International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors

Matthew E. Castel[*]

INTRODUCTION

Cyber attacks, also called computer network attacks, are one of the greatest threats to international peace and security and global economic prosperity given their potentially catastrophic consequences. Canada and the United States of America are particularly vulnerable to cyber attacks as they depend on a large bandwidth running through their respective societies. In the absence of a global agreement on the legal nature of cyber attacks, a majority of states are "leveraging the Internet for political, military, and economic espionage activities".[1] As a result, cyber attacks have become one of the hottest topics in international law.

When carrying out a cyber attack, state or non state hackers use "logic bombs"[2] and "trap doors" also called "Trojan horses"[3] to place virtual explosives in computers. Thus, laptops can replace bombs and bullets and become potential

---

* Hons BA in international development, with distinction, U of Western Ontario; Certificate of International Affairs and Multilateral Governance, Geneva Graduate Institute of International Law and Development Studies; BCL/LLB candidate, teaching assistant, Faculty of Law, McGill University, Montreal; student at Fasken Martineau Dumoulin LLP, Montreal.

1 McAfee, *Virtual Criminology Report* (2008), in J Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media Inc, 2009) at 1.

2 A software application or a series of information that causes a system or network to shut down or erase all data or software on the network.

3 Hackers add unauthorized software to a program to enter into a network or software program. After entry, they leave behind a trapdoor into the million lines of a computer code running, for instance, an air defense program to facilitate access to it. The trapdoor could be instructions on how to respond to certain circumstances or a program that would cause all the computers on the network subject of the attack to crash and be unable to reboot. Preprogramming the flood of Internet traffic to crash or jam the network (called Distributed Denial of Service-DDOS) has already occurred on a number of occasions domestically and internationally. Attacking computers are called botnets or zombies under remote control thus following instructions loaded into them by state or non-state actors without the knowledge of their owners, sometimes months before the attack when the owners went to a webpage or opened an email as nothing appears on their screens. The botnets/zombies may also spread the infection to other computers which in turn do the same. This is called a worm which may quickly infect millions of originating computers around the world. The botnets/zombies distribute the attack over these computers acting in unison. Note that malicious software like viruses, worms, logic bombs, trapdoors, phishing scams (tricking an Internet user to provide information), etc are called malware.

weapons of mass destruction since hackers can "key in" devastation. For instance, within fifteen minutes a sophisticated or terrorist cyber attack against the United States or Canada could shut down all the systems of the U.S. Air Route Traffic Control Centers or the Area Control Centers of NAV Canada, wipe out all the financial data in the financial computer centers of New York or Toronto, provoke a nation-wide blackout, cause train derailments or damage nuclear plants, etc. In other words, the attack would bring the United States or Canada to a standstill causing millions of its citizens to perish and major other industrial and economic damage.[4]

Deterrence is not very effective to control cyber attacks due to their nature, the speed at which they move, the difficulty in tracking them reliably and the fear of the asymmetrical effects that retaliation could have on North American networks due to their vulnerability. Other means must be found to prevent such attacks or respond to them.

This essay, which contains a broad ranging overview of several important issues raised by the recent number of cyber attacks in Canada and elsewhere, begins with a definition of cyberspace and cyber war. It is followed by a brief survey of some cyber attacks that have occurred in Canada and elsewhere in recent years. The first part addresses the question whether present rules of international law applicable to armed attacks using kinetic weapons apply to the wide notion of cyber attacks by a state actor against the government and critical civilian infrastructures of another state and concludes that they do. However, some grey zones still exist which need to be clarified. Not all cyber attacks are of the same gravity and present international law rules were adopted before the age of the Internet. Today, states that are more dependent on highly advanced technology are subject to greater risks and in turn demand greater protective measures.

The last part of the essay is concerned with cyber attacks as cyber crimes when carried out by non-state actors, mostly from a Canadian law point of view.

The conclusion lists a number of proposals to address the present dangers posed by cyber attacks on the international and Canadian levels.

I. DEFINITION OF CYBER-SPACE AND CYBER WAR

Cyberspace is an electronic terrain that does not occupy any physical space. However, it is submitted that the borderless nature of cyberspace should not prevent states from exercising jurisdiction over a cyber attack and its actor since ultimately a cyber attack will control physical processes. The fact that cyberspace is everywhere there is a computer or a processor or a cable connecting to one means that physical space cannot be ignored. The perpetrator and the target of a cyber attack, whether a state or an individual or entity, will frequently be located in one state and the effects of such an attack may be felt on the territory of another state. In other words: "territoriality still turns out to be a prime factor; apparently cyber-

---

4 J Markoff et al, "In Digital Combat, U.S. Finds No Easy Deterrent", *New York Times* (25 January 2010) online: <http://nytimes.com/2010/01/26/world/26cyber.html?d pagewanted=all>.

space is not considered so a-territorial after all."[5]

In the United States, a Bill entitled *Protecting Cyberspace as a National Asset Act*[6] defined cyberspace as follows:

> The term "cyberspace" means the interdependent network of information infrastructure, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

This is a definition which includes physical processes that take place or may have an effect within the territory of a particular state, be it the actor or the target of a cyber attack. Cyberspace is not limited to a state's jurisdiction over its territory and its citizens. Thus, it would seem that, in the international context, physical space is still relevant in the case of a cyber attack, especially with respect to the location of the originating actor and where the effects on the targeted state are felt.[7] The Internet is a medium used by individuals located in physical space to communicate to individuals also located in physical space. Since the Internet traffic often travels through a number of servers located in foreign physical space, the integrated and global nature of this traffic increases the potential for multiple domestic or foreign jurisdictions claiming control over it on the basis of the territorial principle.

On the international level, cyber war has been defined as "the art and science of fighting without fighting and defeating an opponent without spilling blood."[8] It takes the form of a cyber attack, an act by the organs or agents of a state which, by using different types of malware, penetrates the computers, networks or websites of another state, to affect negatively the political, military or economic situation existing in that other state even if it is not preceded or accompanied by military force. Its purpose is to cause damage or destruction.

This type of cyber attack does not fit exactly the traditional description of the use of force or an act of war which is "a hostile contention by means of *armed forces*, carried on between nation states",[9] using kinetic weapons. However, re-

---

5 Bert-Jaap Koops & Susan Brenner, *Cybercrime and Jurisdiction: A Global Survey* (The Hague: TMC Asser Press, 2006) at 6. Also JL Goldsmith, "The Internet and the Abiding Significance of territorial Sovereignty" (1998) 5 Ind J Global Stu 475.

6 2010, S 3480, s 3 Definitions (3). This bill never became law. See also the definition given by R A Clarke & R K Knake, *Cyber War* (New York: Harper — Collins, 2010) at 70: "Cyberspace is all of the computer networks in the world and everything they connect and control. It includes the Internet plus lots of other networks of computers that are supposed to be accessible from the Internet." Placing a logic bomb on the computers of your enemy in cyberspace is like placing a physical bomb on the physical territory of this enemy.

7 See below, III(c) Attribution of Conduct to a State.

8 Carr, *supra* note 1 at 2. See also the more technical definition given by Clarke & Knake, *supra* note 6: "Cyber warfare is the unauthorized penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls."

9 *Black's Law Dictionary*, 6th ed (St Paul, Minn: West Corp, 1991) at 1583, "war" italics added.

cently, the U.S. Government decided to categorize a cyber attack as an act of war enabling the president to consider imposing economic sanctions, resorting to cyber-retaliation and even, as a last resort, ordering a military strike against the actor state if key U.S. computer systems were attacked. According to the U.S. Department of Defence, without question, some activities conducted in cyberspace could constitute a use of force and may well involve a state's inherent right to lawful self-defence."[10]

When the author of the attack is a private individual or entity or a terrorist group using networks, computers, and applications to cause, for instance, a "Distributed Denial of Service," it would not be appropriate to call the cyber attack an act of war. The response would have to be different.

II. RECENT HISTORY OF CYBER ATTACKS

Cyber attacks as a form of non-conventional weaponry are of recent origin. In 1991, when the war against Iraq began, the United States and its allies used the Internet to reach and demoralize Iraqi officers and soldiers and instruct them how to surrender before the conventional attack by the United States air force. This can be considered to be one of the first instances of cyber warfare, akin to the sending

---

10 Department of Defense Cyberspace Policy Report, A Report to Congress pursuant to the *National Defense Authorization Act* for Fiscal Year 2011, Section 934, November 2011, at 9, at para 12, online: <http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf>. Also President Obama's National Security Strategy (17 May 2010), online: <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>; The U.S. position was to some extent established by NATO at the November 2010 Lisbon Summit: <http://www.nato.int/Lisbon2010/strategic-concept-2010-eng.pdf>; U.S. International Strategy for Cyber Space (May 2011), online: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>; U.S. Department of Defense, Strategy for Operating in Cyber-Space (July 2011), online: <http://www.defense.gov/news/d20110714cyber.pdf>, which proposes five strategic initiatives to operate effectively in cyberspace, defend national interests and achieve national security objectives. Note that in March 2011, before the NATO-led strikes against Libya, the Obama administration considered whether to begin intervention in support of the rebels by a cyber attack to disrupt and disable the Quaddafi government air defense system. After an intense debate, it was decided to reject cyber warfare for fear of setting a precedent for other nations especially Russia and China. See E Schmitt & T Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya", *New York Times* (17 October 2011), online: <http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html>. Eventually, the U.S. will have to cross the threshold into overt cyber attacks to defend vital government, military and public infrastructure networks. Also T Shanker, "U.S. Weighs Its Strategy on Warfare in Cyberspace", *New York Times* (18 October 2011), online: <http://www.nytimes.com/2011/10/19/world/africa/united-states-weighs-cyberwarfare-strategy.html>. Presently, there are no specific rules of engagement to guide individual digital operations. Defensive missions might cross the line into offensive actions when applied to the digital domain. This does not mean that active defense is offensive in cyberspace. An active defense in cyberspace seeks to identify and even neutralize threats before they materialize.

of propaganda radio messages or dropping leaflets in World War II.

