Research Essay

NEW CONSIDERATIONS FOR CANADA'S NATIONAL SECURITY IN THE INFORMATION AGE

by

Colonel Richard A. Hatton

Advanced Military Studies Course 1

Canadian Forces College

02 November 1998

NEW CONSIDERATIONS FOR CANADA'S NATIONAL SECURITY IN THE INFORMATION AGE

Introduction

Communications are shrinking the world into a global village. Computers pervade nearly all walks of life and both information and knowledge are growing at explosive rates. Canada and other developed nations are entering the Information Age.

Conceptions of what threatens national security and how to deal with these threats have continued to change over the years. Increased reliance on networked computer-based information technology and systems, which are vulnerable to failure, interference and sabotage, has created new risks to national security. The more dependent we are on networked information systems for decision making and the operation of critical services, the more vulnerable we are to hostile manipulation of those systems.

The aim of this paper is to show that in Canada, the Government must better co-ordinate intelligence and security-related processes and activities at the national level, if we are to deal effectively with existing and emerging security threats to our information systems and critical infrastructure.

Governments, the Armed Forces and the private sector, increasingly dependent on these networks as well as inter-dependent, must pay attention to these new risks. Canada must develop strategies, policies and plans to defend against these threats and vulnerabilities; it cannot afford to wait for a catastrophe. With recent memories of the 1998 Ice Storm, and now making preparations to deal with the looming "Year 2000 Millennium Bug" political leaders and national policy makers are just beginning to appreciate the nature and extent of the threat posed by information warfare to national security.

This paper is focussed at the strategic level. It will briefly introduce the nature of Information Operations, especially as it relates to the threat to computer-based information

systems and critical infrastructure in Canada. It will discuss the link between information systems security and issues of national security, public safety, economic prosperity and public confidence in Government. It will review activities under way in Canada to deal with threats to information systems security, including plans to prepare for the Year 2000. Finally, the paper will recommend an integrated approach for the Government of Canada to take defensive measures to meet this new challenge.

Information Operations

The field of Information Operations is relatively new, although information and how it is used, protected and communicated in operations has long been of interest to military professionals and security-oriented academics. However, since vulnerabilities to information systems extend well outside of defence departments and universities, military forces and scholars alone cannot address the problem.

What is the threat posed by Information Warfare? Much has been written on the subject in recent years, although the body of literature originating in Canada is not rich. Most material is from the United States, where the academic and military communities are heavily involved and where national-level political leadership seems to perceive the need to defend national interests by protecting information systems. The world's pre-eminent political, military and economic power, the United States is also arguably the most tempting target for attacks on its information-based computer systems. This is significant to Canada, considering its close military, industrial and financial links to the US. The United States and other developed countries, to varying degrees, are beginning to take action to defend themselves from attacks on those systems, as well as to develop offensive capabilities.

Information Warfare is about destroying information, reducing information flows, reducing the reliability of information content and denying access to services.[1] Winn Schwartau states:

[1] Matthew G. Devost, "National Security in the Information Age." Thesis prepared in fulfillment of a Masters degree. (University of Vermont, May 1995) http://www.terrorism.coco 845co

> Information Warfare is waged against industries, political spheres of influence, global economic forces, or even against entire countries. It is the use of technology against technology; it is about secrets and the theft of secrets; it is about turning information against its owners; it is about denying the enemy the ability to use both his technology and his information.[2]

Information warfare did exist in industrial and even pre-industrial societies,[3] although protecting information was still considered to be much less important than protection of the fighting power of the armed forces and the production capability of the industrial base. In today's information-based societies, Information Warfare poses a much higher threat than it did in the Industrial Age. Matthew Devost suggests that historical patterns reveal that information warfare may be the warfare of the future. He also states "… not only is Information Warfare an entirely new paradigm for waging war, it must also be adopted as a supplement to traditional and conventional means of warfare if successful campaigns are to be waged."[4]

This new type of warfare is breeding new weapons. Although the scope of this paper precludes a detailed study of the full range of technological capabilities of our potential adversaries, it is important to have some understanding of the technical nature of the threat.

