protecting Canadians from cyber threats.

The Strategy also invited the private sector, NGO's and the academic community to cooperate with the government. It underlined the importance of citizens in the efforts to secure Canadian cyberspace: 'The government can introduce and support important cyber security initiatives, but it cannot protect each of us from every threat we encounter when we go online. Canadians must be aware of these threats, and of the tools available to recognise and avoid them.' Finally, the CCSS clearly identifies the country's preferred allies in the struggle to secure cyber-space: the US, UK and Australia were listed as the closest security partners of Canada. Finally, the document stated that Ottawa will participate in the international cyber-security discussions at key organisations such as NATO, Council of Europe and the United Nations.

Canada is the only non-European state that signed the Convention on Cybercrime.[47]

The CCSS is the first official document to address information challenges and may be assessed from two perspectives. Despite being a late addition, it delivered the long awaited mechanisms to face contemporary cyber-security challenges. It implemented a new division of responsibilities between core institutions tasked to secure computer networks. The CCSS also introduced an innovative understanding of cyber-space, absent in most strategies of NATO members. Such a definition proved accurate, especially considering how, recently, social networks helped influence political changes in the Middle East. Furthermore, the idea of partnerships between public and private, federal, and provincial institutions is also a move in the right direction. Finally, the CCSS introduced interesting ideas regarding how to secure critical infrastructure

Significance of Cyberspace in Canadian Security Policy

lBut, the CCSS is incomplete and omitted a number of important issues. Cyber-security can be understood in many different ways, and that is why it is crucial to make all necessary clarifications in official documents. This is not the case with CCSS, which used multiple terms without providing a clear definition concerning what each term meant which may cause some interpretation problems. And the Strategy consists of a very broad definition of cyberspace while skirting many social and political questions; activities of hacktivists, spammers, social networks, or those using the Internet for propaganda purposes are completely omitted despite its rising importance for the security of states. Then, the international dimension of Canadian cyber-security policy, remains haphazard. As Mehan stated, 'information globalism equals increased exposure,[48] and there is a great need for international cooperation to secure cyber space. The CCSS promised dedication for international efforts, however it does not elaborate. What, for instance, should such global cooperation look like? Finally, the document lacked precision when it came to regular citizens and educational efforts. As stated above, increased citizens' awareness and proper training programs could themselves prevent many cyber threats e.g. the existence of bot-networks.[49] Canada's Cyber Security Strategy lacked specific ideas and how they may be realised.

Conclusion: The Significance of Cyberspace in Canadian Security Policy

Despite the CCSS, Canada continues to face real problems in securing its cyber-domain. The first concerns insufficient government spending, which reveals the level of importance attached to cyberspace for Canadian authorities. Ottawa allocated roughly $100 million (CDN) for cyber-security for a period of 5 years. At the same time, other leaders were spending billions of dollars per year, which is still insufficient to face-down contemporary threats. The huge difference here between Canada and most of the other developed countries causes a growing gap in cyber-potential, and this may become a very serious threat for national security in future. As Deibert noted, the Canadian cyber security strategy was adopted too late and its solutions are insufficient compared to the cyber policies of Canada's allies like the US. According to Deibert:

> It devotes far too few resources to the problem, does not fully address the division of appropriate institutional responsibilities, and only barely nods at the importance of a foreign policy for cyberspace. A recent investigation revealed our public sector infrastructure was so thoroughly infiltrated with malicious activity emanating from foreign jurisdictions that the entire Treasury Board was taken offline for weeks. Embarrassingly, a recent security study ranked Canada among the highest of countries for the hosting of malicious content.[50]

Second, despite the provisions of the Strategy, Ottawa is almost absent in international discussions concerning cyber-security challenges. Even during the most important international summits like the G8 and G20, Canada's role is limited. There is a lack of political willingness to belong. Even within NATO, which is constantly developing cyber-security solutions, Canada's voice is virtually non-existent. Even more troubling is Canadian IT technology, including social media monitoring tools, are being used by Middle Eastern or African countries to 'limit free speech, quash potential rebellions and stifle online freedoms.'[51].

Furthermore, during the age of the cyber arms race, when such countries like the US, Russia, China, Iran, Syria, and Israel have focused on developing cyber potential, Canadian solutions remain mostly outdated. For example, authorities still have not decided whether to create an equivalent of the American military cyber command, which could trigger a major shift for the defence industry. At the same time, law enforcement agencies in Canada are overwhelmed by the surge in

cyber-crime. Domestic juridical solutions do not keep pace with the development of cyber-threats.[52].