In 2007, the Israeli air force destroyed a nuclear facility being built in Syria by North Koreans, on the ground that its purpose was to produce weapons of mass destruction eventually to be used against Israel. The attack was successful in spite of a state of the art air defence radar and missile system built by the Russians. Having hacked into the Syrian defense system and disabled it using light and electric pulses to transmit and control what these radars saw, the Israeli planes were able to penetrate Syrian airspace undetected. In this case, the cyber attack was followed by a conventional military attack using kinetic weapons.

Another example of the use of cyberspace for political objectives but without the use of military force was the case of Estonia which, in 2007, had moved the bronze statue of a Soviet soldier commemorating the liberation of the country in 1945. This move prompted hackers to attack the servers supporting the most used web pages in Estonia by flooding them with simple access requests, thereby collapsing or shutting them down. Access to online banking websites or other electronic services like servers running the telephone network became impossible. The attack lasted for weeks. This "Distributed Denial of Service" attack instantly became a major weapon in the cyber arsenal. Eventually, the attackers were traced to Russia, although this state denied that it was engaged in a cyber war against Estonia and maintained that the attack was done by individual Russian nationalists who were incensed by the act of Estonia. As a result, in 2008 NATO opened a Cyber Defense Center of Excellence in Estonia to deal with cyber wars.

The same year, on the occasion of the invasion of the Republic of Georgia by Russia, cyber attacks took place against Georgian media outlets and government websites. As a result Georgians could not connect to any outside news or send or receive emails. Again, Russia denied that the cyber attacks were the work of its official agents.

In 2009, North Korea sent a coded message to about 40,000 computers around the world which became infected with a botnet virus. The message instructed the computers to ping a number of U.S. and South Korean government websites and international companies. With the zombie computers joining the attack, these sites became flooded with requests to see their pages and eventually these attacks resulted in another "Distributed Denial of Service." In the United States, sites of the Treasury, the Secret Service, the Federal Trade Commission, the NASDAQ, and the New York Stock Exchange, among others, were hit. Eventually, more than 160,000 computers in 74 countries attacked South Korean banks, government agencies and other vulnerable sites. The attacker did not attempt to control any government system or essential services. North Korea denied being the author of these cyber attacks. Even if North Korea was directly involved, it is debatable whether such attacks could be considered as acts of war as psychological pressure and threats are made every day in international relations between hostile states.

In June 2010, a computer worm called STUXNET was configured in such a way as to specifically make uranium enriching centrifuges in Iran spin out of control and shut down.[11] This was a covert cyber operation designed, perpetrated or

---

11 The STUXNET worm moved from computer to computer via Windows security vulnerability allowing it to infect computers not normally connected to the Internet. It

sponsored allegedly by Israel and the United States of America in order to destabilize Iran's controversial nuclear enrichment program. A similar attack took place again in 2011 using a different worm.

In the winter and spring 2011, there were several separate cyber attacks against Canadian government ministries such as the Treasury Board of Canada Secretariat and the Department of Finance, Canadian law firms involved in a foreign attempt to take over Potash Corporation of Saskatchewan and the U.S. defense contractor Lockheed Martin, apparently originating from hackers in China or Russia.

In 2009, as a result of a cyber attack against the computers of the U.S. Military Central Command, a United States Cyber Command was created by the Department of Defense as a sub-unified command of the U.S. Strategic Command with the mission to use information technology and the Internet as a weapon and also to defend the Department of Defense.[12] The Department of Homeland Security defends other parts of the federal government. Although this may change as a result of the new U.S. National Security Strategy, so far no federal agency is charged with the defense of the power grid, the banking system or the transportation networks from a cyber attack on the ground that it is the responsibility of the private sector to do so. Other states like Russia,[13] China,[14] North Korea,[15] France[16] and Israel[17] also created cyber warfare commands. The Canadian military lacks a formal Cyber Command although at the present Communications Security Establishment Canada, a division of the Department of National Defense monitors international Internet communications to protect Canada's electronic network. In 2010, the Canadian Government launched Canada's Cyber Security Strategy designed to protect from hackers certain Canadian assets like the power grid and government departments.[18]

---

disabled 10% of the centrifuges. John Markoff, "Malware Aimed at Iran Hit Five Sites, Report Says", *New York Times* (11 February 2011), online: <http://www.nytimes.com/2011/02/13/science/13stuxnet.html>. Also Matt Liebowitz, "Stuxnet Clone 'Duqu' Possibly Preparing Power Plant Attacks", (18 October 2011), online: <http://www.foxnews.com/scitech/2011/10/18/stuxnet-clone-found-possibly-preparing-power-plant-attacks/>.

12 See online: <http://enwikipedia.org/wiki/united_ states_cyber_command>.

13 A Russian Cyber Command, online: <ieexplore.ieee.org/xpls/abs_all.jsp?arnumber=5954699-Similar>.

14 Cyber warfare units created by China are responsible for offense and defense in cyberspace. Among the many weapons and techniques used, are information mines and logic bombs, changing network data, establishing network spy stations to monitor Internet traffic, degrading and shutting down computer and critical foreign infrastructure systems. Hacking against United States, European and Japanese industries and research facilities is also another activity pursued diligently by the Chinese government.

15 Note that Unit 121 of the [North] Korean People's Army Joint Chiefs Cyber Warfare specializes in destabilizing South Korea' Military Command Control and Communication Network. It operates mostly from China because the few North Korea Internet connections can easily be identified.

16 Online: <www.intelligenceonline.com/. . ./cyber-command-for-french-military.91319142-ART-Similar>.

17 Online: <http://www.ynetnews.com/articles/0.7340.L-4070561>.

18 See online: <http://www.publicsafety.gc.ca/prg/ns/cbr-scc-eng.pdf>.

In May 2011, the U.S. Government prepared an international cyber defense strategy, which is not limited to a cyber-response. All necessary means as appropriate and consistent with applicable international law would be used to respond to hostile acts in cyberspace, especially with respect to cyber attacks that threaten widespread civilian casualties.[19]

The infrastructures of a state subject to a cyber attack usually involve its military, transportation system, electric energy, gas and oil storage and delivery, banking and financial sector services, water supplies, telecommunications, and emergency services. These infrastructures are particularly vulnerable to a cyber attack, given their reliance on integrated computer technologies.[20] Most destructive, would be the initiating of a nuclear catastrophe by a hacker attack, especially by a terrorist, on nuclear power plants or on the command and control of nuclear weapons.

III. CYBER ATTACK BY A STATE ACTOR AGAINST GOVERNMENT OR CRITICAL CIVILIAN INFRASTRUCTURES OF ANOTHER STATE WITHOUT PRECEDING OR ACCOMPANYING USE OF KINETIC FORCE

(a) Cyber Attack by a State as a Use of Force which Amounts to a Breach of the Peace or an Act of Aggression

Is a cyber attack by an organ or agent of a state or its sponsored terrorist organization, not preceded or accompanied by the use of kinetic force in the physical world, an act prohibited by international law (e.g. the *Charter of the United Nations*, the 1974 *Definition of Aggression* by the General Assembly of the United Nations,[21] the 2010 amendment to the *Statute of the International Criminal Court* which now defines aggression,[22] and the 1970 United Nations *Declaration on Prin-*

---

19 *Supra* note 10. Also *supra* note 10, Department of Defense Strategy for Operating in Cyberspace (July 2011). In the USA see two competing bills in the Senate namely the *Cybersecurity Act of 2012*, s. 2105 introduced Feb. 14, 2012, <http://www.govtrack.us/comngress/bills/112/s2105> and the *SECURE IT Act of 2012*, introduced March 1, 2012, <http://www.energy.senate.gov/public/index.cfm/2012/3/senators-introduce-legislation-to-strengthen-cybersecurity>. Both bills are designed to buttress the networks for critical US infrastructures, such as electrical power plants and nuclear reactors.

20 In Canada see Office of Critical Infrastructure Protection and Emergency Preparedness created in 2001 and originally located with the Department of National Defense and now integrated within the Public Safety and Emergency Preparedness Canada portfolio which is part of the Department of Public Safety, online: <http://circ.jmellon.com/agencies/ocipep/>. Thus, in Canada public safety covering cyber attacks comes primarily within the jurisdiction of the Department of Public Safety in cooperation with the Canadian Security Intelligence Service, the Royal Canadian Mounted Police, and the Canada Border Services Agency. The Department of Justice Canada and the Department of National Defense are also involved in their respective sphere of jurisdiction.

21 UNGA Res 3314 (XXIX), (14 December 1974), 13 ILM 710.

22 UN Doc A/CONF 183 /9, 17 July 1998. Art 8 bis, adopted in Kampala on 11 June 2010, Resolution RC/Res 6. Depositary Notification CN 651.2010, Treaties -6, dated

ciples of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations).[23]

Some of these instruments can be relied upon to prohibit cyber attacks.

For this purpose, let us assume that the actor of the cyber attack is an organ or an agent of a state that has been identified and that the attack has caused the banking system to grind to a halt or disrupted the transportation system or electrical grid of the targeted state, creating chaos and endangering its economy.

Article 2.3 of the *Charter of the United Nations* lays down the principle that: "All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered." This obligation is reinforced by article 2.4 which declares that: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations." Interpreting article 2.4 liberally, especially the words "restrain . . . from the . . . use of force against the . . . political independence of any state . . .", it would seem that the disruption of the transportation system or the electrical grid, or stopping the banking system of the targeted state would certainly affect its political independence by endangering its economic and financial stability, leaving that state' government at the mercy of other states. On the other hand, a narrow interpretation of the same words would require that the cyber attack be preceded or accompanied by a physical attack with kinetic weapons. Since in the past the *Charter of the United Nations* has been concerned with conventional warfare, it is unlikely that many of its members would agree that a cyber attack is a "use of force" of a kinetic nature. However, the words "refrain . . . from the use of force . . . in any other manner inconsistent with the purposes of the United Nations" could be interpreted to include a cyber attack without the physical component of the use of force especially if one considers article 1.1 of the *Charter*, which deals with the purposes and principles of the United Nations. In the context of a cyber attack, these principles are the prevention and removal of threats to the peace and the suppression of acts of aggression or other breaches of the peace. Also, a cyber attack does not "develop friendly relations among nations" as required by article 1.2.

