CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
CSC 29 / CCEM 29

EXERCISE NEW HORIZONS / EXERCICE NOUVEAUX HORIZONS

THE SOVEREIGN NATURE OF CYBER WARFARE

By /par Maj/maj M.A.R. Beaton

This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied except with the express permission of the Canadian Department of National Defence.

La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense national.

ABSTRACT

The Unites States and Canada have a history of working together in the defence of the continent. With growing concerns over asymmetric threats, including cyber terrorism and cyber war, there may be consideration for a bi-national cyber defence organization to provide mutual protection.

Although one of the main functions of such an organization would be computer network attack (CNA), this capability would not be effective in a bi-national cyber defence organization. Canada and the US approach decision-making on critical issues in different ways. In the case of a cyber attack or the threat of one against the continent, the possibility of quick answers and agreement on response is remote. Accordingly, it is highly unlikely that we could expect timely and unified action, thus making the bi-national organization ineffective.

That is not to say that cyber warfare is something to be ignored. Canada must remain current in addressing this threat and work with allies to stay in front of an increasingly threatening world. In the end, though, Canada must retain sovereign control over computer network attack capabilities.

The Sovereign Nature of Cyber Warfare

Canada and the United States have an interesting continental relationship. Although we are inseparable by geography, it is our economic reliance that is the significant measure of our closeness.[1] Depending on one's perspective, which can change over time, our overall situation is good fortune or bad luck. Nevertheless, throughout our shared history, dealings have been characterized by constructive partnerships and collaboration. The two countries have spent very little time as adversaries, and compared to the epic wars in Europe, hostilities in North America have been mere skirmishes. Indeed, the last serious engagement was not Canada-US initiated, but a 'war by proxy' executed on behalf of Irish extremists.[2]

That is not to say we view every issue the same way and aspire to the same goals.[3] In fact, the level of enthusiasm with which we cooperate is variable, dependant on many transient factors such as political and party policies, economic benefits, and world events. Sometimes our commitment to partnership seems feeble, other times it is whole-hearted, but on balance, we can and do work well together.

[1] "Canada and the United States share the largest and most comprehensive trading relationship in the world. Approximately $2 billion in goods and services cross the border each day. The two countries are each other's largest customers and biggest suppliers." Canada, The Standing Senate Committee on National Security and Defence, *Defence of North America: A Canadian Responsibility*, Sep 2002 p 27.

[2] "The third and last occasion when Canadians were compelled to take up arms to meet the military threat from the south was during the Fenian Raids of 1866–71. The Fenian Brotherhood was an association of Irish Americans … whose intention was to win freedom for Ireland by striking at Britain's colonies in North America." LF Organization [http://www.army.dnd.ca/LF/organ/armychrono/chrono_fenian_e.html], accessed May 8, 2003.

[3] For example, Sir Robert Borden was against Free Trade in 1911, Canada declared war on Germany in 1939 while the United States did not commit until 1941and more recently, although both countries have reasonably similar environmental concerns, they could not agree on Kyoto.

Nowhere is this more evident than in NORAD. Since 1958, Canada and the US have participated in cooperative continental air defence, primarily monitoring air space and on alert to respond immediately to any air breathing threat. Although it would seem protection against nuclear threats favoured continental US because interception was expected to occur in the north, NORAD has been a hallmark for defence interoperability. But there have been disharmonious occasions as well in this defence relationship. One need only recall Canada's reluctance to accept nuclear weapons on its soil, our confused response to the Cuban missile crisis and our incoherent position over Ballistic Missile Defence. Through it all, NORAD has survived, and while the pendulum of political interest swings between sharp indifference and reasonable cooperation, the military partnership lumbers along in an increasingly threatening world.

One threat of particular interest to our respective military and civilian security services is computer network attack (CNA), or 'cyber attack.'[4] In a roundabout way, this has occurred because of the world's growing reliance on information and related technologies to manage infrastructures.[5] This technology, a symbol of success and perhaps a modern day 'Achilles' Heel,' has become the target for darker cyber advancements aimed at

[4] This is the attacking aspect of cyber war. Cyber war can be defined as: "conducting military operations according to information-related principles. It means disrupting or destroying information and communications systems. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself." John J. Arquilla and David F. Ronfeldt, "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict," Fall 1995, [http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/cyberwar.html], May 7, 2003.

[5] "Activities involving the operation and control of essential *physical and functional infrastructures*--power grids, air traffic control systems, telecommunications and the like--are increasingly shifting from mechanical/electrical control to electronic/software control." Fall 1995, [http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/wild.html]. accessed May 7, 2003.

denying, disrupting, degrading and exploiting services.[6] To make matters worse, in this interconnected world, traditional lines of defence and borders do not slow these aggressors as they travel international pathways to the heart of unprotected infrastructures. As one study ruefully notes, "one dimension of the global information grid commerce (and other activities) is that this vulnerability is decoupled from traditional linkages between territorial integrity and security."[7] In countering this assault, a worldwide industry has evolved to protect information and information systems. Governments, recognizing the importance of information[8] have, to varying degrees, developed procedures, standards and organizations to defend information and, paradoxically, begun to develop their own capabilities to deny, disrupt and degrade information and control systems.[9] Fortunately, unlike a Russian view that a nuclear response would be acceptable to a cyber attack,[10] we can expect responsible states to

[6] Keith A. Rhodes, chief technology officer of the General Accounting Office, is quoted as saying "Over 100 countries already have or are developing computer attack capabilities...NSA (the National Security Agency) has determined that potential adversaries are developing a body of knowledge about U.S. systems and methods to attack them." Bartlett Cleland, "Grandstanding on terrorism and tech," October 9, 2002, [http://news.com.com/2010-1071-961295.html], accessed May 7, 2003.

[7] Phil Williams, Timothy Shimeall, and Casey Dunlevy, "Intelligence Analysis for Internet Security." *Contemporary Security Policy,* Vol 23, No 2 (August, 2002) p 3.

[8] "In the past few years, threats in cyberspace have risen dramatically. The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible." Forward by President G.W. Bush. United States, *The National Strategy to Secure Cyberspace (Draft)* Feb 2003. [http://www.whitehouse.gov/pcipb/], accessed May 7, 2003.

[9] A Congress Research paper on cyberwarfare includes a Naval Intelligence assessment that identifies "Russia, China, Indian and Cuba as counties who have acknowledged policies of preparing for cyberwarfare and who are rapidly developing their capabilities." Many others are reported to have some capability and are active in the field. Steven A. Hildreth, "Cyberwarfare." *Congressional Research Service, The Library of Congress*. Order Code RL30735. June 2001, p 1.