High Energy Radio Frequency (HERF) guns are essentially special radio transmitters which are able to direct enough energy at a target, such as a computer network, to overload its electronic circuitry and disable it, at least temporarily. Electromagnetic Pulse Transformer (EMP/T) bombs operate under the same principle as HERF guns but they are much more powerful, causing permanent damage to systems.[5] EMP/T bombs detonated over densely

---

[2] Winn Schwartau, Information Warfare: Chaos on the Information Highway (New York: Thunder's Mouth Press, 1994) 291

[3] Sun-Tzu, the ancient Chinese military strategist, certainly understood the value of Information Warfare. See Sun-Tzu, The Art of Warfare (New York: Ballantyne Books, 1993). Also see John Arquilla and David Ronfeldt, in "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict" (Rand Research Review, Fall 1995) (http://www.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html) who relate how the ancient Mongols and the more recent combined forces of North Vietnam and the Viet Cong fought successfully according to cyberwar principles, each organised more like a network than a hierarchy.

[4] Devost 9

[5] Schwartau 179-180

populated urban areas could cause complete failure of communications and electronic equipment and power blackout.[6]

System intrusion or "hacking" is the electronic penetration of networked information systems for purposes of information gathering, alteration or sabotage. Emissions-capture and espionage may be accomplished by special, yet inexpensive devices. Computer viruses and other special programmes can be introduced surreptitiously into networked systems to destroy, modify or corrupt data, databases and hardware.[7] Furthermore, innocent human error and natural disasters can interrupt or even destroy information systems.

The extent of the threat to our information systems should not be exaggerated, but neither should it be underestimated. The technology to produce functioning HERF guns and EMP/T bombs exists today. The literature is replete with examples of hackers who, either for fun, ideology or profit, have intruded into some of the most sensitive data of military, government, financial and commercial institutions.

> Politically and strategically, there are many attractions to state-sponsored information warfare. It is low-cost, timely, not location-specific, provides no early warning, is not taboo, inflicts low human life costs, and can be waged in complete anonymity.[8]

In 1994, Robert Ayers, Chief of the US Center for Information Systems Security, reported that a special government team assigned to test the vulnerability of US Government systems, using hacker tools freely available on the Internet, was effective in 88% of attempts to penetrate systems. Ninety-six percent of these penetrations went undetected and 95% of the detections were unreported. Ayers also estimated that US government systems were illegally accessed, though not necessarily maliciously, at least 300,000 times a year.[9]

---

[6] Devost 10
[7] Devost 10-12. Other special programmes include logic bombs, Trojan horses and worms.
[8] Devost 17
[9] Devost 16

US Government experts note that cybercrime involves penetrations of banking and financial institutions by organized crime and drug cartels for the purposes of money laundering, illicit transfers and extortion. The hesitancy of financial institutions to report losses related to lapses in information security creates extremely lucrative possibilities for those with the tools, knowledge and daring to intrude into fat and vulnerable financial information systems and accounts.

Attacks on US Department of Defence computer systems, involving theft, modification and destruction of both data and hardware have been costly and damaging. In some instances unwanted "back doors" have been installed to circumvent normal system protection and to allow attackers unauthorised future access. Entire systems and networks have been shut down. Although no one could possibly know the exact number, the US Defence Information Systems Agency (DISA) estimates that the Defence Department may experience approximately 250,000 attacks a year and that the number is increasing.[10] Since 1992, DISA experts using the Internet attempted to penetrate computer systems at various US military and defence agency facilities. They reported in January 1997, that in 38,000 "test" attacks, successful access was gained 65% of the time, 96% of these attacks were undetected and 73% of detected attacks were unreported.[11]

Defence systems are enticing targets for attackers for a number of reasons. Enemies may want to steal information of intelligence value. Terrorists may want to access information to assess other weaknesses for attack or to directly interfere with military and other security operations. Important research information could be accessed for competitive advantage. There is potential for monetary gain through direct access to financial systems and accounts, although this might be less profitable than accessing private sector banks and financial systems.[12] Certain individuals, whether for political purposes or just for mischief, may wish to access information to

[10] If this number is correct, Ayer's preceding estimate of 300,000 attacks each year for all US Government systems seems low. However, the estimated total number is not as important as the recognition that the large number of intrusions is a serious problem.
[11] Clarence Robinson, "Western Infrastructures Face Rogue Data Stream Onslaught," Signal Magazine (Jan 1997) http://www.us.net/signal/Archive/Jan97/Western-jan.html 2
[12] Robinson 5

embarrass the government or the armed forces. Some are motivated simply by the personal challenge.