Furthermore, in determining whether the Charter of the United Nations applies to the threat or use of non-conventional weapons of mass destruction, the International Court of Justice in its advisory opinion on *The Legality of the Threat or Use of Nuclear Weapons*, indicated that articles 2.4, 51 and 42 of the *Charter of the United Nations* do not refer to specific weapons. They apply to any use of force regardless of the weapons used. Thus it could be argued that since "the *Charter* neither expressly prohibits, nor permits the use of any specific weapon",[24] cyber attacks by computers are covered by the words "use of force", "armed attack" or

---

29 November 2010, available online: <http://treaties.un.org>. The amendment will come into force one year after ratification by 30 states parties to the Court which will be able to exercise jurisdiction on this ground at the earliest only after 1 January 2017.

23 UNGA Res 2635 (XXV) UN GAOR 25th Sess, Supp No 28 at 121. UN Doc A/8028 (1971) adopted by consensus on 24 October 1970.

24 [1996] ICJ Rep 226, at para. 39.

"act of aggression".

Article 39 of Chapter VII of the United Nations *Charter* which gives the Security Council the task of determining "the existence of any threat to the peace, breach of the peace, or act of aggression" and making recommendations or deciding what measures must be taken to maintain or restore international peace and security can be interpreted as applying to a cyber attack. Such an attack would be a breach of the peace and even an act of aggression, particularly if one considers the collateral damage which could result from such an attack.

In order to characterize a cyber attack as an act of aggression, one must examine how the international community has defined an "act of aggression". In one of its Resolutions adopted in 1974, the United Nations General Assembly[25] defined aggression in article 1 as ". . . the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the *Charter of the United* Nations, as set out in this Definition." Reference is made to "armed force" in the physical sense. It is consistent with the Preamble of the *Charter of the United Nations* which states that "armed force shall not be used, except in the common interest." This reference to armed force would prevent the characterization of a cyber attack as an act of aggression unless preceded or accompanied by physical force. If that were the case, the use of a cyber attack would fall within the traditional scope of *jus in bello*.

Article 2 of the Definition also refers to the "first use of armed force". Article 3 gives a long list of acts which, regardless of a declaration of war, qualify as an act of aggression. All the acts listed in paragraphs (a) to (g) of article 3 describe physical attacks by "armed forces", which would further eliminate a cyber attack from the definition of aggression. Yet, article 4 leaves the door open to extending this definition to include cyber attacks since it declares that: "The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter."

The *Statute of the International Criminal Court*[26] listed the crime of aggression in article 5.1(d) but did not define it in 1998 when the Court was created. However, in 2010, article 8 bis was added to this statute which now defines the crime of aggression as

> the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a state, of an act of aggression which, by its character, gravity and scale constitutes a manifest violation of the *Charter of the United Nations*.

Paragraph 2 of the new article then defines an "act of aggression" as

> the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations. . . .

This is followed by a list of acts of aggression similar to those described in article 3 of the 1974 Resolution. Crimes of aggression will only be prosecuted after

---

25 *Supra* note 21. For a comprehensive analysis and comments by the Canadian Delegation see JG Castel, *International Law*, *Chiefly as Interpreted and Applied in Canada*, 3d ed (Toronto: Butterworths, 1976) at 57–63.

26 *Supra* note 22.

the Security Council has made a determination that an act of aggression has been committed. In article 8, which covers war crimes and contains a long list of these crimes, reference is always to a physical "armed force" which would rule out a cyber attack. Thus, articles 8 bis and 8 do not comfortably apply to cyber attacks.

The *Declaration of Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations*[27] was drafted in a pre-computer age. Reference is made to the "use of force" against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purpose of the United Nations, repeating what appears in article 2.4 of the *Charter of the United Nations*.

To conclude, the most important international text provisions that support the view that a cyber attack by a state is a "use of force" that is a threat to the peace, a breach of the peace or an act of aggression that gives jurisdiction to the Security Council to apply the measures found in Chapter VII of the *Charter of the United Nations* are articles 2.4 and 39 *et seq.* of the *Charter*. However, whether a cyber attack could be considered a violation of the *Charter* would depend upon its character, gravity and scale. Not all cyber attacks would qualify.

To put this matter to rest the Security Council could add cyber attacks to the list of acts of aggression in article 3 of the 1974 *Definition of Aggression*.

(b) International Law of State Responsibility for Internationally Wrongful Acts

Another possible avenue for holding a state responsible for a cyber attack that is not preceded or accompanied by the use of kinetic force is the customary international law of state responsibility that "Every internationally wrongful act of a State entails the international responsibility of that State."[28]

According to the *Draft Articles on State Responsibility* "There is an internationally wrongful act of a State when conduct consisting of an action or omission (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State."[29] Depending on the context, a cyber attack by the organ or agent of a state, or by a terrorist organization sponsored by a state, may amount to a breach of the international obligations that states have not to harm one another.[30] That obligation attracts the state's international responsibility, as for instance in the case of a "Distributed Denial of Service."

To remedy this situation, the targeted state would be able to resort to self-help measures, such as reprisals,[31] distinct from those listed in Chapter VII of the *Charter*, which would not be applicable in the absence of proof that the attack amounted to the "use of force", an "armed attack", or an act of aggression. However, the state

---

27 *Supra* note 23.

28 Art 1, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Report of the International Law Commission on the Work of its 53rd Sess, UNGAOR, 56th Sess, No 10 UN Doc A/56/10 [*Draft Articles on State Responsibility*].

29 *Ibid* art 2.

30 *Corfu Channel Case*, *United Kingdom v Albania (Merits)*, [1949] ICJ Rep 4 at 2224.

31 Below, V(f) Reprisals — Countermeasures.

responsible for the cyber attack would be under an obligation to: "(a) cease that act, if it is continuing; and (b) to offer appropriate assurances and guarantees of non-repetition, if circumstances so require",[32] and to compensate the targeted state for the damages caused thereby.[33]

(c) Attribution of Conduct to a State

To hold a state responsible for a cyber attack it is necessary to determine where the attack originated. The clandestine nature of cyberspace makes this difficult, especially when the cyber attack is conducted through intermediate computer systems to disguise the identity of the attacker. The more an attacker routes the attack through intermediary systems, the more difficult it is to trace the attacker's identity.[34] Yet, the identification of the attacker state is a legal requirement before the targeted state can decide how to respond.

Can a cyber attack using local or foreign servers be attributed to the state when the attack is carried out by government organs, by others who have acted under the direction, instigation or control of these organs as agents of the state, by a terrorist organization or by an individual terrorist sponsored or tolerated by that state? A state is responsible for its organs or agents acting as hackers provided that they have that status under the domestic law of that state.[35] To trigger the international responsibility of the state, the cyber attack must result from the active participation of these organs or agents under cover of their official character. However, the state cannot invoke an excess of authority by its organs or agents to block a claim by the state targeted by the cyber attack.[36]

A state that has sponsored or tolerated a cyber attack by a terrorist organization or an individual terrorist may violate article 2.4 of the *Charter*[37] if the attack meets the threshold for the use of force. It would also violate conventions dealing

---

32 *Supra* note 28 at art 30.

33 *Ibid* art 36.

34 Trace back software can be used to find the origin of the attack. However, some servers may not co-operate. If that is the case, hacking into these servers could help unless the actor directed the attack from a server located in another state which could be that of the target!

35 *Draft Articles on State Responsibility*, *supra* note 28 arts 4-5.

36 *Ibid* art 7.

37 See UNSC Res 748 (1992), 31 March 1992, UN Doc S/RES/748 involving Libya and the aerial incidents at Lockerbie and in Niger (1992), 31 ILM 717: "The Security Council . . . Reaffirming that, in accordance with the principle in Article 2, paragraph 4 of the Charter of the United Nations, every State has the duty to refrain from organizing, instigating, assisting or participating in terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when such acts involve a threat or use of force." Since on several occasions, the members of the Security Council have expressed their deep concern over acts of international terrorism and emphasized the need for the international community to deal effectively with all such acts, they would probably be prepared to condemn a state sponsoring a cyber attack by a terrorist organization. UNSC Res 1373, para 2, 28 September 2001, UN Doc S/RES/1373.

with terrorism and the customary international law rule that a state has a duty "not to allow knowingly its territory to be used for acts contrary to the rights of other states."[38] Furthermore, according to paragraph 1 of the *Declaration of Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations*,[39]

> Every State has the duty to refrain from organizing, instigating, assisting or participating in . . . terrorist acts in another State nor acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.

It is doubtful that an act of cyber terrorism could also be an act of aggression under article 3(g) of the 1974 *Definition of Aggression*[40] and article 8 bis 2(g) of the *Statute of the International Criminal Court*.[41] Although these rules and principles were adopted before the advent of the Internet, they should be extended to include this type of cyber terrorism. Targeted states would then be able to respond in self-defence.

The conduct of the terrorist organization will be attributed to the state sponsoring or tolerating it if "the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State."[42] The degree of control required in order for the cyber attack to be imputable to the state is that of effective control over the terrorist organization, which may not often be the case.[43] In *Prosecutor v Dusko Tadic*[44] the International Tribunal for the former Yugoslavia held on appeal that where a state has a role in organizing, coordinating and providing support for a group, it has sufficient overall control for the acts of the group to be attributable to the state.

States that have not sponsored terrorists involved in a cyber attack against the targeted state, but are hosting them, may become sanctuary states by failing to track them down and prevent further attacks.[45] Is this sufficient to make the sanctuary

---

38 *Corfu Channel Case*, *supra* note 30 at 22.

39 *Supra* note 23.

40 *Supra* note 21.

41 *Supra* note 22.

42 *Draft Articles on State Responsibility*, *supra* note 28 art 8.