[10]"from a military point of view, the use of Information Warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict whether there were casualties or not . . . considering the possible catastrophic use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces . . . Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself." V.I.Tsymbal, "Kontseptsiya 'Informatsionnoy voyny'", (Concept of

counter a cyber attack with cyber weapons. For example, in the United States, the culmination of a significant defence review was a realigned US Strategic Command (USSTRATCOM) with the added responsibility to "coordinate and, when directed, conduct computer network attack in support of combatant commanders' and national objectives."[11] Furthermore, the subordinate Joint Task Force – Computer Network Operations (JTF-CNO) organization "is responsible for ensuring that CNA capabilities can be efficiently employed in support of U.S. National Security objectives."[12] Understandably, arguments have been made in Canada to develop similar computer network exploitation (CNE) and CNA capabilities as adjuncts to our Canadian Forces Information Operations capability.[13] Furthermore, as this could arguably be a continental problem, some experts see value and logic in wrapping us in a bi-national security blanket. Security professionals such as Lieutenant-Colonel Allen have suggested that,

> a combined approach to conducting global network surveillance would be of benefit to both nations…[and extending] interoperability to the fields of CNE/CNA is not beyond reasonable expectations.[14]

There is reason to believe that the pendulum is moving, albeit at a snail's pace, towards a stronger "participative" partnership in continental defence,[15] rallied onward by many

Information Warfare), speech given at the Russian-U.S. conference on "Evolving post Cold War National Security Issues," Moscow 12-14 Sep., 1995 p 7 as quoted in Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," *Parameters,* (Winter, 1996-97) p. 82.

[11] USSTRATCOM Joint Task Force/Computer Network Operations (JTF/CNO) Fact Sheet, Feb 2003

[12] *Ibid.*

[13] See LCol Francis Allen, "CN(EH?): Should the CF Adopt Computer Network Exploitation and Attack Capabilities?" *Canadian Forces College Review 2002.*

[14] *Ibid,* p 10.

[15] What could be clearer than the statement in *Strategy 2020* that, "[o]ur most important ally now and for the future is the United States where our strong relationship has long benefited both countries. We must plan to nurture this relationship by strengthening our inter-operability with the US Armed Forces, training together, sharing the burden for global sensing and telecommunications and pursuing collaborative ways to

interested experts, advising and recommending a 'course correction' for Canada.[16] Ambassador Paul Cellucci has called for a strong North American security perimeter.[17] The Honourable John McCallum has also reaffirmed our enduring defence relationship, noting that,

> [o]ver the years, Canada and the United States have disagreed on many issues. However, not one of these issues compromised Canada's core commitment to the joint defence and security of the people of North America. I can assure you today that no future action by this Government will ever compromise that core commitment.[18]

On the horizon, Canada and the US face similar cyber threats and defensive needs while behind us stands a tradition of successful defence partnerships. The case for cyber interoperability and a cyber alliance, therefore, seems easy to make. Certainly, in the realm of surveillance and analysis there are traditional bonds that link Canada and the US that would extend to the covert activities of CNE. On the battlefield, fighting as a coalition, we find synergy in interoperability. Computer exploitation and attack could be integrated into the tactical and operational war-fighting plan, much the same as naval ships and fighter aircraft in past missions such as Operation Allied Force. One might even argue for a 'cyber command' similar to NORAD, to guide bi-national CNA and Computer Network Defence (CND) operations. However, it is one thing to envision

respond to emerging asymmetric threats to continental security." *Strategy 2020, Canadian Defence in the 21st Century* [http://www.cds.forces.gc.ca/pubs/strategy2k/s2k07_e.asp], accessed May 7, 2003.

[16] Danford Middlemiss suggests that the 9/11 attacks served to broaden interoperability "to include a potential integration of command and control arrangements across the board and at the highest level." Danford Middlemiss and Denis Stairs, "The Canadian Forces and the Doctrine of Interoperability: The Issues." *IRPP – Policy Matters*, Vol 3, No 7, (June, 2002), p 23.

[17] Ambassador Paul Cellucci , "US Ambassador Emphasizes Security Concerns, Not Sovereignty," Interview with Lisa Laflamme, Canada AM, CTV, October 31, 2001.

[18] The Honourable John McCallum, "Canada-US Relations" (Speaking Notes for the Minister of National Defence at the Conference of Defence Associations Annual General Meeting), Ottawa, Feb 27, 2003.

solutions for bi-national cyber defence, but premature to be contemplating the sod turning ceremony! Indeed, notwithstanding the success of our current and past defence arrangements, Canada must maintain sovereignty over computer network attack capabilities.

For CNA to be an effective weapon, it is vital that it be employed at the most opportune time. Equally important, if it is to be an effective bi-national weapon, support from both nations for its use must be unequivocal. Although these characteristics are obvious prerequisites for the successful application of cyber force,[19] they are not achievable without bi-national consensus on the critical questions of when to respond and with what weapons. This paper will show how fundamental differences between Canada and the United States in reaching key decisions on response will invariably derail timeliness and unity, thus rendering the bi-national CNA function ineffective. The first step, however, is to frame a theoretical reference point by characterizing what CNA brings to the strategic fight and then postulating what a bi-national mechanism for controlling and employing this capability would look like.

What can cyber weapons do for Canada and the US? Notwithstanding that concrete examples are not in the public domain, a reasonable assumption would be 'whatever is available at large.' Certainly this capability would be gathered, studied and enhanced for military use along with the development of more sophisticated variants. The United

[19] Even at the time NORAD was standing up, senior leaders recognized the same situation. In fact, in 1957 they agreed "that the air defence of Canada and the United States is one problem and that both countries will react automatically and in unison against any attack on the North American continent." Ann Denholm

States Air Force Information Warfare Battlelab has identified more that 270 warfare concepts forwarded between 1997 and 2001, with 37 projects started.[20]

If past accomplishments are the seeds of future capability, then what could develop is impressive. The "I Love You" virus caused losses estimated in the billions of dollars, while simple to generate[21] Distributed Denial of Service (DDoS) attacks against infrastructure targets such as the Internet Domain Naming Service (DNS) servers and routers disrupted numerous services as the Internet was flooded with massive amounts of traffic. [22] NIMDA, a blend of worm and virus, caused an estimated loss of as much as $3 billion in damages and productivity.[23] The 'Code-Red' worm was another nasty event when on July 19, 2001, "more than 359,000 computers connected to the Internet were infected with the Code-Red (CRv2) worm in less than 14 hours. The cost of this epidemic, including subsequent strains of Code-Red, is estimated to be in excess of $2.6 billion."[24] One high-speed worms now being seen, the 'Slammer', spreads two orders of magnitude faster than Code-Red, and "represents a significant milestone in the evolution

Crosby, "A Middle-Power Military in Alliance: Canada and NORAD." Journal of Peace Research, Vol 34, Issue 1 (February, 1997), p 44.

[20] Robert Wall and David A. Fulghum, "New Tools Emerge for Info War Battle." *Aviation Week & Space Technology*, Feb 26, 2001, pp 58-60.

[21] Web literature indicates Trin00 is popular Distributed DoS tool and that it likely originated "as UDP based [daemons], access-restricted remote command shells, possibly used in conjunction with sniffers to automate recovering sniffer logs." David Dittrich [dittrich@cac.washington.edu] "The "Tribe Flood Network" distributed denial of service attack tool," October 21, 1999, [http://staff.washington.edu/dittrich/misc/tfn.analysis], accessed May 7, 2003.

[22] On April 15, 2000, the Royal Canadian Mounted Police (RCMP) arrested "MAFIABOY" for the Distributed Denial of Service (DDoS) attack on CNN in Atlanta, Georgia, on February 8, 2000. Thirteen Internet 'Root Servers' were attacked in Oct 2002.