This threat is not fiction. Significant attacks on military systems have occurred and others could occur. A sixteen-year-old hacker from Britain was able to infiltr426.20349 626.1940006r41 626.15

twit.

jeadinspe(ctiovdetailst)Ti-0.00131 Tc -0

> biological weapon, could be a software bomb or computer virus that attacks a nation's commercial information infrastructure to devour a multi-trillion dollar economy in a single afternoon.[15]

Information Warfare may we waged by the government and armed forces of a rival nation-state against another. Illicit groups involved in terrorism, proliferation of weapons of mass destruction or drug smuggling, could employ it. It might even involve activist or advocacy groups with environmental, human or animal rights, social or religious agendas.

Information operations act on the information environment, but the objective is the decision-maker. As defined in the Canadian Forces (CF) Publication B-GL-300-005/FP-000 Information Operations:

> Information Operations are continuous military operations within the Military Information Environment that enable, enhance, and protect the commander's decision-action cycle and mission execution to achieve an information advantage across the full range of military operations.[16]

Current thinking within the specialist staff in the CF Information Operations Group is that the above definition does not sufficiently take into consideration the need for co-ordinated military and civilian action to both protect and exploit the value of information vulnerabilities, and to prevent a potential adversary from doing the same. The new definition in favour, but not yet incorporated into published CF doctrine, is:

> Information Operations are actions taken in support of political and military objectives which influence decision-makers by affecting adversary information, while exploiting and protecting one's own information.[17]

---

[15] Robinson 4

[16] Canadian Forces Publication, B-GL-300-005/FP-000 Information Operations, 17. The same definition appears in the earlier CFP 300-1 Conduct of Land Operations – Operational Level Doctrine for the Canadian Army.

This intent of the latter definition is preferred for use in this paper because it allows for national and international, civilian and military measures, both offensive and defensive, whether in peace, crisis or war. It applies to tactical, operational and strategic levels in all types of situations and operations. Although Information Operations has both offensive and defensive applications, the recommendations made in this paper will focus on defensive aspects only.

Canadian Responses

Canadians are becoming increasingly aware of the threat posed by attacks on computer-based information systems. Importantly, there are concerns about the impact of this threat on such vital national considerations as critical infrastructure, the economy, essential services and national security.

DND and the Canadian Forces have made significant progress in recent years in the field of Information Operations. The subject of Information Operations has been addressed in annual Defence Planning Guidance (DPG) since 1997. DPG 99 lists "the protection of information systems to ensure Year 2000 operational readiness" as DND's first Strategic Management Priority.[18] It also states that:

> The Deputy Chief of Defence Staff and the DND CIO have been tasked to jointly develop, seek DMC [Defence Management Committee] approval and implement policy and doctrine for Information Operations within DND and the CF in conjunction with OGDs [other government departments] and other Canadian agencies as well as our Allies. Priority is to be given to the development of a defensive IO [Information Operations] capability.[19]

The CF has established an Information Operations Steering Committee (IOSC) at National Defence Headquarters, chaired by the Chief of Staff J3 and including senior members

---

[17] Department of National Defence, "Information Operations in Canada" J6 Information Operations Briefing (Ottawa: 1998) 13
[18] National Defence Headquarters, Defence Planning Guidance 1999 (Ottawa:1998) article 202
[19] Defence Planning Guidance 1999 article 208

from the NDHQ Joint Staff and representatives from the Navy, Army and Air Force. An Information Operations Working Group reports to the IOSC.[20] To date, Canada has borrowed heavily from the US Department of Defence in the development of CF doctrine, which has now been published as B-GL-300-005/FP-000 Information Operations.[21] Work on refining both policy and doctrine continues.