43 *Military Activities In and Against Nicaragua*, *Nicaragua v United States of America (Merits)*, [1986] ICJ Rep 14 at paras 113–115 [*Military Activities in and against Nicaragua*] where the issue was whether the acts of the Contras could be imputed to the United States of America. D Jinks, "State Responsibility for the Acts of Private Armed Groups" (2003), 4 Chicago J Int'l L 83.

44 IT-94-1-A,; (1999), 38 ILM 1518 at 1541, at para. 117.

45 See UNGA Res 55/63, UN Doc A/RES/55/63, 22 January 2001. UNSC Res 1368 at para 3, UN Doc S/RES/1368, 12 September 2001; UNSC Res 1373, UN Doc S/RES/1373, 28 September 2001. Responsibility of the Taliban when they were in power for harboring and protecting Al Qaeda for their conduct with respect to 9/11. Note that Bill C-10 tabled in the House of Commons of the Canadian Parliament on 20 September 2011 and entitled the *Safe Streets and Communities Act*, contains in Part I the *Justice for the Victims of Terrorism Act*, ss 4–9, which, when passed by the Senate

state a legitimate target of action taken by the victim state in self-defence as was the case with the invasion of Afghanistan by the U.S. after 9/11? First, it would be necessary to establish the gravity of the conduct in order to determine whether an "armed attack" took place against the targeted state. If so, could the conduct of the terrorists be attributed to the host state or, in the alternative, could the host state be responsible for failing to have prevented such attack? The host state would have to be substantially involved in the attack to be held responsible.[46]

(d) Resort to Self-Defense

According to article 51 of the *Charter*:

> Nothing in the present *Charter* shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security . . .[47]

For the targeted state to resort to self-defence, the cyber attack by a state actor would have to be characterized as an "armed attack". There is no definition of an "armed attack" in any provision of the *Charter* or other international document. However, it is generally accepted that the use of force is an "armed attack" when it is of sufficient scope, duration and intensity.[48] Does a cyber attack qualify as a "use of force" similar to an armed attack? The 1974 *Definition of Aggression*[49] requires the first use of force and its consequences to be of "sufficient gravity" before it is considered an "armed attack". An unconventional use of force like a cyber attack could be considered equivalent to an "armed attack" when its scope, duration and intensity are of sufficient gravity. Several approaches can be used for this purpose:

(2d reading and in Committee at the time of writing), is designed to deter terrorism by creating a cause of action that "allows victims of terrorism to sue their perpetrators and their supporters" (s 3). This legislation will cover states supporting terrorists involved in cyber attacks. For this purpose, the proposed Act amends the *State Immunity Act* (RSC 1985 c S-18) to prevent a foreign state from claiming immunity of jurisdiction when being sued in Canada by a victim of terrorism arising from actions that are related to the support of terrorism. Will this legislation violate international law rules pertaining to immunity of states? Such a suit will also raise some interesting issues of private international law.

46 *Military Activities In and Against Nicaragua*, *supra* note 43 at para 195.

47 Note that art 21 of the *Draft Articles on State Responsibility*, *supra* note 28, declares that: "The wrongfulness of an act of a State is precluded if the act constitutes a lawful measure of self-defence taken in conformity with the Charter of the United Nations."

48 It has been suggested that six criteria define an "armed attack", namely severity, immediacy, directness, invasiveness, measurability and presumptive immediacy. See M Schmitt, "Computer Network Attack and the Use of Force in International Law" (1999) 37 Colum J Transnat'l L 885 at 913–15.

49 *Supra* note 21 art 2. However, see US Letter to the President of the UN Security Council (7 October 2001) UN Doc S/2001/946 with respect to action against the Taliban regime in Afghanistan after 9/11: The armed attack need not emanate from another state to give rise to a right of self-defense. See also *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, (9 July 2004) Advisory Opinion, ICJ Rep 136.

whether the damage caused by a cyber attack previously could have been achieved only with a physical attack (instrument based approach); whether the cyber attack had an overall disruptive effect on the victim state (effects based approach); and, automatically treating a cyber attack on infrastructures as an "armed attack" (strict liability approach). The effects based approach takes the others into account.[50] If in certain circumstances the US categorization of a serious cyber attack by a state actor as an act of war is accepted by the international community, it would be a "use of force" similar to a traditional "armed attack", which could justify acts of self-defence including a kinetic response on the part of the targeted state.[51] Furthermore, since the provisions of the *Charter* "do not refer to specific weapons, they apply to any use of force regardless of the weapons employed".[52] A computer used to carry out a cyber attack is a weapon that makes an attack an "armed attack".

(e) Pre-emptive Self-Defence

Article 51 is limited in its extent, but the existence of a right to resort to pre-emptive self-defence independently from the *Charter* has been recognized by customary international law and used on a number of occasions. It is based on the inherent and natural right of a state to self-preservation in the face of a serious and imminent threat to its national security.[53] As opposed to article 51 no actual "armed attack" has to take place before pre-emptive self-defence can be used. In the 2003 invasion of Iraq, the United States of America went a step further and argued that a state can act in preventive or anticipatory self-defence against not just an immediate proximate threat but even against a non-imminent or non-proximate, but still real threat, especially in case of sponsored terrorism. According to JG Castel, the "concept of imminent threat relevant to pre-emptive self-defense had to be adapted to the capabilities and objectives of today's adversaries."[54] Thus, when a state is expecting a cyber attack or an armed attack even in the distant future, it could resort immediately to measures of self-defence to remove the potential future threat. The recent cyber attacks against Iranian nuclear installations, allegedly by Israel and the United States of America, to prevent a potential Iranian nuclear kinetic

---

50 Carr, *supra* note 1 at 59.

51 *Supra* note 10. See Department of Defense Cyberspace Policy Report, *supra* note 10 at paras 11, 12: "Without question, some activities conducted in cyberspace could constitute a use of force, and may well invoke a state's inherent right to lawful self defense."

52 *The Legality of the Threat or Use of Nuclear Weapons*, *supra* note 24 at para 39. See also discussion in Section V(a) below.

53 See the *Caroline Case*, *United Kingdom v United States of America*, 2 Moore's Digest of International Law 409 at 412, preventive action in a foreign territory is justified only in case of "an instant and overwhelming necessity or self-defence, leaving no choice of means and no moment of deliberation." See also *Military and Paramilitary Activities In and Against Nicaragua*, *supra* note 40 at paras 102-103.

54 JG Castel, "The Legality and Legitimacy of Unilateral Intervention in an Age of Terror, Neo-Imperialism, and Massive Violations of Human Rights: Is International Law Evolving in the Right Direction?" (2004), 42 Can YB Int'l L 3 at 13. See also *A More Secure World: Our Shared Responsibility*, 29 November 2004, UN Doc A/59/565, at paras 188–194.

attack on Israel, is a case in point. Yet, since Iran is a party to the *Treaty on the Non Proliferation of Nuclear Weapons 1968*[55], suspicion of the production of nuclear weapons may not justify disrupting its nuclear program by a cyber attack.[56] However, if it is widely accepted by the international community so as to become customary international law, the concept of non-proximate threat could justify the alleged Israel/U.S. cyber attack against Iran in spite of the 19 June 1981 Security Council Resolution condemning Israel for its armed attack on the Iraqi Nuclear Research Centre.[57]

Self-defence against a cyber attack may take the form of active self-defences such as a counter cyber attack on the infrastructures of the attacking state or electronic countermeasures designed to strike attacking computer systems and shut down cyber attacks mid-stream. Passive self-defences to defend computer networks such as system access or data controls, security administration and a secure systems design are not measures of self-defence *stricto sensu*, since they do not breach the normal prohibition against the use of force.

The difficulty is attributing to a particular state or its agents a cyber attack in progress in order to respond with active defences. To qualify as legitimate self-defence the response to a cyber attack must meet the criteria of necessity, proportionality and immediacy.[58]

In light of the recent U.S. categorization of cyber attacks as acts of war and the declaration that, depending upon the circumstances, military means using kinetic weapons may be used as self-defence to respond to such attacks, the first "armed" attack by the U.S. in response to a cyber attack would not "constitute *prima facie* evidence of an act of aggression" as prohibited by article 2 of the 1970 *Definition of Aggression*.[59]

(f) Reprisals — Countermeasures

Reprisals, also called countermeasures, which are taken by a state whose rights have been violated by another state, are unlawful but may be justified if they meet certain conditions. If a cyber attack falls short of the "armed attack" threshold required for the application of article 51 of the *Charter*, the targeted state can still

---

55 729 UNTS 161, (1968), 7 ILM 811, 1970 CanTS 1970 No 7.

56 In a non-cyber attack context see UNSecurity Council Resolution 487 (19 June 1981) UN SCOR, 36th Year Res and Docs 10, UN Doc S/INF/37 (1982), which unanimously condemned the military attack by Israel on the Iraqi Nuclear Research Centre as in clear violation of the Charter of the United nations and the norms of international conduct. See also Security Council Debate (12 June 1981), UN Doc, S/PV 2280, reprinted in (1981) 20 ILM 965. Iraq was a party to the Treaty on the Non Proliferation of Nuclear Weapons, *supra* note 55.

57 *Ibid.* Also Memorandum from the Legal Bureau of the Department of External Affairs (27 November 1981), (1982), 20 Can YB Int'l L 303.

58 See *Military Activities In and Against Nicaragua*, *supra* note 43 at paras 96-97. Note this case also analyzes the concept of collective self defense mentioned in art 51 of the Charter of the United Nations; Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons*, *supra* note 24 at 822.