[23] Indeed as a SANS Institute Report states, "NIMDA severely compromises the security of infected hosts, as it provides remote attackers with full Administrative authority over the victim and access to the entire file system. NIMDA infections are further very difficult to clean, as the worm makes numerous modifications to system files and registry settings." The NIMDA Worm/Virus Report, [http://www.incidents.org/react/nimda.pdf], October 3, 2001, accessed May 7, 2003.

[24] David Moore, Colleen Shannon, Jeffery Brown, "Code-Red: a case study on the spread and victims of an Internet worm," [http://www.caida.org/outreach/papers/2002/codered/codered.pdf], accessed May 8, 2003.

of computer worms."[25] There are also logic bombs and Trojan horses, available for future nefarious use, hidden in software patches and tools.[26] An area where a sophisticated attack could be disastrous is web defacement. As quoted in the Washington Post, "according to iDefence, a Reston, Va. based Internet security firm, the pro-Islamic hacking group, *Unix Security Guards*, defaced nearly 400 Web sites…with antiwar slogans written in Arabic and English."[27] Furthermore, attack planning is taking on a higher level of sophistication. Faris Muhammad Al Masri of a group called UNITY suggested that there might be a phased Arab e-jihad against Israel.

> Phase one might consist of disabling official Israeli government sites…[p]hase two focuses on crashing financial sites such as those belonging to Israel's Stock Exchange and central bank; phase three involves knocking out the main Israeli ISP servers; and phase four consists of blitzing major Israeli e-commerce sites to cause the loss of hundreds of online transactions.[28]

[25] "Although it did not contain a destructive payload, Sapphire spread worldwide in roughly 10 minutes causing significant disruption of financial, transportation, and government institutions. It clearly demonstrates that fast worms are not just a theoretical threat, but a reality -- one that should be considered a standard tool in the arsenal of an attacker." The report details that "[t]he Sapphire Worm was the fastest computer worm in history. As it began spreading throughout the Internet, it doubled in size every 8.5 seconds. It infected more than 90 percent of vulnerable hosts within 10 minutes. The worm (also called Slammer) began to infect hosts slightly before 05:30 UTC on Saturday, January 25 [2003]. Sapphire exploited a buffer overflow vulnerability…The worm infected at least 75,000 hosts, perhaps considerably more, and caused network outages and such unforeseen consequences as canceled airline flights, interference with elections, and ATM failures." David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford and Nicholas Weaver, "The Spread of the Sapphire/Slammer Worm," [http://www.cs.berkeley.edu/~nweaver/sapphire/], accessed Feb 14 2003.

[26] It is recognized that legitimate software tools freely available through the Internet are being hacked into and Trojan horses installed to create back doors; an opening for clandestine entry at a later date. Peter Piazza. "Who's Winning the Cyberwars?" *Security Management*, December 2002, p71-2.

[27] Brian Krebs writes that "anti-virus vendors and security experts warned users to be on the lookout for the "Ganda" worm, a virus that promises a screensaver program with pictures "taken by one of the US spy satellites during one of it's [sic] missions over Iraq." The virus tries to shut down various anti-virus and security products running on the recipient's machine, and then attempts to delete vital system files. The message is signed "VX Heavens," a reference to an underground virus-writing group that has posted messages urging the United States to "stop the oil war."" Brian Krebs, washingtonpost, March 20, 2003 [http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A62865-2003Mar20&notFound=true], accessed May 8, 2003.

[28] Giles Trendle, "Cyberwars: The Coming Arab E-Jihad," *The Middle East*, No. 322 (April 2002), p. 6.

Looking closer to home, cyber attacks have, apparently, been successfully employed by the United States. Allegedly, US military cyber attacks were staged in Haiti during Operation Uphold Democracy and in Kosovo against Yugoslavia air defence system, where air targets were inserted into the electronic systems.[29] Technological ability was presumably put to use during the 1990-91 Gulf War when US military analysts read Iraqi e-mail.[30] Thus, although cyber attack ability is based on anecdotal evidence and isolated incidents, there is evidence that the capability could be exploited for tactical and strategic war fighting purposes. In a future defensive response role, strategic effects could include targeting classified networked data bases, mounting demonstrations such as shutting down a country's electrical power, manipulating television broadcasts or locating an adversary's national command, control and communications nodes and destroying them.[31] There are other potential coercive and destructive uses of CNA as well. As Colonel William Bayles notes, cyber attacks could be used "to stress a population at large, which in turn will put pressure on the policymakers of the attacked state."[32] Indeed, this has an eerie parallel to the Trenchard doctrine, which suggested, "that civilian morale could be undermined by attacking vital industrial and communications

[29] The Washington Post reported that "[c]omputers were broken into and exploited during Operation Uphold Democracy in Haiti in 1994, according to sources. President Clinton personally approved the operation." Also reported were attacks on Milosevic's financial structure and the air defence system. Bill Arkin, [http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm], accessed May 7, 2003

[30] One Intelligence Forum has stated that "[d]uring the 1990-91 Gulf War, US Intelligence was able to read Iraqi email, but there was no active manipulation of enemy computers. The USAF then had cyberwar capabilities to insert themselves into the Iraqi systems." Association of Former Intelligence Officers, [http://www.afio.com/sections/wins/1999/35.html], accessed May 7, 2003.

[31] David A. Fulghum and Robert Wall, "U.S. Shifts Cyberwar to Combat Commands," *Aviation Week & Space Technology*, 26 Feb 2001, p 51.

[32] William J. Bayles, "The Ethics of Computer Network Attack," *Parameters* (Spring, 2001) p 47.

targets and that the resulting loss of will would cause the civilians to pressure their government into making terms."[33]

Evidence suggests, therefore, that we must always be vigilant against cyber threats and prepared to use cyber weapons,[34] but is the current capability truly effective? There is room for caution in this regard. We believe that cyber attacks can cover vast space with extraordinary destructiveness, and that with the click of a mouse we can bring a nation's economy to its knees. But perhaps assertions based on limited examples and hypothesis should be viewed with skepticism. For example, Margaret Purdy, head of Canada's Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), in building a case for concern, noted that hackers had "taken control of a sewage treatment plant in Australia.[35] On closer examination, though, we find it was a disgruntled consultant with inside access who needed 45 access attempts to enter the system and release sewage (possibly one million litres) into the coastal waters of Queensland. The cost to clean up was less than twenty thousand dollars.[36]

[33] David R. Mets, *The Air Campaign: John Warden and the Classical Airpower Theorists*. (Alabama: Air University Press, 1999), p 22.

[34] A Rand Review comment in 1995, which is still valid today for the world at large states "Our reliance on information technology has grown much faster than our grasp of the vulnerabilities inherent in the networks, systems and core technologies that knit the nation together." David C. Grompet, "Keeping Information Warfare in Perspective," Fall 1995, [http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/perspective.html], accessed May 7, 2003.

[35] Margaret Purdy, "Critical Infrastructure Protection: A Canadian Perspective." in *Fortress North America?: What 'Continental Security' Means for Canada*. Ed. by David Rudd and Nicholas Furneaux, (Toronto: The Canadian Institute of Strategic Studies, 2002), p 24.

[36] Robert Lemos, "Cyberterrorism: The real risks." Aug 2002, p 4. [http://news.zdnet.co.uk/story/0,,t269-s2121358,00.html], accessed May 8, 2003.