Significantly, in May 1998, a new organisation called the Canadian Forces Information Operations Group (CFIOG) was stood up. The CFIOG is part of the Defence Information Services Organisation (DISO) which is responsible to the Vice-Chief of Defence Staff. The CFIOG includes a joint staff element, a Network Vulnerability Assessment Team (Red Team) and components that deal with Signals Intelligence, Information Security and Joint Electronic Warfare.[22]

The establishment of the CFIOG has enabled the CF to work more closely with NATO staffs and also bilaterally with Allies, to advance Canadian knowledge, security and capabilities. The CF has completed two Memoranda of Understanding, one with the US and one with the UK, to share information. Exchange officers are now in place with the US Joint Command and Control Warfare Centre and with the UK Air Warfare Centre. The CFIOG is establishing a Computer Emergency Response Team to detect and react to network intrusions. DND has begun to work with other government departments and agencies, but national policy direction is still lacking.[23]

Canada's Defence Research and Development Branch (CRAD) now has programmes specifically dedicated to supporting both offensive and defensive Information Operations objectives of DND and the CF and it also provides technological support to the Federal Government in the protection of national infrastructure.[24] The formation of the CF Information

[20] "Information Operations in Canada" 20-21
[21] Canadian Forces Publication, B-GL-300-005/FP-000 Information Operations
[22] "Information Operations in Canada" 21. The briefing includes a detailed explanation of the organisation.
[23] "Information Operations in Canada" 21-23
[24] The Canadian Defence Research and Development Branch (CRAD) discusses some of these programmes in "R&D Programmes - Command and Control Information Systems" (http://www.crad.dnd.ca/program/cgccis_e.html)

Operations Group will greatly assist DND and the CF in more clearly defining their requirements for CRAD's research.

In its 1997 Public Report, the Canadian Security and Intelligence Service (CSIS) acknowledged the threat posed to the security of Canada by foreign intelligence services, criminal organisations, terrorist groups and individual hackers, who either have, or can access, the capability to penetrate government and private sector computer-based systems. CSIS co-operates with other government departments to counter the threat from Information Operations and provides assessments on Canadian vulnerabilities and the capabilities of those who might exploit them.[25]

These developments demonstrate a notable commitment to Information Operations on the part of DND, the CF and CSIS. This by itself is not enough, however. Some other government departments and agencies and many enterprises in the private sector, understandably less focussed on issues of national security, have been slow to recognise the threat posed to information systems, on which they are no less dependent. Dealing with the threat on a national scale will require commitment, leadership and co-ordination from the highest levels. As noted above, DPG 99 directed DND and the CF to work with other government departments and agencies. However, until there is clearer national policy direction and improved co-ordination from the Privy Council Office, there is a limit to what the Department and the Forces can accomplish by themselves.

US Responses

By way of comparison and also in acknowledgement of our very close information network links, an examination of recent US Government initiatives would be useful. In 1996, in response to assessments concerning the potential threat posed by attacks to critical infrastructure, US President Clinton created the Presidential Commission on Critical Infrastructure Protection (PCCIP). In a major study, the PCCIP considered critical infrastructure to be grouped into five

[25] Canadian Security Intelligence Service, 1997 Public Report (Ottawa: 1998) http://www.csis.scrs.gc.ca/eng/pub1997e.html 6

sectors – Information and Communications, Banking and Finance, Energy, Physical Distribution and Vital Human Services.[26] The Commission's findings were published in 1997, and examined in the same year by a US Government Interagency Working Group, which reported to the President.

In May 1998, US policy on critical infrastructure protection was published in a White Paper known as Presidential Decision Directive 63. The paper explained the key elements of the policy and declared that "the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on … critical infrastructures, including … cyber systems."[27] The Decision Directive established national goals for the development of an operating capability to protect critical infrastructures from intentional acts. It also directed the development of a National Infrastructure Assurance Plan, issued tasks to departments and agencies, with milestones, in the development of the plan and outlined an organisational structure and assigned responsibilities. As threats to infrastructure would affect facilities in the economy as well as government, the President called for a partnership and co-ordinated efforts of both the public and private sectors. Although it is too early to assess the progress made since the recent Presidential Decision Directive was issued, at least it could be said that the US Administration has exhibited the type of national-level commitment and leadership which is needed to face up to this threat. Having stated the aims, enunciated the strategy and issued orders, the US Government is better positioned now to deal with the issues.

A comparable degree of engagement and direction from senior levels of government has, unfortunately, not been apparent in Canada. DND, the CF and CSIS are involved and progressing, but they cannot solve the problem for other government departments and agencies or the private sector.