59 *Supra* note 21.

resort to countermeasures against the state which launched the attack.[60] However, prior to taking countermeasures, the targeted state must have asked the actor of the cyber attack to discontinue the attack or make reparation and the actor must have failed to do so.[61] This is unrealistic due to the nature and speed of a cyber attack. The countermeasures must also be proportionate to the gravity of the attack and could include the use of a limited cyber counter-attack although it need not mirror the initial violation.[62] Finally, the countermeasures cannot be of a military nature as they would constitute a violation of articles 2.4 and 51 of the *Charter*.[63]

(g) Conduct of Cyber War

What would be the legal consequences if a cyber attack, as an act of cyber war by a state actor, were to be considered equivalent to the "use of force", the use of "armed force" or "an armed attack" in physical space allowing the targeted state to use kinetic weapons in response? In 1907 at The Hague, it was agreed that "the right of belligerents to adopt means of injuring the enemy is not unlimited."[64] Several more recent international conventions may also be relevant as a model for banning cyber war. For instance, the 1980 Convention on *Prohibition or Restriction on the Use of Certain Conventional Weapons and Protocols*[65] which serves as an umbrella for protocols dealing with specific weapons, such as mines, could be the object of a new protocol dealing with cyber attacks. The *Geneva Conventions for the Protection of War Victims* of 1949, especially *Convention IV Relative to the Protection of Civilian Persons in Time of War*[66] and the *Additional Protocols I*[67] and *II*[68] to this Convention adopted in 1977, and some articles of the *Statute of the International Criminal Court* of 1998[69] could also be relevant.

If a cyber attack is considered to be an act of war, a state using kinetic force in response has to respect the *jus in bello* principles of distinction, humanity, necessity and proportionality. These principles require that a distinction be made by the belligerents between the civilian population and combatants and only the latter are

---

60 *Draft Articles on State Responsibility*, *supra* note 28 art 49.

61 *Ibid* art 52.

62 *Ibid* art 50.1(a).

63 *Ibid* art 50. See also Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, *supra* note 23.

64 Hague Convention No IV Respecting the Laws and Customs of War on Land and Annex (Regulations), (18 October 1907) US Stat 2277, 1 Bevans 631.

65 See online: <http://www.un.org/millennium/law/xxvi-18-19.htm> and <http://treaties.un.org/doc/publications/UNTS/volume%202041/v.2041.pdf>. See also the Hague Convention No IV, *supra* note 64.

66 (1950), 75 UNTS 287.

67 (1977), 1125 UNTS 3. Note that art 36 requires a state adopting or developing a new weapon first to determine whether or not it is prohibited by international law. At present, methods of cyber attacks are not prohibited unless they fit within existing international conventions. Therefore, it is unlikely that a laptop is a prohibited weapon.

68 (1977), 1125 UNTS 609.

69 UN Doc A/CONF/183/9, 17 July 1998, arts 5–8.

targeted. The proportionality test weighs the use of force against the possibility of incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof. The use of weapons designed to cause unnecessary suffering is also prohibited. The amount of force to be used against a legitimate target is limited to the amount necessary to accomplish a valid military objective. The use of force must not be "excessive in relation to the concrete and direct military advantage anticipated"[70] These limitations arise if the use of force can harm civilians.

The use of kinetic weapons to respond to a cyber attack is dangerous and non-effective as well as capable of causing disproportionate collateral damage. It would be better to respond by active defenses such as tracking the attack back to its source immediately and disrupting it.[71] This raises the issue of whether computers are legitimate military objectives. To date cyber attacks have not been considered part of the traditional conduct of war in physical space. However, in light of the new U.S. cyber defence international strategy, a traditional military response to a cyber attack using kinetic weapons should be launched only as a last resort[72] as a matter of policy rather than a legal limitation. A state that has sustained an armed attack is entitled to respond with a use of force, including kinetic and other weapons, provided they are not prohibited by international law. The United States has recognized that "Cyberspace's unique aspects may require clarification in certain areas."[73] This is particularly true with respect to the law of armed conflict.

(h) Electronic Espionage

Spying through hacking without authorization into the networks, computers or data bases of a foreign state or a non-state enterprise to collect sensitive information to which access is denied without adding or altering data, damaging or disrupting the networks or things the networks control in physical space is difficult, if not impossible, to detect when it is done by a state organ that has the means to cover its tracks. This kind of espionage is cheaper, more successful and has fewer consequences than traditional espionage and is not prohibited by international law, although it may be punished by the domestic law of the targeted state.[74] It becomes an international wrong when those who spy upload software packages such as logic bombs to damage or destroy the network they spy upon.

Most of the cyber spying by state organs targets technological information and especially intellectual property rights protected by international conventions. This type of espionage should qualify as an international cyber crime for which the acting state should be held responsible. On the international level it would be most difficult to reach an agreement to limit or ban electronic espionage and enforce such a ban.

---

70 Additional Protocol I, *supra* note 67 art 51(5)(b).

71 Carr, *supra* note 1 at 72.

72 Department of Defense Cyberspace Policy Report, *supra* note 10.

73 *Ibid* at 7-8 paras 9-10.

74 In Canada, see *Security of Information Act*, RSC 1985, c O-5 as am, especially economic espionage, s 19.

(i) The Birth of a New International Customary Law?

The decision by the United States of America in 2011 to categorize a cyber attack by a state as an act of war[75] equivalent to a traditional "armed" attack, the "use of force" or an act of aggression, if accepted and followed by other states could evolve into a new international customary law applicable to cyberspace. This categorization would overcome the present difficulty arising from the fact that the *Charter* and other relevant international instruments were adopted before the age of the computer and are concerned with armed conflict using kinetic weapons in physical space not cyber weapons in cyberspace. In view of the seriousness of the issue, and until such categorization meets the criteria of constant usage and acceptance as a matter of law (*opinio juris*), which could take place within a relatively short period of time, individual states should be able to act outside existing categorizations and be justified when responding to cyber attacks on the ground of self-defence outside the *Charter*.[76] Yet, this may not be necessary if one accepts the declaration by the U.S. in the International Strategy for Cyberspace document that: "Consistent with the United Nations Charter, states have an inherent right to self-defence that may be triggered by certain aggressive acts in cyberspace."[77] This implies that any such aggressive act amounts to an "armed attack" within the meaning of article 51 of the *Charter*. The exponential increase of cyber attacks and their potential catastrophic consequences for the international community require quick action to address this threat. By categorizing such attacks as acts of war, many states and their organs will hesitate to resort to them especially against the infrastructures of other states. The response would have to respect the principles of *jus in bello* and particularly the proportionality requirement.

---

75 *Supra* note 10.

76 See *North Sea Continental Shelf Cases*, [1969] ICJ Rep 3; *Military Activities In and Against Nicaragua*, *supra* note 43 at paras 94–106; *Restatement of the Law Third, Foreign Relations Law of the United States*, (St Paul, Minn: American Law Institute Publishers, 1987) s 102(2). In the context of International Humanitarian Law, see J-M Henchaerts & L Doswald-Beck, *Customary International Humanitarian Law*, 2 vols (Cambridge: Cambridge University Press, 2005) and MM Casagrande *et al*, Canadian Red Cross, delivered at the International Conference on Customary International Humanitarian Law: challenges, practices and debates, Montreal, Panel 1; *Origin and conclusions of the IRRC study on customary international humanitarian law* (29, 30 September & 1 October 2005). It could be argued that until a formal international instrument condemns cyber attacks by a state against the civil infrastructures of another state, by analogy to the Martens clause introduced into the preamble of the 1899 Hague Convention II on the Laws and Customs of War, see online: <http://en.wikipedia.org/wiki/Martens_Clause> and included in the 1907 Hague Conventions, civilian population should remain under the "protection and empire of international law as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience", which for the purpose of establishing a custom banning these attacks would not insist on the requirement of constant usage but emphasize *opinio juris*. See A Cassese, "The Martens Clause: Half a Loaf or Simply Pie in the Sky" (2000) 11 JIL 187.

77 *Supra* note 10 at 10, Basic Norms.

IV. CYBER ATTACK AS A CYBERCRIME BY A NON-STATE ACTOR

(a) Responsibility of States for Cyber Attacks by Non-State Actors

It is well established that: "Ordinarily, a state is not responsible for acts by individuals or other private entities."[78] However, even if a state is not involved directly or indirectly in a cyber attack, it has certain obligations towards the targeted state. There is a duty on its part to prevent such hostile action by private parties when originating from servers and actors located within its physical boundaries. This duty includes preventing the cyber attack and, if that is too late or impossible, attempting to identify the actors, and bringing to justice all those who tried to disrupt or damage the systems of the targeted state. This duty finds support in the general customary international law of state responsibility[79] which holds that:

> In general, a state is responsible for inaction when it fails to carry out some international obligation to act, whether an obligation assumed by international agreement, or one imposed by customary law.[80]

The existence of this custom has been acknowledged on a number of occasions. For instance, in the *Steamship Lotus, France v Turkey* case, Judge John Basset, in a dissenting opinion on another issue, declared that "a state is bound to use due diligence to prevent the commission within its dominions of criminal acts against another state."[81] It also finds support in the *Corfu Channel* case, where the International Court of Justice held that a state has a duty "not to allow knowingly its territory to be used for acts contrary to the rights of other states."[82] In the *U.S. Diplomatic and Consular Staff in Tehran* case, the International Court of Justice reiterated that states are required under international law to take appropriate measures to protect the interests of other states from non-state actors within their territory.[83]

Where the target is not a foreign state but a foreign private individual or entity: "In addition to liability for failure to take appropriate steps to prevent harm to a foreign national, a state may be liable for failure to take steps to punish a violation of such rights."[84] A state cannot avoid liability simply by declaring that the cyber attack is the act of a private party in its territory. The private target, for instance, Visa, in a case of a "Distributed Denial of Service," or a private utility in the case of a cyber attack on its grid, should be able to obtain damages not only from the hacker but also from the state that did nothing to prevent or control such

---

78 *Restatement of the Law Third, Foreign Relation of the United States*, *supra* note 76, s 207, Comment c at 97.

79 Draft Articles on State Responsibility, *supra* note 28 art 2, omission.

80 *Restatement of the Law Third, Foreign Relations of the United States*, *supra* note 76, s 207, Reporter's Notes, 5 State inaction at 99. Also, 1970 Declaration on Principles of Friendly Relations, *supra* note 23.

81 1927 PCIJ (Ser A) No10 at 88.

82 *Supra* note 30 at 22-23.

83 [1980] ICJ Rep 3 at 32-33, 44.

84 *Restatement of the Law Third, Foreign Relations Law of the United States*, *supra* note 78 s 207, Reporters' Notes, 5 State inaction at 99.

attack.