Clearly, the concept of creating a national emergency by disrupting or destroying a utility is debatable[37] and the efficacy of attacks against economies are questionable. According to analyst James Lewis,

> [t]he financial costs to economies from cyber attack include the loss of intellectual property, financial fraud, damage to reputation, lower productivity, and third party liability. Opportunity cost (lost sales, lower productivity, etc) make up a large proportion of the reported cost of cyber attacks and viruses. However, opportunity costs do not translate directly into costs to the national economy.[38]

To date, there is no public record of devastating cyber attacks that have imposed long-term suffering on any nation state. There is evidence that attacks have occurred, but their reach and lethality has not been impressive.[39] Indeed, although public awareness of the threat and software security enhancements are slow to take hold, [40] the natural maturing of security services and the growing sophistication of systems may give the long term advantage to defence. A recent war gaming exercise headed by the US Naval War College and Gartner Ltd suggested that it was possible to carry out a digital terrorist attack; given five years to prepare, a $200 million budget and inside knowledge of the

[37] A US analyst notes that in the US there are hundreds of similar utilities across the country that are not interconnected or using the same operating software. This significantly impedes any effort to mount a concerted, multi-front attack. As Lewis suggests, if the goal is to not let cyberwar disrupt even a single day of electricity or water, then we need to consider what happens even today with natural events. There are 54,000 separate water systems in the US alone, and systems do go out for days or more. James A Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats." *Center for Strategic and International Studies*, December 2002.

[38] *Ibid*, p 9-10.

[39] "Around 5:00 p.m. EDT on Monday,[21 Oct 2002] a "distributed denial of service" (DDOS) attack struck the 13 "root servers" that provide the primary roadmap for almost all Internet communications. Despite the scale of the attack, which lasted about an hour, Internet users worldwide were largely unaffected, experts said…Chris Morrow, network security engineer for UUNET, said "This is probably the most concerted attack against the Internet infrastructure that we've seen"." David McGuire and Brian Krebs, "Attack On Internet Called Largest Ever" washingtonpost.com Staff Writers, October 22, 2002.

[40] A real problem, though, is what is not being done to protect business and possibly government applications. The US Government's security strategy notes that in the US approximately 3,500 software vulnerabilities are reported annually, but what is not being reported? United States, "The National

systems.[41] In a sophisticated cyber world, mounting an attack requires the aggressor to navigate through a gauntlet of defences that are continually changing and improving. Rapid virus detection and updates, firewalls, isolation of networks, procedural improvements and education are continually improving defences. As well, through efforts to combat contingencies such as natural disasters, utilities and industries are reducing the potential harm of cyber attacks. Finally, although business presents a great deal more vulnerabilities than the military and government,[42] there is an encouraging trend to include more redundancies in complex networks that are susceptible to failures.

Assuming, with some caution, that CNA is a viable strategic weapon, it could be employed as a defensive response to cyber attacks against Canada and the United States. All that is needed is a bi-national organization providing clear command and control, and for both countries, effective national command authorities providing direction and approval. Clearly, key decision-making for actions that impact national policies and international relations are the purview of the national command authorities.[43] Whether or not NORAD would be the home for such a capability is a moot point, however, it does

Strategy to Secure Cyberspace," February 2003. p 32. [http://www.whitehouse.gov/pcipb/], accessed May 8, 2003.

[41] William Jackson, "War College calls a digital Pear Harbor doable," 23 Aug 2002, [http://www.gcn.com/vol1_no1/daily-updates/19792-1.html], accessed May 7,2003.

[42] "A preliminary review…suggests that computer network vulnerabilities are an increasingly serious business problem but that their threat to national security is overstated. Modern industrial societies are more robust than they appear at first glance," Lewis, A*ssessing the Risks*…., p 2.

[43] A Department of State observation in 1959 is telling, "[The Canadians are] concerned about the possibility of being involved in a course of action contrary to their national interest through CINCNORAD increasing the readiness of Canadian forces under his control without prior consultation having been accomplished between the political authorities of both countries." Ivan B. White, *CINCNORAD's Authority to Increase the State of Readiness of NORAD Forces* (Department of State, Assistant Secretary), 23 Sep 59. The US National Command Authority focuses on the President and Secretary of Defence. In Canada, it is less well understood. Although the Senate Committee on Defence has noted that our National Command Authority is always available to make decisions affecting the nation, there is no indication of how that

present an excellent model and historical reference. For example, just as the nuclear role of NORAD was always controversial,[44] it is likely that the unknown aspects of CNA would also be a sensitive issue. CNA is a weapon of unknown potential. Not only does it strike at 'hyper-speed', but also, like nuclear weapons, the strike cannot be recalled after the trigger is pulled and the results are conceivably devastating. As Major General Bruce Wright has noted, whereas 8th Air Force could strike anywhere in the world in 18 hours with cruise missiles, an offensive computer algorithm can be launched in 8 seconds.[45] Just as Prime Minister Pearson was careful to guard his authority with respect to nuclear weapons use,[46] the National Command Authorities today will cautiously considered the effects of CNA before its use.

The Standing Senate Committee on National Security and Defence noted in a report that, should Canada be passive with regard to defence, "the United States will unilaterally move to defend its security perimeter – which it primarily defines as North America – without Canadian knowledge or consent."[47] In order for a bi-national cyber organization to be effective, defensive actions must be timely and the nations in full agreement with

decision process would take place. See Canada, The Standing Senate Committee on National Security and Defence, *Defence of North America: A Canadian Responsibility*. Ottawa, September 2002.

[44] While there was tacit agreement that Canada would participate in defensive nuclear strikes, this was very much downplayed for the public. A US State Department message in 1968 notes that " Canadian Govt is also concerned that there is the possibility that issue [using nuclear weapons] may become public, and that the Govt may be faced with need to make public response in Canada. In this case, Canadian Govt, unilaterally, would respond as follows: "Provision is made for the possibility of surprise attack in such a way that military requirements are adequately met while the responsibility of the Govt for a decision to employ nuclear weapons is maintained." R. Straus, *Nuclear Weapons for NORAD*, (US Department of State Telegram), 17 Apr 68.

[45] Fulghum, *U.S. Shifts cyberwar* …., p 50.

[46] Pearson at one point reiterated to his cabinet that "he understood the principle of joint control to mean that both countries would have, in effect, a veto over the use of the nuclear weapons…[and how]…the Canadian control over use was to be exercised would have to be worked out in the light of practical military necessity…" 139th Meeting of the Cabinet Defence Committee, May 7, 1963 para 14.

those actions. If action is taken unilaterally, then the authority of the alliance is weakened and if the nations are sidetracked waiting for consensus, then initiative and resolve are lost. But what circumstances would sabotage timely agreement between the two nations? The answer is in our differences. The two nations approach decision-making from different perceptions, traditions and motivation, and they may not necessarily arrive at the same decision in a timely fashion, if ever. Consider John Boyd's well known command and control model, the Observe-Orient-Decide-Act, or OODA loop.[48] Boyd, in one of his last presentations, notes the importance of orientation.