To counter these problems Canada should create

> a comprehensive strategy to protect the cyber commons [...] [it] should begin by linking the international consequences of domestic policies [...] We need to give law enforcement new resources, capabilities, proper training and equipment to sort through voluminous flows of existing data. But alongside those resources, Canada should be setting the highest standard of judicial oversight and public accountability. New resources, yes, but the same if not more rigorous checks and constraints on powers [...] Part of Canada's cyberspace strategy needs to focus outward. Our Foreign Affairs department should be at the forefront of the promotion of decentralized and distributed security mechanisms, while actively resisting proposals that seek to alter the constitution of cyberspace through top-down, heavy-handed government controls (...) Diplomatically, we should work to build a broad community of like-minded states who share this common vision, and have an interest in a secure and open cyber commons across the many different venues of cyberspace governance. Such rules should include the promotion of norms of mutual restraint in cyberspace, protections for privacy and civil liberties, joint vigilance against cyber-crime networks, and respect for the free flow of information.[53]

Canadian authorities have, for many years, danced around adopting a proper strategy to address pressing cyber-security challenges. In 2010 the CCSS was adopted but was insufficient. Compared to US and some European documents, the CCSS – despite some interesting solutions – omitted many essential issues such as: hacktivism, bot-networks, social networks, education and training, and international cooperation. In the 21st century, such a simple strategy is not enough to face contemporary challenges. Canada has devoted too few resources to secure its cyberspace and neglected several important issues, such as training and educational programmes and functioning international cooperation, especially with the US and other allies. There is a serious need for Canada to implement a new, updated strategy, which would address all the omitted problems and contain the ideas on how cyberspace challenges should be managed by the government internally and external-

ly for the upcoming years. The way cyberspace will be perceived by Canadian authorities will not only affect Canadian national security. It will also surely be one of the key factors influencing the future status and position of Canada on the international stage and the manner in which its allies choose to behave towards it. In many ways, states are the product of their times and if Canada cannot keep apace of the changes to security brought about over the past three decades, it risks increased security dependence from those that may not be able to afford providing security for a country that can scarcely secure itself.

***

Miron Lakomy is affiliated to the Institute of Political Science and Journalism at the University of Silesia in Katowice, Poland and may be reached at: miron-lakomy@wp.pl

** Author's note: This manuscript was created with the assistance of the Government of Canada/avec l'appui du gouvernment du Canada, under the Faculty Research Program of the International Council for Canadian Studies.

Notes

1 'Internet Growth Statistics,' *Internet Growth and Stats*, available at: <www.allaboutmarketresearch.com/internet.htm> (accessed 22 January 2011).

2 See: Esterle Alain (2009), 'La securité de l'information et des réseaux est-elle une affaire d'état(s)?,' *Annuaire Francais de Relations Internationales*, vol. 10; Ryszard Zięba (1999), *Instytucjonalizacja bezpieczeństwa europejskiego*, Warsaw: Wydawnictwo Scholar, pp. 31-35 and Miron Lakomy (2010), 'Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku,' *Stosunki Międzynarodowe –International Relations*, 42:3-4, pp. 55-56.

3 Misha Glenny (2011), 'Canada's Weakling Web Defences,' *Information Warfare Monitor*, at: <www.infowar-monitor.net/2011/05/canadas-weakling-web-defences> (accessed 18 October 2011).

4 William Gibson (2009), *Neuromancer*, Warsaw: Książnica.

5 Steven A. Hildreth (2002), 'Cyberwarfare,' in John V. Blane (ed)

(2002), *Cyberwarfare: Terror at a Click*, New York: Novinka Books.

6 See: Myriam Dunn Cavelty (2008), *Cyber-Security and Threat Politics*, London: Routledge and Alicja Bógdał-Brzezińska, Marcin F. Gawrycki (2003), *Cyberterroryzm i problem bezpieczeństwa informacyjnego we współczesnym świecie*, Warsaw: Fund, Studiów Międzynarodowych.

7 War in the Fifth Domain,' *The Economist*, 01 July 2010.

8 Tomasz Formicki (2007), 'Komandosi cyberprzestrzeni,' *Stosunki Międzynarodowe*, 07 November 2007, <www.stosunki.pl> (accessed 22 January 2011).

9 Jean Guisnél (1995), *Guerres dans le cyberespace*, Paris: La Découverte/Poche, pp. 117-127; Jean Guisnél (1999), *Cyberwars: Espionage on the Internet*, New York: Basic Books and David S. Wall (2007), *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity Press.