(b) 2001 Council of Europe Convention on Cybercrime

This Convention[85] which entered into force in July 2004 lays down guidelines for all states wishing to adopt legislation against crimes committed via the Internet and other computer networks and to foster international co-operation. It is not concerned with cyber war conducted by the organs or agents of a state. Canada, although not a member of the Council of Europe, signed the Convention on 23 November 2001 and is planning to ratify it as soon as Parliament has adopted legislation implementing all of its provisions.[86] With respect to the subject matter of this essay, the Convention is important to the extent that it covers cyber attacks on computers and computer networks by non-state actors including terrorists.

Article 1 of the Convention contains definitions of 'computer system', 'computer data', 'service provider' and 'traffic data', wide enough to cover further technical developments.

According to article 2 of the Convention:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Legislative and other measures to be adopted by the parties cover the interception made by technical means of non-public transmissions of computer data from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data;[87] the damaging, deletion, deterioration, alteration or suppression of computer data;[88] the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;[89] and, the production, sale, procurement for use, import, distribution or otherwise making available a device designed or

---

85 Council of Europe, CETS No 185, (2001) 41 ILM 282 and Additional Protocol not directly related to cyber attacks, CETS No 189, 2003. For an analysis see the Explanatory Report, online: <http://conventions.coe.int/Treaty/en/Reports/html/185.htm> and Mike Keyser, "The Council of Europe Convention on Cybercrime" (2003) 12 J Transnat'l L & Pol'y 287 and RJ Currie, *International & Transnational Criminal Law* (Toronto: Irwin Law Inc, 2010) at 392–405.

86 Not ratified as of February 2012. The Convention was ratified the Senate of the US in 2006. For a criticism of the Convention on the ground that it gives too much power to investigative authorities and force Internet providers to respond to foreign evidence orders, see M Goodwin, "Watch Out. An International Treaty on Cybercrime Sounds Like a Great Idea Until You Read the Fine Print", (April 2001), online: <http://cryptome.org/cycrime-goodwin.htm>.

87 *Supra* note 85, art 3.

88 *Ibid* art 4.

89 *Ibid* art 5.

adapted for the purpose of committing any of the offenses just described against the confidentiality, integrity and availability of computer data and systems.[90] For criminality to attach, the illegal access and interception, data interference, system interference and misuse of devices must be committed intentionally and without right. For instance, in the case of illegal interception, the act is justified if the intercepting person "acts on the instructions or authorization of the participants of the transmission. . .or if surveillance is lawfully authorized in the interests of national security or the detection of offences by investigating authorities".[91]

The list of offenses signatories are required to incorporate in their domestic law also includes offences related to the infringements of copyright and related rights.[92]

Articles 2, 3, 4, 5 and 6 would cover espionage, especially industrial espionage, since it involves illegal access, illegal interception, data and system interference as well as misuse of devices.

In Canada, everyone who fraudulently and without color of right uses a computer service or system "is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years or is guilty of an offence punishable on summary conviction."[93] The *Criminal Code* contains a number of useful definitions including: 'computer programs', 'computer service', 'computer system', 'function', 'intercept' and 'traffic'. Most relevant is the definition of data as "representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system."[94]

Section 430(1.1) of the *Criminal Code*, which covers mischief in relation to data, is most important. It provides that:

> Every one commits mischief who willfully
>
> (a) destroys or alters, data;
>
> (b) renders data meaningless, useless or ineffective;
>
> (c) obstructs, interrupts or interferes with the lawful use of data; or
>
> (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

As in the case of the unauthorized use of a computer, the author of the mischief in relation to data: "(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or (b) is guilty of an offence punishable on summary conviction."[95] Data has the same meaning as in section 342.1(2) of the

---

90 *Ibid* art 6.

91 Explanatory Report, *supra* note 85 at para 58.

92 *Supra* note 85, art 10. See also arts 7-8 on computer related offences not relevant to cyber attacks.

93 *Criminal Code*, RSC 1985, c C-46 as am, s 342.1(1).

94 *Ibid* s 342.1(2). See also s 342.2 (1), possession of device to obtain computer service and s 191(1), possession, sale or purchase of a device for surreptitiously intercepting private communications.

95 *Ibid* s 430(5).

Criminal Code dealing with the unauthorized use of a computer.[96]

Sections 342.1 and 430(1.1) of the *Criminal Code* are adequate to sanction the authors of cyber attacks who spread and attempt to spread computer viruses and other malware designed to deny Internet services, shut down all computers or wipe out any type of data, provided of course that they can be identified and brought to justice. They cover the substantive provisions of the *Cybercrime Convention*. Although these provisions have no extraterritorial effect, they would apply to foreign hackers provided the effects of their nefarious attacks were felt in Canada.

Articles 23 to 35 of the *Convention on Cybercrime* deal with co-operation and mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. The Convention also creates an obligation to give law enforcement authorities the power to compel Internet Service Providers to monitor a person's online activities.[97]

In Canada, the *Mutual Legal Assistance in Criminal Matters Act*[98] provides for the implementation of treaties for mutual legal assistance in criminal matters. Part I covers the situation where Canada is the requested state. It deals with the authority and procedure for responding to a request by a foreign state or entity that is a party to such treaty or has entered into an administrative arrangement for legal assistance with Canada covering foreign investigations or other proceedings.[99] Such legal assistance pertains to search and seizure,[100] the gathering of evidence for use abroad,[101] and the lending of exhibits.[102] Part II deals with the situation where Canada is the requesting state. It lays down rules for the admissibility in Canada of evidence, especially foreign records, obtained abroad pursuant to an agreement.[103] Finally, Part III also addresses various issues arising when Canada has made a request to a foreign state such as the special authorization given to a

---

96 *Ibid* s 430(8). Note that Bill C-51 introduced in Parliament by the Minister of Public Safety on 1 November 2010, intended to amend the *Criminal Code*, the *Competition Act* and the *Mutual Assistance in Criminal Matters Act* (*Investigative Powers for the 21st Century Act*), in clause 10 would have made it illegal to possess a computer virus for the purpose of committing mischief and also made it an offense to import or make available a computer virus. It died on the order paper but will probably revived during the 41st session of Parliament.

97 *Supra* note 85, art 20. In Canada Bill C-52 entitled *Investigating and Preventing Criminal Electronic Communications Act*, which was introduced on 1 November 2010 in the House of Commons but died on the order paper, would have required telecommunications service providers to put in place and maintain certain capabilities allowing for the interception of information transmitted by telecommunications.

98 RSC 1985, c 30 (4th Supp) as am. For a detailed analysis see Department of Justice of Canada, The Federal Prosecution Service, Desk Book, Part VIII International Assistance Chapter 43, see online: <http://www.ppsc.gc.ca/eng/fps-sfp/fpd/ch43.html>.

99 *Ibid*, s 8.

100 *Ibid*, ss 10–16.

101 *Ibid*, ss 17–23.

102 *Ibid*, ss 30–34.

103 *Ibid*, ss 36–39.

person in a foreign state or entity who is not admissible under Canadian immigration rules to come to Canada to a designated place and for a limited period of time for the purpose of giving evidence in a proceeding or to give assistance in relation to an investigation or proceeding.[104] It further provides that records sent by a foreign state or entity in accordance with a Canadian request are privileged.[105]

From the point of view of cyber attacks and other cyber crimes, Parts II and III are particularly important when the attack originated outside Canada in a state party to an agreement providing for mutual assistance in criminal matters. However, the Canadian legislation will have to be amended to comply with the provisions of the *Convention on Cybercrime* dealing with procedural enforcement tools.

To be a "hacktivist" for fun or malicious purposes does not give that person a right or a license to hack into networks and disrupt or damage them. Probably, all types of hacking constitute a violation of some international or national law, or both, even if the hacker assuming the role of the network administrator or authorized user does not do anything harmful.[106] It should also be noted that the *Convention on Cybercrime* requires the parties to it to take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person has made possible the commission of a criminal offence established in accordance with its provisions.[107]

To fully implement the Convention, Canada must adopt more cyber specific criminal offences and give the police more power to conduct Internet surveillance in order to investigate cyber crimes. New legislation to that effect is pending before Parliament and it will probably include previous Bills.[108]

(c) Terrorists

A number of multilateral international conventions have been adopted that seek to prevent and punish different types of terrorist acts such as, *inter alia*, hijacking and other attacks on civil aviation including airports, the taking of hostages, attacking maritime vessels and fixed platforms on the continental shelf.[109] States parties to these conventions have agreed to amend their domestic criminal law to provide for wide bases of jurisdiction over these terrorist acts and either to extradite or prosecute their alleged perpetrators. Canada has implemented these conventions in its *Criminal Code*.[110]

---

104 *Ibid*, ss 40-41.

105 *Ibid*, s 44.

106 With the exception of espionage at international law or where a state has not criminalized the gaining of unauthorized access to someone else's computer system.

107 *Supra* note 85, art 12.2.

108 See *supra* notes 45, 96, 97. Some states which are vulnerable to cyber attacks may not be prepared to face this issue for lack of adequate resources or a willingness to do so. This attitude would hinder cooperation with Canada.

109 For a list see the Canadian *Criminal Code*, *supra* note 93, s 83.01(1) (Definition of "terrorist activity").

110 *Ibid*, ss 83.01–83.33. See also offences committed in or outside Canada also connected to terrorism: ss 7(1) (aircraft), 7(2.2) (fixed platforms), 7(2.31) (space stations), 7(3) (internationally protected persons), 7(3.1) (hostage taking), 7(3.2) (nuclear material),

The *European Convention on the Suppression of Terrorism*,[111] the *Declaration on Principles of Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations*,[112] the 1994 *Declaration on Measures to Eliminate International Terrorism*[113] and the 1996 *Declaration on Strengthening International Security*[114] also contain important provisions dealing with terrorism.