> The second "O," orientation--as the repository of our genetic heritage, cultural tradition, and previous experiences--is the most important part of the O-O-D-A loop since it shapes the way we observe, the way we decide, the way we act.[49]

Thus, even though there may be a direct attack against our nations or an imminent threat of one, the speed in reaching critical decisions is highly dependant on the attitudes of our national command authorities. Although this deduction is somewhat evident, it becomes obvious when one compares Canadian and US reactions to the questions: do we respond and what do we respond with?

Given a cyber attack has occurred, or there is the threat of one, the first step for the partnership is to quickly agree whether or not to respond. For the monitoring organization, a key task would be to determine the intent of the aggressive act and who

[47] The Standing Senate Committee on National Security and Defence, *Defence of North America: A Canadian Responsibility*. (Ottawa, September 2002). p 24.
[48] See Grant T. Hammond, "The Essential Boyd," [http://www.belisarius.com/modern_business_strategy/hammond/essential_boyd.htm], accessed May 2003.
[49] John R. Boyd, "Organic Design for Command and Control," May 1987, [http://www.belisarius.com/modern_business_strategy/boyd/organic_design/organic_design_frameset.htm] accessed May 7, 2003.

initiated it in order to give the national command authorities enough information to plan a response. The difficult task of identification is made harder because cyber weapons are not just found in the arsenals of responsible states, they are the tools of non-state actors, rogue states and "cut-outs", that is, third party attackers working for a state government. Furthermore, their use is not reserved for time of war or solely against military or state infrastructure. The anonymity of the cyber weapon forces the defender to apply precious time to determine if it is significant enough to be an act of war.[50] Should disagreement over the threat be added to this scenario, the critical decision point becomes a point of divergence and possibly paralysis. As an example, one of the early concerns in NORAD was the command "ambiguity between CINCNORAD and his Deputy, [and how it] would become relevant where their threat assessments differed."[51] Asserting that a speedy response is critical, the national command authority's decision-making cycle will be reduced. Although the chances of this may be slim, it is a potential handicap for the bi-national decision-making process.

Should both Canada and the US agree that a cyber attack had been perpetrated by a state and constituting an act of war, what then? According to international law, specifically Article 51 of the UN Charter, if an armed attack occurs, self-defence is acceptable.[52] Thomas Wingfield asks in reference to this situation, "is a computer network attack an

[50] Of course knowing the intent of the weapon presupposes knowing who initiated the attack and their motivation. Because of the nature of the global information grid, this information will be very difficult to ascertain unless the aggressor sends a signature of some type.

[51] David J.R. Angell. "NORAD and Binational Nuclear Alert: Consultation and Decisionmaking in the Integrated Command." *Defence Analysis*, Vol 4, No 2 (1988), p 133.

[52] Article 51 states that "nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations." See UN Charter, Department of National Defence. B-GG-005-027/AF-022 *Collection of Documents on the Law of Armed Conflict- 2001 Edition*, Ottawa: DND Canada, 2001.

‘armed attack’ that justifies the use of force in self-defence?”[53] The answer is that there is clear support for the proposition that self-defence is warranted against acts other than classic armed attacks.[54] Thus, if the alliance (or either me decisions. Thus, when it comes to defending the homeland, there is no firm foundation to provide detailed guidance and hold authorities from drifting around solutions. Brigadier General (Retired) Macnamara provides an additional negative view of national direction in that in the absence of a clear definition of national interest, our foreign and defence policy is developed in an ad-hoc manner, "reflecting the personal interests of politicians and officials,"[56] and there is no consistent national security policy-planning framework within the key government offices.

Without firmer direction and guidance, Canadian decision-making is a case of improvisation, inevitably a lengthy process and bound to be out of sync with the United States. NORAD provides a relevant historical example. During the Cuban missile crisis, the US Continental Air Defence Command (CONAD) declared Defence Condition (DEFCON) 3, 22 Oct 62,[57] a decision that affected all USAF forces assigned to NORAD, while Canada, after cabinet deliberation, 'officially' went to DEFCON 3 two days later.[58] Incredibly, prior to government action, the Royal Canadian Navy put to sea to shadow Soviet submarines in the Atlantic, and the Royal Canadian Air Force (RCAF) went on alert, ready to launch against bombers.[59]

[55] The Standing Senate Committee on National Security and Defence, *Defence of North America: A Canadian Responsibility*. Ottawa, September 2002. p 49.

[56] W.D. Macnamara, and Ann Fitz-Gerald. "A National Security Framework For Canada", *IRPP – Policy Matters*, Vol 3, No 10, (October, 2003), p 12.

[57] National Archives, "Narative Report, Ottawa NORAD Sector, Edgar, Ontario 1 Jun 62 - 30 Nov 62," [http://www.pinetreeline.org/misc/misc11.html], accessed 7 May 03.

[58] The US Secretary of State was informed 24 Oct, 1962 that "Cabinet at meeting this morning has authorized Defence Minister Harkness to invoke for Canadian Air Force (NORAD only)…DEFCON 3." Priority Message No 541, US Department of State Telegram, Ottawa, October 24, 1962.

[59] J.L Granatstein, "A Friendly Agreement in Advance: Canada-US Defence Relations Past, Present, and Future." *C.D. Howe Institute Commentary*, No 166 (June, 2002), p 5.

According to some, Canada should be better equipped for guiding senior decision-makers against threats. In the Senate Committee record of proceedings, Professor Bland is identified as stating that a national security policy should concentrate on the means to mitigate threats and to address vulnerabilities at the same time. Furthermore he outlined what should be in that policy, to include a statement of purpose, that is, a clear description of what is to be secured, from what, from whom, etc.[60] Clearly, without the right tools, an efficient process for addressing threats is missing. As long as we do not have this assistance and decisions are tardy, it is highly probable that there would be lost opportunity to show resolve and strike as a coalition when the impact would be greatest. The problem is compounded if we cannot agree on the legitimacy of the threat. Referring to NORAD again, Angell suggests that "there are no grounds for assuming that the confusion which characterized the 1962 response [to the Cuban missile crisis] could not rise again, were Canada again asked to increase her alert level."[61]

In the situation where an attack against the alliance has not occurred but appears imminent, another conundrum arises. Article 51 of the UN Charter makes it clear that collective self-defence is authorized if an armed attack occurs against any one of the states,[62] however agreement over what constitutes an attack is not spelled out. From a US perspective, the trigger for action in self-defence ranges well beyond the physical attack. As noted lawyer Richard A. Falk suggests:

[60] The Standing Senate Committee on National Security and Defence, *Canadian Security and Military Preparedness.* Ottawa, February 2002. p 51.
[61] Angell, "NORAD and Binational…., p 136.
[62] In fact it is spelled out as "a member state of the UN" which in this case reflects both the US and Canada.