---

[26] Willis Ware, The Cyber-Posture of the National Information Infrastructure Rand Report No. MR-976-OSTP (1997) http://info.rand.org/publications/MR/MR976/mr976.html 6-7

[27] US Presidential Directives and Executive Orders, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63" (Washington DC: 22 May 1998) http://www.fas.org/irp/offdocs/paper598.htm 1

The 1998 Ice Storm

Canada can not afford to wait for a catastrophe, but ironically, recent memories of the disastrous January 1998 Ice Storm experienced in Eastern Ontario and Western Quebec might serve to remind senior levels of government and officials of involved departments about our vulnerabilities. Although the electrical power outages were caused by physical damage from a unique and localised weather phenomenon, the interruption to essential services and the disruption experienced by the population, the private sector and government operations have been compared by some experts with the consequences of a concerted attack on critical information systems.[28]

The Year 2000 Millennium Bug

Another potential crisis looms on the horizon, one that we expect and largely understand – Year 2000 or "Y2K". The microchips embedded in many computer systems and data bases, as well as in systems which operate many items of technical equipment upon which our modern society depends, use only two digits (e.g., 98) vice four digits (e.g., 1998) to represent the date. On January 1, 2000, many of those systems operating information data bases, telecommunications, energy supply, transportation, traffic control, navigation, finance, commerce, government services, military and medical equipment, to name only some, will malfunction and cease to operate.[29] This will, or could, if the problems are not fixed, impact very significantly on the operation of critical infrastructure, public safety and continuity of services.

To varying degrees, public and private sector organisations have been working to deal with the Y2K problem, but there are a number of significant weaknesses in the *ad hoc* approach taken so far. General awareness of the nature of the problem and its potential strategic impact is

[28] James Adams, "Big Problem – Bad Solution: The Crisis in Critical Infrastructure and the Federal Solution", Speech given at Online News Summit '98 (Washington DC: 18 May 1998) http://206.132.10.154/idmarketsite/jadocs/Online.doc 2. Also discussed was the recent massive electrical power failure in Wellington, New Zealand.

[29] James Adams, "The Enemy Within: A New Paradigm for Managing Disaster," Speech given at Disaster Forum '98 Conference," (Alberta: 29 June 1998) http://www.ndu.edu/inss/books/uc/uchome.html 5

poor. Although individual government departments and many private sector enterprises have been working hard to ensure that their own equipment and systems are "Y2K compliant", not enough is being done to address the interdependencies of departments and organisations. There is a great need for better co-ordination within the federal government, between levels of government and with the private sector.

To date, there is no comprehensive list of critical information databases and systems, and components of critical infrastructure, including inter-dependencies. Such a list would need to transcend all levels of government (i.e., federal, provincial and municipal) and include both the public and private sectors.

This problem is not simply a technical "glitch" to be handled by computer experts. There exist important issues involving national security, public safety and economic prosperity, which have not yet been adequately addressed. In a political sense, what is at the very heart of the issue - the strategic "centre of gravity" - is the confidence of the Canadian public in their Government.

The Canadian Government has been slow in appreciating the potentially disastrous consequences of the Y2K problem and in becoming engaged at the national level in formulating plans and directing appropriate action. This hesitancy vividly illustrates the need for better awareness regarding the vulnerability of computer-based information systems, our dependence on them, the interdependence of government and private sector information systems and the extent to which dealing with these issues is fundamentally in the national interest.

As this paper is being written, the Government of Canada is forming a Y2K Interdepartmental Planning Group in Ottawa to work on the problem. DND has been appointed as the lead department in the Planning Group. Individual government departments and agencies continue to be responsible for ensuring that their systems are Y2K-compliant.[30] Although the Planning Group is just getting started in its work, it represents a significant step in providing much-needed co-ordination and awareness at the national level.

[30] Major-General Alain Forand, Canadian Forces member on the Y2K Interdepartmental Planning Group, personal interview, 16 Oct 1998.

But time runs short and stakes are high. Forming a planning group is not enough. The Government must act quickly to show determined leadership, to get all players "on side" and to dedicate needed resources and authority to the Planning Group. There needs to be a strong, clear and formal policy statement concerning the Government's commitment to ensuring continuity of critical infrastructure and services in the Year 2000, as a top priority domestic issue. For this to work effectively, the Government must establish a strategic partnership, which includes all federal government departments and agencies, provincial governments and the private sector.

The initial task of the Y2K Interdepartmental Planning Group, working closely with all involved departments and agencies, is to establish a base line survey of critical infrastructure. The Group will also develop possible Y2K-related scenarios involving failure of systems and services, examine departmental plans to deal with those scenarios and help identify areas needing further action or co-ordination.[31] On receipt of the recommendations of the Interdepartmental Planning Group, and in consultation with the private sector, the Government will need to formulate an effective over-arching strategy and plan of action for Year 2000.