In Canada, the *Criminal Code* would cover cyber attacks by terrorists.[115] For instance, such attacks come within the scope of section 83.01(1)(b) of the *Criminal Code* which defines "terrorist activity" as

> an act or omission, in or outside Canada,
>
> (i) that is committed
>
> (A) in whole or in part for a political, religious or ideological purpose, objective or cause, and
>
> (B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and
>
> (ii) that intentionally
>
> (A) causes death or serious bodily harm to a person by the use of violence,
>
> (B) endangers a person's life,
>
> (C) causes a serious risk to the health or safety of the

7(3.71) (UN personnel), 7(3.73) (financing terrorism), 7 (3.72) and 431.2 (explosives or other lethal devices), 7(3.74) (terrorism offence committed outside Canada), 7(3.75) (terrorist activity committed outside Canada), 76 (hijacking), 77 (endangering aircraft or airport), 78 (offensive weapons and explosive substances), 78.1 (seizing control of ship or fixed platform). See also Bill C-10, *Safe Streets and Communities Act*, Part I, *Justice for the Victims of Terrorism Act*, *supra* note 45.

111 27 January 1977, ETS No 97. However, art 1 does not cover cyber attacks.

112 *Supra* note 23.

113 UNGA Res A/RES/49/60 (9 December 1994). Also UNSC Res 1189, (13 August1998) and UNSC Res 1373 (2001), UN Doc S/RES/1373 (28 September 2001).

114 UN Res 51/151 (13 December 1996).

115 *Criminal Code*, *supra* note 93, ss 83.01-83.33 and 7(3.74) (terrorism offence committed outside Canada), 7(3.75) (terrorist activity committed outside Canada). In the US see *The Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act)*, 2001 as am, Title VIII, *Strengthening the Criminal Laws Against Terrorism*, s 814 (deterrence and prevention of cyber terrorism), 18 USC s 1030(a)(5) and (e) (2) (definition of "protected computer"). See also Proposal for an International Convention on Cyber Crime and Terrorism, definition of "cyber terrorism", art1.2, online: <http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf> at 26.

> public or any segment of the public,
>
> (D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or
>
> (E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C).

Harboring or concealing a person whom he or she knows to be a terrorist for the purpose of enabling that person to facilitate or carry out any terrorist activity is guilty of an indictable offence.[116] This would also include a cyber attack.

Until there is a quasi-universal condemnation of cyber crimes and a wide adoption of the *European Convention on Cybercrime*, it is not possible to affirm that such crimes give all states universal jurisdiction to punish its non-state perpetrators as is the case with piracy.

(d) Prescriptive Jurisdiction over Cyber Offences

The Council of Europe Convention on Cybercrime in article 22.1 lists two of the traditional bases upon which a party may found claims to prescriptive jurisdiction over cyber offences. The first is the territorial principle which gives jurisdiction to the state in whose territory the offence is committed.[117] This includes its territory, ships flying its flag and aircraft registered therein.[118] The Convention does not take any position on the scope of the territorial principle. Does it mean exclusively the place where the offending act was commenced (subjective or initiatory principle), or where the act was consummated or where the last constituent element of the offence had occurred (objective or terminatory principle), or where the detrimental effects of the offence were felt? The territorial principle could also mean the place where any element of the offence occurred. Since article 22.1 does not exclude any criminal jurisdiction exercised by a party in accordance with its domestic law, the territorial principle could be interpreted to mean the state which has a reasonable and legitimate interest in taking jurisdiction or the state which has a real and substantial link with the offence and the offender.[119] Since the effects of a cyber attack would be felt in the territory of the targeted state, any of the bases for exercising jurisdiction pursuant to the territorial principle could be used except the subjective or initiatory principle.

Second, the Convention lists the active nationality principle, which bases jurisdiction on the nationality of the offender provided the offence is punishable

---

116 *Criminal Code*, *supra* note 93, s 83(23).

117 In Canada, *Criminal Code*, *ibid,* s 6(2). As a general rule no person shall be convicted of an offence committed outside Canada.

118 *Supra* note 85, art 22.1, a, b, c.

119 In Canada see *R. v. Libman*, [1985] 2 S.C.R. 178 (jurisdiction where a substantial portion of the activities has taken place in Canada).

under the criminal law where it was committed or if the offence was committed outside the territorial jurisdiction of any state.[120] Canada uses the principle of active nationality sparingly.[121]

Unlike Canadian legislation,[122] the Convention does not mention the passive personality principle based on the nationality of the victim. On the other hand, a state victim of a cyber attack should be able to use the protective principle to establish its jurisdiction over the offender since such attack would be prejudicial to its security and economic well-being.[123] The universal principle should also enable states to exercise jurisdiction over terrorists committing cyber offences — especially where extradition of the offenders is not possible and there are no other bases for the exercise of jurisdiction.

Canadian legislation complies with the provisions of the Convention dealing with jurisdiction.[124] It also enables Canadian courts to assert extra territorial jurisdiction over cyber crimes and some of its non-state actors.[125] However, assertions of extra-territorial jurisdiction may result in disproportionate distribution of Internet regulation which would allow the state that prescribes the most stringent laws to prevail. The effects doctrine would limit such assertion and give the strongest claim to the state that felt the most substantial effects of a cyber attack.

(e) Extradition

The *Convention on Cybercrime* contains provisions dealing with the extradition of individuals who have committed the cyber offences listed therein "provided they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty."[126] These extraditable offences are deemed to be included in any existing extradition treaties between the parties to the Convention. Since many states will not extradite their nationals, the *Convention on Cybercrime* provides that if the extradition is refused solely on the basis of the nationality of the person sought, or because the state has jurisdiction over the offence, the requested state shall submit the case at the request of the requesting state to its competent authorities for the purpose of prosecution.[127] With respect to terrorists, the political offence exception could be a barrier to their extradition since the *Convention on Cybercrime* provides that "Extradition shall be subject to the conditions provided by the law of the requested

---

120 *Supra* note 85, art 22.1.d.

121 *Criminal Code*, *supra* note 93, ss 46(3), 7(2.3), 7(3,7)(c), 7(3.71)(c), 7(3)(c), 7 (3.1)(c)(i), 7(3.5)(c), 7(3.7)(c), 7(3.72)(c)(i), 7(3.73)(c)(i), 7(3.74)(a). In general, see JG Castel, "The Internet in Light of Traditional Public and private International Law Principles and Rules Applied in Canada" (2001), 39 Can YB Int'l L 3 at 9–22.

122 *Criminal Code*, *ibid*, ss 7(2.31)(a), 7(2.1)(f), 7(3.1)(e), 7(3.71), 7(3.72)(e), 7(3.75).

123 *Criminal Code*, *ibid*, ss 7(2.1)(g), 7 (2.31)(b), 7 (3.1)(d), 7(3.72)(f), 7(3.73)(e), 7(3.75)(b),(c).

124 *Ibid.*

125 *Ibid*, ss 83.01(1), (Definitions, "terrorist activity" (a) and (b); 7(3.74), and 7(3.75)).

126 *Supra* note 85, art 24.

127 *Ibid*, art 24.6.

Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition."[128] However, modern extradition treaties have eliminated this exception and replaced it with a humanitarian exception to allow the accused to claim that he or she will not receive a fair trial in the requesting state. This is not the case in Canada where the *Extradition Act* provides that the Minister shall refuse to make a surrender if "the conduct in respect of which extradition is sought is a political offence or an offence of a political character,"[129] except in the case of a person subject to a request for surrender issued by the International Criminal Court.[130] However, some conduct such as murder, extortion, using devices in circumstances in which human life is likely to be endangered or property damage is likely to be caused, does not constitute a political offence or an offence of a political character.[131] This provision would cover a cyber attack if it is an offence included in the relevant extradition treaty. To overcome these barriers to extradition many states have used other methods such as exclusion, deportation or rendition of the accused.

Once the accused is before the courts of the requesting state, treaties of mutual assistance in criminal matters are designed to help the prosecution gather the evidence necessary for obtaining a conviction.[132]

In the absence of a treaty of extradition, the requested state would be under no obligation to extradite the offender found in its territory. For states that are not parties to the *Convention on Cybercrime* extradition would depend on the treaties in existence between the states concerned.

As with state perpetrators, the greatest difficulty is identifying and locating the actor of the cyber attack, whether a private individual or a terrorist, for the purpose of prosecution or extradition, as some states may not be properly knowledgeable or equipped to do so.

CONCLUSIONS

Global security in cyberspace is an absolute necessity given the global nature of the Internet. Preventing and stopping a cyber attack, especially against the critical infrastructures of a particular state, requires the co-operation and assistance of all states in the investigation of such attack and in blocking all traffic with the offending state Internet Service Providers. Multilateral responses are necessary as they are in other situations involving threats to international peace and security. Cyber attacks are a global problem like global warming, because no one state can deal adequately with the problem on its own.[133] Existing customary and conven-

---

128 *Ibid*, art 24.5. For political offences see S Williams & JG Castel, *Canadian Criminal Law. International and Transnational Aspects* (Toronto: Butterworths, 1981) at 347–378.

129 SC 1999, c 18, s 46 (1)(c).

130 *Ibid*, s 47.1.

131 *Ibid*, s 46(2).

132 For instance, Convention on Cybercrime, *supra* note 85, arts 25–35.

133 HH Perritt Jr "The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Government" (1998) 5 Ind J Global Legal Stud 423 at 429.

tional international law rules are not as clear and effective when applied to a cyber attack by an organ or agent of a state or by its sponsored terrorist organizations as when applied to a cyber attack by a non-state actor. Simply reaffirming the applicability of present international law rules to cyber attacks is not sufficient. Some gaps and uncertainties still exist in their application which must be addressed due to the fact that cyber warfare is of very recent origin. However, it will not be easy to change present international law rules to reflect the interests and desires of a significant number of states especially those of the United States of America, China and Russia. Any new international law rules will have to achieve a suitable balance between the threats and opportunities cyberspace creates.

With respect to cyber attacks as cyber crimes by non-state actors including terrorists, the present legal situation is much better since an ever increasing number of states have implemented the *Council of Europe Convention on Cybercrime*, which so far has proven to be reasonably effective. A global solution is in sight. However, there is still room for improvement on the Canadian domestic level.

It is worth considering a number of possible solutions which could be adopted at the international and Canadian levels.