> [a]lthough it is true that no agreed definitions of self-defence exist, there has been a general acknowledgment that the core meaning of self-defence relates to responses against either an actual armed attack or a credible impression of imminent armed attack.[63]

In the case of no-nonsense, assertive states such as the US, and the now defunct Soviet Union, the inference is obvious, respond with purpose! For example, the Soviet Union argued that the 1960 Gary Powers U-2 reconnaissance over-flight of their territory was an act of aggression because of its unknown mission and was, therefore, justifiably shot down.[64] Wingfield provides the legal cover for cyber attack, writing that anticipatory self-defence is permissible, based on the need to protect sensitive systems of vital national interest. If the intruder is known, then the victim state can "lawfully respond in anticipatory self-defence with a necessary and proportional use of force, either in kind through cyberspace or by more traditional uses of force."[65] The US Executive Branch has, of course, already signaled in their Security Strategy readiness for pre-emptive action should they believe the threat is valid.[66]

[63] Richard A. Falk, "The Cambodian operation and international law." *American Journal of International Law.* 65 no. 1 (January 1971): p 17. The classic precedence for attacking in self-defence is the "Caroline incident" as described by John Bender. "An armed body of men, acting under the orders of a British officer, crossed from Canada into the United States and destroyed the Caroline, a ship that had been used by Canadian insurgents." From this incident, Daniel Webster summarized that to justify the destruction, the attackers would have to demonstrate a "necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment of deliberation." Letter from Daniel Webster to Mr. Fox, April 24, 1841. in British Parliamentary Papers, Vol 61 (1843),quoted in John C. Bender, "Self-defence and Cambodia: a critical appraisal." *Boston University Law Review* 50 (Spring 1970) Reprinted in Falk, Richard A., ed. Vietnam War and international law. Princeton, NJ: Princeton University Press, 1972. v. 3 p 142. See also Wingfield, *The Law of….*, p 451.

[64] Wingfield, *The Law of….*, p 96.

[65] *Ibid*, pp 355-6.

[66] The US National Security Strategy states, "the United States has long maintained the option of preemptive actions to counter a sufficient threat to our national security. The greater the threat, the greater the risk of inaction – and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack. To forestall or prevent such hostile acts by our adversaries, the United States will, if necessary, act preemptively." "The National

Even though the US embraces the ideals of international order and law,[67] the nation will only support rules that allow its independent action and autonomy, as demonstrated by the Administration's refusal to ratify the International Criminal Court treaty.[68] In fact, the US has signaled a clear position in their draft *Secure Cyberspace* policy document regarding the consequences of a cyber attack on them. Should there be sufficient cause,

> [w]hen a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies.[69]

In contrast, Canadian political authorities are committed to UN leadership and guidance. Prime Minister Chrétien has recently reaffirmed his policy that Canada will work within the greater mandate of multilateral organizations such as the United Nations."[70] Thus, there can be no doubt that Canada would aspire to the more collegial approach of UN Charter Article 2(3), "all members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not

Security Strategy of the United States of America." September 2002. p 15, [http://www.whitehouse.gov/nsc/nss.html], accessed May 7, 2003.

[67] Faulk states, "the [UN] Charter is a treaty that has been ratified with the advice and consent of the Senate, and is, according to the U.S. Constitution, part of the supreme law of the land." Falk, *The Cambodian….*, p 9.

[68] In a letter to Secretary General Kofi Annan, the US Under Secretary of State for Arms Control and International Security wrote, "This is to inform you, in connection with the Rome Statute of the International Criminal Court adopted on July 17, 1998, that the United States does not intend to become a party to the treaty. Accordingly, the United States has no legal obligations arising from its signature on December 31, 2000. The United States requests that its intention not to become a party, as expressed in this letter, be reflected in the depositary's status lists relating to this treaty." John R. Bolton, "International Criminal Court" [http://www.state.gov/r/pa/prs/ps/2002/9968.htm], accessed May 6, 2003.

[69] United States, "The National Strategy to Secure Cyberspace." February 2003, p 59, [http://www.whitehouse.gov/pcipb/].accessed May 7, 2003.

[70] "All members must reaffirm our fundamental commitments to the multilateral institutions which have served the world so well…Canada believes in a multilateral approach, where the world community, through the accepted, mandated and established focus of the United Nations can project its collective will in the interest of international peace and security." Jean Chretien, "The Road to Baghdad leads through the UN," IRPP - Policy Opinions, April 2003, [http://www.irpp.org/po/], accessed May 7, 2003.

endangered."[71] At a more practical level, Canada might have a problem with anticipatory coalition strikes, given the reality that the US has far more enemies ready to attack them than Canada does. Far removed from the Cold War days, where there was one mission, a known ideological enemy and low probability of a war, world associations today are fluid and complex. Therefore, it is highly unlikely that Canada would ever be in consonance with US pre-emptive action against a foreign state, certainly in any timeframe necessary to make the response decisive. The implications of partnership with the US defending against cyber attacks are far more dangerous for our peace than our membership in NORAD during the bi-polar superpower days. Lastly, a study of NORAD leads to an important assessment of US feelings towards hesitation. As Angell suggests,

> assurances of consultation are offset by indications that consultations would not take place…the requirement for secrecy and speed would weigh more heavily on American actions in time-urgent situations than would their commitment to consult with Canada, particularly where such consultation risks anything but Canadian consent.[72]

Whereas timely bi-national agreement to attack is likely difficult to achieve, gaining agreement over what cyber weapons to use presents an even greater problem. Strategic computer network attack represents a new, untested frontier and although there may be weapons in the arsenal, the international legal basis for their use is unresolved. Consequently, there is limited national guidance to follow in the use of such weapons. It may be simple for Canada and the US to agree that cyber weapons are non-

[71] This theme continues in UN Charter Article 33. Parties shall "seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice."

[72] A clear departure from a common understanding that our agreement would be necessary even in the most extreme crisis. Angell, *NORAD and Binational…*, p 134.

discriminatory;[73] however, the principles of military necessity, distinction, proportionality and neutrality present greater problems for bi-national agreement.[74]

"Military Necessity presupposes that the use of force is necessary to achieve the [quick and least destructive] submission of the enemy."[75] In this case it is the leadership practicing the art of cyberwar, sagely employing effects based targeting to reach Decisive Points and impact the postulated Center of Gravity. On the one hand, military objects that can be identified and isolated are straightforward targets. On the other hand, targeting loosely connected, strategic objects is problematic. For example, a desirable effect might be to halt the war material support for a nation. This could be done by disrupting a nation's economic system and rendering their currency unstable, which would cause a loss of international confidence and war financing capability.[76] The unfortunate second order effect on innocent members of society could be rationalized as a small price to pay for expediency. However history has shown, as Bayles suggests, that when a nation is targeted, "economic attacks cause widespread civilian suffering long before any noticeable effect might occur on the military potential of a warring nation."[77]

[73] Non-discrimination affirms that the Laws of Armed Conflict (LOACs) are not to be applied in a different fashion for discriminatory reasons. Suffice to say, attack discrimination is related to the accuracy of the weapon. Just as iron bombs are highly non-discriminate, so too are attacks such as computer viruses. Discrimination might become an issue when computer attack fidelity is improved; however, this seems highly unlikely. Arguably, the more sophisticated, tolerant and conformist to international laws and norms we become, the less likely is the chance that discrimination would be a target criterion. Additionally, as a strategic weapon, it is hardly likely that it would be used without the collective deliberation of a senior military and national security group. CNA will always remain a highly 'egalitarian' weapon.

[74] Department of National Defence, B-GG-005-027/AF-021 *The Law of Armed Conflict at the Operational And Tactical Level –Annotated*, Ottawa: DND Canada, 2001, p 2-2.

[75] *Ibid*, p 2-1.