10 Lakomy (2010), p. 55-58.

11 Richard A. Clarke and Robert K. Knake (2010), *Cyber War*, New York: Ecco, pp. 36.

12 Bradley Graham (2005), 'Hackers Attack via Chinese Web Sites,' *Washington Post*, 28 August 2005.

13 Lakomy (2010), p. 55-58.

14 Jeffrey Carr (2011), *Inside Cyber Warfare*, Sebastopol: O'Reilly Media

15 Estonia Cordons off Parliament, Start Exhumation by Statue,' *RIA Novosti*, <http://en.rian.ru/world/20070428/64629451.html> (accessed 10 June 2011)

16 See, for instance, 'Stuxnet Heralds Age of Cyber Weapons, Virtual Arms Race,' *Homeland Security Newswire*, <http://homelandsecuritynewswire.com/stuxnet-heralds-age-cyber-weapons-virtual-arms-race> (accessed 25 May 2011) and Aleksandr Matrosov, Eugene Rodionov, David Harley, Juraj Malcho (2010), 'Stuxnet Under the Microscope,' *ESET Report*, 31 January 2010, available at: <http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report-2010.pdf> (accessed 25 May 2011)

17 Strategic War … In Cyberspace,' *Rand Research Brief*, January 1996

18 Julie E. Mehan (2008), *CyberWar, CyberTerror, CyberCrime*, Cambridge: IT Governance Publishing, pp. 31-41; Aneta Janowska (2003), 'Cyberterroryzm- rzeczywistość czy fikcja?,' in Lesław H. Haber (ed) (2003), *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, Kraków: Uczelniane Wydawnictwa Naukowo-Dydaktyczne AGH, pp. 448-449 and Lakomy (2010), p. 56

19 Clarke and Knake (2010), pp. 70

20 Limore Yagil (2010), *Terroristes et Internet: La Cyberguerre*, Montre-

al: Abebooks, pp. 55

21 John A. Warden (1995), 'Enemy as a System,' *Airpower Journal*, 9, p. 40-55

22 William J. Lynn (2010), 'Defending a New Domain,' *Foreign Affairs*, (September/October 2010)

23 Stanford Encyclopaedia of Philosophy

24 Brian W. Ellis (2001), 'The International Legal Implications and Limitations of Information Warfare: What Are Our Options?' *US-AWC Strategy Research Project*, Pennsylvania: US Army War College, p. 3

25 Ibid, p. 3

26 Philippe Lagasse (2011), 'Email Communication to author,' See also: Theodore Olson (ed) (1988) , *Canadian Defence And The Pursuit of Peace*, York Centre International and Strategic Studies; Hugh Segal (ed) (2005), *Geopolitical Integrity*, Montreal: IRPP and David Rudd, Jim Hanson and Nicholas Furneaux (eds) (2002), *Vision into Reality: Towards a New Canadian Defence and Security Concept*, Toronto: CISS

27 Emmanuel-Pierre Guittet (2009), 'La militarization de la lutte antiterroriste au Canada,' in Stephane Leman-Langlois, Jean-Paul Brodeur (ed) (2009), *Terrorisme et antiterrorisme au Canada*, Montreal: Presses de l'Université de Montréal, pp. 161-164

28 E-mail to author, August 2011

29 Douglas L. Bland and Sean M. Maloney (2004), *Campaigns for International Security*, Queen's University Press, pp. 21

30 Integrated Threat Assessment Centre (ITAC),' at: <www.itac-ciem.gc.ca/prtnrs/index-eng.asp> (accessed 24 June 2011).

31 Cross-Cultural Roundtable on Security,' at: <www.publicsafety.gc.ca/prg/ns/ccrs/index-eng.aspx> (accessed 24 June 2011)

32 *Securing an Open Society: Canada's National Security Policy*, Privy Council Office, Canada, April 2004; *Securing Open Society: One Year Later*, Privy Council Office, Canada, April 2005. Hereafter CCSS

33 Libicki (2008), *Conquest in Cyberspace*

34 'On-line Forms and Services by Topic,' Government of Canada at: <www.canada.gc.ca/forms-formulaires/onlineformstop.html> (accessed 11 August 2011) and *Securing an Open Society*

35 Benoit Gagnon (2009), *Informatique et cyberterrorisme*, in Stephane Leman-Langlois and Jean-Paul Brodeur (ed) (2009), *Terrorisme et antiterrorisme au Canada*, Montreal: Presses de l'Université de Montréal, pp. 131

36 David Bradbury (2011), 'Where is Canada's Cyber Security Strategy?' *Geek Town*, at: <www.geektown.ca/2010/04/where-is-cana-

das-cyber-security-strategy.html> (accessed 29 June 2011)

37 Ian Austen (2011), 'Canada Hit by Cyberattack,' *Information Warfare Monitor*, <www.infowar-monitor.net/2011/02/canada-hit-by-cyberattack/> (accessed 28 June 28)