(a) On the International Level

To adapt international law rules to this new form of nefarious cyber activity, states could:

> 1. Clarify the notion of use of force in article 2 paragraph 4 of the *Charter of the United Nations* by having this body declare that it includes cyber attacks. This finds support in the advisory opinion of the International Court of Justice in the nuclear weapons case;[134] or
>
> 2. Amend the definition of aggression to include cyber attacks by states or sponsored by them without being preceded by or accompanied by physical armed attacks. This would enable the Security Council to intervene pursuant to Chapter VII of the *Charter of the United Nations* and the International Criminal Court to exercise jurisdiction when authorized to do so by the Security Council, pursuant to article 5.1(d), which lists the crime of aggression as defined in article 8 bis adopted on 11 June 2010. This amendment would not affect the concept of self-defence. However, it may be considered unnecessary by the U.S.A., which recently emphasized in its *Declaration of an International Strategy for Cyberspace* that: "Consistent with the United Nations Charter, states have an inherent right to self — defense that may be triggered by certain aggressive acts in cyberspace."[135] or
>
> 3. Adopt a multilateral or bilateral Convention on Cyber Space prohibiting states from resorting to cyber attacks on the Internet and other computer networks as the international community has done with respect to other weapons in the *Geneva Gas Protocol* prohibiting the use in war of

134 *Supra* note 24.

135 *Supra* note 10.

poisonous gases,[136] the *Biological Weapons Convention*,[137] and the *Chemical Weapons Convention*.[138] The convention could be limited in scope to cyber attacks most seriously endangering the security of states and their economic well-being; for instance, banning cyber attacks against financial institutions such as altering data or damaging their networks through logic bombs. More generally, the convention could ban cyber attacks against all civilian infrastructures except in case of self-defence; and

4. Due to the unique aspects of cyberspace, clarify its impact on the law of armed conflict and ban or limit cyber attacks by adding a Protocol to that effect to the 1980 *Convention on Prohibition or Restriction on the Use of Certain Conventional Weapons* and *Protocols*;[139] and amend the *Geneva Conventions* and Protocols accordingly;[140] and

5. Monitor compliance by international inspection teams for which an International Cyber Forensics and Compliance Body under the auspices of the United Nations would be created similar to those in the *Treaty on the Non-Proliferation of Nuclear Weapons* whose signatory states have concluded agreements with the International Atomic Energy Agency with respect to compliance[141] or the *Chemical Weapons Convention*.[142] Flow monitoring devices could be placed at key nodes leading into the networks of states to watch how the traffic moves and to look for unusual patterns in order to detect the origin of the attack. The sanctions for breaching such conventions would be to limit or prevent the international Internet and telephone traffic flows into the offending state thus denying service to legal entities, persons, state agencies and devices participating in an attack. Monitoring compliance is important as the value of an international convention to ban or limit cyber attacks would depend upon detecting violations. This is not easy since a cyber attack by state A against state B can come from a botnet computer in state C. Even if a state admitted that an attack came from a hacker in its territory, it could claim that such attack was the act of an anonymous citizen. National cyberspace accountability is difficult to establish.

6. If options 1, 2, 3, 4 or 5 are not possible at the present time, a new customary international law rule could be developed by a majority of states by categorizing a cyber attack by or sponsored by a state as an act of war depending upon the circumstances and effects of such attack.

7. Create a multilateral International Standing Emergency Response

136 (1925) 94 LNTS 565, (1975) 14 ILM 49.

137 (1972) 26 USTS 583, (1972) 11 ILM 310.

138 (1993) 32 ILM 800.

139 *Supra* note 65.

140 *Supra* notes 66, 67, 68.

141 Art II, online: <http://www.state.gov./www/global/arms/treaties/npt1.html>.

142 See *supra* note 138.

Body;[143] and

8. Create an International Cyber Reduction Risk Center with obligation to assist targeted states; and

9. Become a party to the Convention on Cybercrime,[144] and include a cyber attack as an offense in the domestic criminal legislation; and try to provide penalties similar to those prevailing in the other member states; and

10. Become a party to conventions of mutual legal assistance in criminal matters that cover cyber crimes by providing information and evidence to facilitate finding, prosecuting and punishing those responsible for such crimes; and

11. Include cyber crimes in treaties of extradition and remove the political offence exception from the treaties that still contain this exception; and

12. Modify the scope of the international law rules pertaining to state immunity by removing the immunity from jurisdiction of states resorting to or sponsoring terrorism.

Some states have already adopted some of these proposals. However, as already mentioned, regulation of the Internet to prevent cyber attacks is a transnational problem that must receive global support.

(b) On the National Level in Canada

On the national level, Canada could take the following steps to reduce its vulnerability to cyber attacks:

1. Participate actively in the adoption of new international law rules with respect to cyber attacks on the international level as proposed above.

2. With respect to cyber attacks by state actors, adopt the U.S. categorization of such attacks as acts of war until clarified by the Security Council.

3. Implement as soon as possible Canada's Cyber Security Strategy.[145]

4. Adopt legislation to implement the provisions of the *Convention on Cybercrime* which are not yet part of the existing federal legislation to enable Canada to ratify it. In the last Parliament the government had introduced three Bills[146] for this purpose one of which has already been be

---

143 See for instance, NATO Cooperative Cyber Defense Center of Excellence in Estonia created in 2008 following the 2007 Cyber attack on that country's public and private institutions.

144 *Supra* note 85.

145 *Supra* note 18.

146 40th Parliament: Bill C-50, *An Act to amend the Criminal Code (Interception of Private Communications and Related Warrants and Orders)*; Bill C-51, *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act (Investigative Powers for the 21st Century Act)*; Bill C-52; *An Act regulating telecommunications facilities to support investigations (Investigating and Preventing Criminal Electronic Communications Act).*

re-introduced and adopted by the 41st Parliament and is now before the Senate for final approval.[147] The others will probably be re-introduced soon. The most important provisions of these bills from the point of view of cyber crimes deal with improved access to investigative tools including: the extension of the maximum period for the use of tracking devices in investigations of terrorism; tracing communications back to a suspect; making it illegal to possess a computer virus for the purpose of committing an offence of mischief and importing and making available a computer virus; enhancing international co-operation to help in investigating and prosecuting cyber crimes that go beyond Canada's borders; and, the obligation of telecommunications service providers to put in place and maintain devices that facilitate the lawful interception of information transmitted by telecommunications to be supplied to police and security intelligence services including basic information about their subscribers.

5. Resort to unilateral measures such as the use of active defenses by the Canadian system administrator who, having traced the source of the attack using trace programs, would back hack and disrupt it, in the absence of specific international instruments relating to the enforcement of data protection laws with states which are not parties to the *Cybercrime Convention* or in case of refusal to cooperate. This solution may be an appropriately forceful response to a cyber attack whether by a state or a non-state actor. Another solution would be cyber deterrence by way of countermeasures against the attacker network. It would not amount to cyber war and could be justified as a countermeasure if the attack was by a state actor.

6. Create a national cyber attack early warning system whether or not such attack is politically motivated.

7. Create a Cyber Command similar to the one existing in other states, notably in the United State of America. It could be in charge of running the early warning system.

8. As proposed by Canada's Cyber Security Strategy, fix the vulnerability of the Canadian power grid, banking system and other civilian networks. To reduce Canada's vulnerability to cyber attacks on her infrastructures is not easy as the critical infrastructure networks pertaining to electricity,[148] banking, manufacturing, transportation, etc., are all connected to the Internet. A solution would be to keep these networks separate from the Internet and secure. To do so would minimize and even eliminate any interruption and manipulations of Canada's critical functions thereby avoiding any concerted attack on the computers of an important sector of

147 Bill C-10, *supra* note 45, (deals with the recourse available to victims of terrorism against terrorists and those sponsoring them).

148 In the USA see David M Nicol, "Hacking the Lights Out" (July 2011) *The Scientific American* 70. Also, "Trustworthy Cyber Infrastructure for the Power Grid" Multi-university research project funded by the U.S. Department of Energy, online: <www.tcipg.org>.

the Canadian economy.

9. Adopt federal regulations pursuant to Canada's Cyber Security Strategy and proposed legislation,[149] to create cyber security requirements for the large Internet Service Providers operating in Canada forcing them to engage in deep packet inspection at line rate speed with no latency or by flow analysis to identify the signature of the malware. This could be done automatically. Again the difficulty may come from the fact that the packets may be routed through a state that is not the source of the attack. In China, for instance, the government actively defends the network. In Canada and the United States of America, this is not yet the case because cyber connections are privately owned and operated. The Canadian government cannot disconnect the entire nation's network from the rest of cyberspace to stop malware and prevent a "Distributed Denial of Service." Federal regulation of the network even for reasons of security has to be limited for fear of violating privacy issues and the freedom of opinion and expression including media of communication guaranteed by the Canadian *Charter of Rights and Freedoms*.[150] The best solution would be a federal government widely integrated cyber security program that included standards for private companies. Canada could also require Internet Service Providers to deny service to actors who participate in cyber attacks and to report them to the authorities and black list them in the future.[151]

Over the centuries, international law has evolved in order to keep up with new methods of human interaction on land, sea, air, outer space and, more recently cyberspace. With the end of the outer space age,[152] the international regulation of cyberspace has become what one could describe as the final frontier and one the greatest challenges of the 21st century.

---

149 See Bill C-51, *supra* note 146.

150 *Constitution Act, 1982*, Schedule B to *Canada Act 1982*, (UK), 1982, c 11, s 2(b) (fundamental freedoms).

151 The basis for federal legislation over the Internet and cyberspace could be based on the opening words of s 91 (power of the Parliament over the Peace, Order, and good Government of Canada) and ss 91(29) and 92(10)(a) and (c) (by reason of the nature of the service provided by the Internet) *Constitution Act, 1867*, 30 & 31 Vic, c 3.

152 "It is equally quite conceivable that the fantasy-made-reality of human space flight will return to fantasy. It is likely that the Space Age is over." See "The End of the Space Age", *The Economist* 400:8740 (7 July 2011) 7.