[76] As Wingfield notes, during Desert Storm the US targeted the electrical power system in Baghdad – a lawful military target; however, the Iraqis portrayed it as an act of attempted genocide because the interruption of the sewage pumps in the city could have resulted in an epidemic disease. The scenario would surely be the same if it had been a computer attack. Wingfield, *The Law of….*, p 442.

[77] Bayles, "The Ethics of…., p 50.

The solution, in keeping with our doctrine, is to conduct proper targeting assessments and bi-national agreement before responding.[78] With the vagueness of the weapons, and varied opinions related to acceptable effects, bi-national consensus would certainly be difficult to achieve.

“[D]istinction imposes an obligation on commanders to distinguish between legitimate targets and civilian objects and the civilian popul38.760 1i.

attack "despite its negligible lethality, it nonetheless violates the principle of noncombatant immunity."[83]

Proportionality "implies that collateral civilian damage arising from military operations must not be excessive in relation to the direct and concrete military advantage anticipated."[84] This issue addresses targeting facilities and services that overlap the civilian and military realms. One effect sought might be the degradation or disruption of the military command and control system or air traffic service. The action might be taken, indirectly, by shutting down power grids, flooding commercial communication nodes and disrupting or spoofing air traffic control software. However, the propagation of the weapon on commercial networks is unknown and therefore the effect on unrelated infrastructure and services beyond the borders of the enemy is not predictable. It seems then, that one would have difficulty satisfying the proportionality measure for a cyber attack. Indeed, many analysts recognize this.[85]

Neutral countries are not immune from cyber war. The aspect of striking from a distance "means that attackers may navigate numerous third-party nations, which may or may not approve of the attack or the means used."[86] As a point of distinction, Wingfield, citing the Hague Conventions, surmises that belligerents can expect to use third party communications facilities without restriction, however, it is clear that information processing or generation by a neutral country is prohibited and could be stopped in self-

[83] John Aquilla. "Ethics and Information Warfare." p 395, [http://www.rand.org/publications/MR/MR1016/MR1016.chap13.pdf], accessed May 7, 2003.
[84] Department of National Defence, B-GG-005-027/AF-021 *The Law of...,* p 2-3.
[85] For example, Wingfield, *The Law of…,* Bayles, *The Ethics of….,* Arquilla, *Ethic and….,*

defence.[87] The US used the argument of self-defence to justify their incursion into Cambodia in 1970, arguing that neutral Cambodia would not (and could not) fulfill its obligation to evict the North Vietnamese and Viet Cong from their 'sanctuary bases' and thereby protect Americans.[88]

In terms of neutrality, the US has shown in the past it is prepared to attack neutral countries hosting known enemies and threats. Canada, on the other hand, has built foreign relationships that differ in scope and purpose from the US, and encompass differing friendships. Thus, a unilateral US attack against a neutral country could alienate Canada from many friends and further raise domestic ire.[89] Indeed, the problem may be impossible to avoid given the complexity of the cyber world, and our reluctance to support would only serve to erode any bi-national cyber defence relationship.

The principle characteristic that distinguishes Canada and the US from shadowy aggressors is our adherence to the Laws of Armed Conflict (LOACs) and the principles

[86] Bayles, "The Ethics of…., p 46.

[87] Wingfield, *The Law of*…., p 444.

[88] William. H. Rehnquist in defence stated,"[t]he President feels… that he has an obligation as Commander-in-Chief to take what steps he deems necessary to assure the safety of American Armed Forces in the field." William H. Rehnquist, "The Constitutional Issues – Administration Position," in *The Cambodian incursion: legal issues: proceedings of the Fifteenth Hammarskjold Forum.* Edited by Donald T. Fox. Dobbs Ferry, NY: Published for the Association of the Bar of the City of New York by Oceana Publications Inc., 1971, p 14.

[89] Following current events, one might have the sense that some Canadians take the position that 'my neighbor's enemy will be my friend'. As Jack Granatstein stated to SCONDVA on 18 Feb, 2003, "Canada clearly does not want to accept its global and continental responsibilities. Instead we want only to be a moralizing do-gooder, the world's moral superpower. We fear terrorism and global instability, but we appear to fear the United States more, an attitude springing from our endemic and unworthy anti-Americanism." J.L. Granatstein, "Presentation to the House of Commons Standing Committtee on National Defence and Veterans Affairs," [http://www.ccs21.org/articles/feb03/scondva_feb18-03.pdf], accessed May 7, 2003. Granatstein has also characterized Canada as "a defence freeloader, and like sponges everywhere, we dislike those who carry the burden for us." J.L. Granatstein, "A Friendly Agreement in Advance: Canada-US Defence Relations Past, Present, and Future." *C.D. Howe Institute Commentary*, No 166 (June, 2002). p 16.

that support them. Wingfield could be speaking for Canada when he states, "it is a firmly established position of the United States that US forces will fight in full compliance with the law of war."[90] But, absent guidance from international law, what is tolerable for one may not be for the other. Where the US is prone to sidestepping or meandering around agreements if nationally advantageous,[91] Canada seeks consensus and invariably falls in with the global community. Given the nature of US international actions, evidence from their past dealings with adversaries, and their efforts at building up a CNA capability, it is highly probable that a US Administration would sanction cyber weapon use. Canada, given the unknown legal status of cyber weapon use, would be extremely unlikely to do the same. These differences are clearly not conducive to a viable bi-national cyber defence organization.

In the domain of national and continental defence, it is a reasonable expectation that Canada and the United States would work as one team. As well, in this time of growing interest in cyber warfare, where there is a move throughout many nations to develop this capability, it is only natural to envision Canada – United States interoperability in the development of a bi-national cyber organization with computer network attack capability. If this did occur, we would likely want a "NORAD-like" command and control structure with reach-back to the national command authorities. This organization would be tasked to guard against cyber attacks and engage in attack when required.

[90] Wingfield, *The Law of….*, p 442.

[91] For example, the legal basis for the 1970 US incursion into Cambodia has never been unanimously upheld. Additionally, the US unilaterally cancelled the Anti-Ballistic Missile Treaty, which has removed a restraint on National Missile Defence development. Lastly, the US has not followed the international community, including Canada, in supporting the International Criminal Court and the 1996 'Landmine Treaty'. Although the US belongs to the UN Committee on the Peaceful Uses of Outer Space, military development through the Department of Defence is not precluded.

Recognizing that the efficacy of the bi-national cyber defence organization will depend on timely and unified action, when we consider the characteristics of national decision-making, the effectiveness of such an organization is questionable. Canada and the US have significant differences that would make it difficult for each to answer at the same time: do we respond and how do we respond? In the first place, if there is a cyber attack against the continent, the US is prepared to respond without hesitation. Canada is not. Canada, historically, looks to consultation and debate before key decisions are made, while the US has clear guidance in this regard. Examples from NORAD show that the alliance has had difficulties before in critical situations where timely decisions were needed. Secondly, the US has signaled a clear message to all adversaries that it is ready to respond preemptively to any national threat. This goes against the principles of the UN Charter, which is a hallmark of international relations and a key guide for Canada. Thirdly, significant portions of the principles that underpin the laws of armed conflict have not been adapted to cyber war. That has not stopped the development and potential use of cyber weapons, even among responsible nations. In the case of the US, it is highly conceivable that they would resort to using cyber weapons should they be attacked in a like manner. For Canada, because their legal status remains unclear, it is highly unlikely that we would follow suit. Canada has a history of following the international community and solidly supporting international law.