38 'Canadian Press Interviews Victor Beitner about Harper "Breakfast Incident" Hoax,' *Cyber Security Canada*, <www.cybersecuritycanada.com/news/2011/06/08/canadian-press-interviews-victor-beitner-about-harper-breakfast-incident-hoax.html> (accessed 26 June 2011)

39 CCSS

40 Nestor E. Arellano (2011), 'Canada's Phishing Activity Booming, Report Warns,' *Information Warfare Monitor*, at: <www.infowar-monitor.net/2011/05/sign-up-for-our-newsletters-email-the-editor-email-a-friend-print-this-page-canadas-phishing-activity-booming-report-warns/> (accessed 26 June 2011) and Misha Glenny (2011), 'Canada's Weakling Web Defences,' *Information Warfare Monitor*, at: <www.infowar-monitor.net/2011/05/canadas-weakling-web-defences> (accessed 26 June 2011).

41 Andrew Duffy (2010), 'Ottawa Focused on New Cyber-Security Strategy,' *Ottawa Citizen*, 08 April 2010

42 CCSS

43 Ibid.

44 'Strategic War… in Cyberspace,' *Rand Research Brief*, January 1996.

45 'Cyber Threat Source Description,' *The United States Computer Emergency Readiness Team*, at: <www.us-cert.gov/control_systems/csthreats.html> (accessed 11 August 2011)

46 CCSS, pp. 4-6.

47 Ibid, p. 7

48 Mehan (2008), pp. 83

49 Ibid, pp. 71-82

50 Ronald Deibert (2011), 'Cyber Security: Canada Is Failing the World,' *Huffington Post*, 26 May 2011

51 Matt Hartley (2011), 'Mesh 2011: Citizen Lab's Ron Deibert on "Repression 2.0,' *Financial Post*, 25 May 2011 and Deibert (2011)

52 E-mail message to author, September 2011

53 Deibert (2011)

Distributed Cyber Security as Cyber Strategy. However, there are also major challenges around cyberspace policy and security for Canada. A report by the International Telecommunications Union ranked Canada 26th among countries worldwide based on 11Â Another set of breaches, also connected back to China, hit several government agencies, including the Treasury and Finance Departments and the DRDC.9 Federal employees were forced offline for several months as a consequence of the breach.10 Meanwhile, another Canadian company, Research in Motion (RIM), has faced cyber security challenges of a different sort: dozens of governments have sought access. Canadaâ€™s Cyber Security Strategy. For a stronger and more prosperous Canada. Â© Her Majesty the Queen in Right of Canada, 2010. Cat. No.Â Canadiansâ€™ personal and professional lives have gone digital: we live, work, and play in cyberspace. Canadians use the Internet, computers, cell phones and mobile devices every day to talk, email, text and twitter with family, friends and colleagues. We do business online everyday, from banking to shopping to accessing government services â€“ and we do it from wherever we happen to be. Digital infrastructure makes all this possible, and also keeps essential services up and running. Canadians â€“ individuals, industry and governments â€“ are embracing the many advantages that cyberspace offers, and o Our Cyber Security Strategy outlines the Bankâ€™s approach to cyber security for the medium term: reducing risk and promoting resilience. While it is important to prevent cyber attacks where possible, we must be prepared to respond and recover quickly if a breach does occur. We are investing in system-wide defences to ensure the Bankâ€™s operations are secure. And we intend to work closely with our financial system partners to promote cyber security in Canada and around the world. Filipe Dinis, COO. Cyber Security Strategy 2019â€“2021 | Reducing Risk, Promoting Resilience. he Canadian Centre for Cyber Security (Cyber Centre) is Canadaâ€™s authority on cyber security. As part of the Communications Security Establishment (CSE), the Cyber Centre is a growing organization with a rich history. The Cyber Centre brought operational security experts from across the Government of Canada under one roof. In line with the National Cyber Security Strategy, the Cyber Centre represents a shift to a more unified approach to cyber security in Canada.Â CSEâ€™s foreign intelligence mandate provides us with valuable insights into adversary behaviour in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements. ASSESSMENT PROCESS. This article analyses policy response to cyber security issues. By comparing U.S. and Canadian responses, the authors conclude that the nature of cyberspace, defined as a public good with market value as well as an offensive and defensive tool, does not correspond with prevailing public policy models. The authors arrive at this conclusion by a chronological review of technological development, an analysis of conventional models, and consideration of existing public policy. Short descriptionÂ By comparing U.S. and Canadian responses, the authors conclude that the nature of cyberspace, defined as a public good with market value as well as an offensive and defensive tool, does not correspond with prevailing public policy models.