Notwithstanding the NORAD example of success in the defence of North America, there is little convincing evidence to suggest that Canada and the US would promptly agree to use cyber weapons if the need arose. Furthermore, it is difficult to believe that there would be any agreement regarding what weapon to use or what targets to attack. In truth, because there is little chance of timely and unified action, such a bi-national cyber defence organization would be impotent and meaningless. That is not to say that activities in the area of cyber defence should halt. There is evidence that cyber war is a menace for the future and we should be prepared for it. Certainly our allies will continue their work in this area and it is to our benefit to share knowledge and procedures with them. For our protection, though, Canada must maintain vigilance against cyber threats and ultimately be capable of defeating any cyber attacks directed against us.

Lastly, to quote an old carpenter's axiom; "measure twice and cut once." Indeed, it is natural and responsible to avoid making hasty decisions that could lead to embarrassment. Canada should continue to develop expertise in the area of computer network attack but definitely think twice before committing to a bi-national computer network attack capability.

Bibliography

Allen, LCol Francis. "CN(EH?): Should the CF Adopt Computer Network Exploitation and Attack Capabilities?" *Canadian Forces College Review 2002*

Angell, David J.R. "NORAD and Binational Nuclear Alert: Consultation and Decisionmaking in the Integrated Command." *Defence Analysis*, Vol 4, No 2 (1988), pp 129-146.

Arquilla, John, and David F. Ronfeldt. "The Advent of Netwar". RAND, AS36 R288 no 789. (1996).

Arquilla, John. "Ethics and Information Warfare." [http://www.rand.org/publications/MR/MR1016/MR1016.chap13.pdf]. 1999.

Bayles, William J. "The Ethics of Computer Network Attack." *Parameters* (Spring, 2001) pp 44-58.

Bender, John C. "Self-defence and Cambodia: a critical appraisal." *Boston University Law Review* 50 (Spring 1970) Reprinted in Falk, Richard A., ed. Vietnam War and international law. Princeton, NJ: Princeton University Press, 1972. v. 3 pp 138-147.

Boyd, John R. "Organic Design for Command and Control," [http://www.belisarius.com/modern_business_strategy/boyd/organic_design/organic_design_frameset.htm]. May 1987.

Canada, Department of National Defence. B-GG-005-027/AF-021 *The Law of Armed Conflict at the Operational And Tactical Level –Annotated*, Ottawa: DND Canada, 2001.

Canada, Department of National Defence. B-GG-005-027/AF-022 *Collection of Documents on the Law of Armed Conflict- 2001 Edition*, Ottawa: DND Canada, 2001.

Canada, Department of National Defence, Chief of the Defence Staff. *Strategy 2020, Canadian Defence in the 21st Century*, [http://www.cds.forces.gc.ca/pubs/strategy2k/s2k07_e.asp], May 2003

Canada, The Standing Senate Committee on National Security and Defence, *Defence of North America: A Canadian Responsibility*. Ottawa, September 2002.

Canada, The Standing Senate Committee on National Security and Defence, *Canadian Security and Military Preparedness.* Ottawa, February 2002. [http://www.parl.gc.ca/37/1/parlbus/commbus/senate/com-e/defe-e/rep-e/rep05feb02-e.pdf]

Clemmons, Commander Byard Q. and Brown, Major Gary D. "Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction." *Military Review*, September-October, 1999, pp 35-45.

Crosby, Ann Denholm. "A Middle-Power Military in Alliance: Canada and NORAD." Journal of Peace Research, Vol 34, Issue 1 (February, 1997), pp 37-52.

Falk, Richard A. " The Cambodian operation and international law." *American Journal of International Law.* 65 no. 1 (January 1971): pp 1-25.

Fulghum, David A. and Wall, Robert. U.S. Shifts Cyberwar To Combat Commands." *Aviation Week & Space Technology*, February 26, 2001, pp 50-1.

Gompert, David C. "Keeping Information Warfare in Perspective." *RAND Research Review*, Vol XIX, No 2, (Fall, 1995).

Granatstein, J.L. "A Friendly Agreement in Advance: Canada-US Defence Relations Past, Present, and Future." *C.D. Howe Institute Commentary*, No 166 (June, 2002).

Hildreth, Steven A. "Cyberwarfare." *Congressional Research Service, The Library of Congress*. Order Code RL30735. June 19, 2001.

Lemos, Robert. "Cyberterrorism: The real risks." [http://news.zdnet.co.uk/story/0,,t269-s2121358,00.html]. 2002.

Lewis, James A. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats." *Center for Strategic and International Studies*, 2002.

Macnamara, W.D. and Fitz-Gerald Ann. "A National Security Framework For Canada", *IRPP – Policy Matters*, Vol 3, No 10, (October, 2003).

Mets, David R. *The Air Campaign: John Warden and the Classical Airpower Theorists*. Alabama: Air University Press, 1999.

Middlemiss, Danford and Stairs, Denis. "The Canadian Forces and the Doctrine of Interoperability: The Issues." *IRPP – Policy Matters*, Vol 3, No 7, (June, 2002), pp 1-40.

Moore, David, Shannon Colleen and Brown, Jeffery. "Code-Red: a case study on the spread and victims of an Internet worm," *Proceedings of the Second the ACM Internet Measurement Workshop*, 2002, [http://www.caida.org/outreach/papers/2002/codered/codered.pdf], 2002.

Moore, David, Paxson, Vern, Savage, Stefan, Shannon, Colleen, Staniford, Stuart and Weaver, Nicholas. "The Spread of the Sapphire/Slammer Worm," [http://www.cs.berkeley.edu/~nweaver/sapphire/], Feb 2003.

Piazza, Peter. “Who’s Winning the Cyberwars?” *Security Management*, Dec 2002, pp 71-8.

Purdy, Margaret. “Critical Infrastructure Protection: A Canadian Perspective.” *Fortress North America?: What ‘Continental Security’ Means for Canada*. Edited by David

Rehnquist, William H. “The Constitutional Issues – Administration Position,” in *The Cambodian incursion: legal issues: proceedings of the Fifteenth Hammarskjold Forum.* Edited by Donald T. Fox. Dobbs Ferry, NY: Published for the Association of the Bar of the City of New York by Oceana Publications Inc., 1971.

“U.S. Notification of Intent Not to Become a Party to the Rome Statute.” *American Journal of International Law*, Vol 96, Issue 3 (July, 2002) p 724.

United States, “The National Security Strategy of the United States of America.” [http://www.whitehouse.gov/nsc/nss.html]. September 2002.

United States, “The National Strategy to Secure Cyberspace.” [http://www.whitehouse.gov/pcipb/]. February 2003.

Wingfield, Thomas C. *The Law of Information Conflict: National Security Law in Cyberspace*. Falls Church: Aegis Research Corporation, 2000.

Williams, Phil, Shimeall, Timothy and Dunlevy, Casey. “Intelligence Analysis for Internet Security.” *Contemporary Security Policy,* Vol 23, No 2 (August, 2002) pp 1-38.