Considerations for the Canadian Government

There is a danger that interest in addressing the overall vulnerability of our computer-based information systems and computer-dependent infrastructure will wane as the Y2K threat passes. As discussed earlier in the paper, serious and less predictable, insidious threats to our information systems will remain. Special efforts will need to be made at very senior levels of Government to maintain national-level leadership and continued commitment to deal with the continuing threat. The government and all departments and agencies should capitalise on their growing Y2K planning experience. The very same strategic partnership needed to prepare for Y2K will be needed to deal effectively with continuing cyber-threats to our information systems and critical infrastructure. Just as with Y2K, at stake are continuity of critical infrastructure and services, economic prosperity, national security, and in political terms, public confidence in Government.

[31] MGen Forand, personal interview, 16 Oct 1998

Although the challenge is great, solutions are achievable. The basis for the development of a national commitment in Canada to defensive Information Operations exists.

A Recommended Approach for the Government of Canada

The Government needs to lead an integrated national approach to deal with the security of computer-based information systems. This approach should be signalled with a forthright national policy statement, committing the Federal Government to the protection of computer-based information systems and the assurance of critical infrastructure and essential services for the Year 2000 and beyond. The statement should announce the intention to develop an over-arching National Information Systems Security Plan and a Critical Infrastructure Assurance Plan. It should assign clear responsibilities to departments and agencies for planning and co-ordination, giving milestones for completion. Protection of infrastructure and continuity of government services in the face of the Y2K challenge should be highlighted as a major step in this direction and the top domestic priority for the Government.

The Government of Canada should establish and sustain a strategic partnership, involving all departments and agencies, provincial governments and the private sector, which is committed to an integrated national approach to ensure information systems security. It should utilise the very real and immediate need to address the Y2K challenge as the basis to motivate and orchestrate such a partnership.

Although DND has been assigned responsibility as lead department on the Y2K Interdepartmental Planning Group, the Privy Council Office and all appropriate departments and agencies need to remain fully engaged. Ways need to be found to effectively involve provincial government departments and agencies and the private sector in development and implementation of plans.

As a priority, the Government needs to establish a comprehensive base line assessment of vulnerability of information-based systems and critical infrastructure dependencies. This is the

first main task of the Y2K Interdepartmental Planning Group, but once developed, the assessment needs to be maintained on an ongoing basis by an assigned lead department or agency, beyond year 2000.

The Privy Council Office is responsible for co-ordinating the activities of the Canadian security and intelligence community and for overseeing the operation of interdepartmental committees dealing with security and intelligence matters.[32] Information systems security is a subset of security. Accordingly, the Privy Council Office should establish an integrated process to monitor threats and share information concerning information systems security on an ongoing basis. The best approach would be to utilise the existing "Canadian Intelligence Community" with its well-functioning Security and Intelligence Committee Structure.[33] Many involved departments and agencies, especially DND and CSIS, already have the advantage of close links with Allies, most significantly the US and UK. The PCO-led Interdepartmental Committee on Security and Intelligence, with its subordinate Intelligence Policy Group and Intelligence Assessment Committee (IAC), is the most appropriate national focal point for the co-ordination of intelligence and security issues. This should apply also to information systems security. To support the IAC, the PCO should form a new "Interdepartmental Experts Group" to deal specifically with security of information systems. This Experts Group should capitalise on the developing expertise and committed resources of DND (especially the CF Information Operations Group) and CSIS.

DND and the CF possess well-trained, professional and energetic personnel, useful (albeit limited) resources, very good links and relations with Allies and reliable organising and planning abilities. They are developing appropriate technical knowledge, expertise and capabilities in the newly formed CF Information Operations Group. Once fully operative, the CF Network Vulnerability Assessment Team and the Computer Emergency Response Team could assist the Privy Council Office and other government departments and agencies in assessing their network vulnerabilities. If appropriate, they could help others to set up their own evaluation and response

[32] Canadian Forces Publication, Intelligence Analysts' Handbook para 211
[33] for a description of the Canadian Intelligence Community and the Security and Intelligence Committee structure, see the Intelligence Analysts' Handbook paras 201-215. Although the document is classified SECRET AUSCANUKUS EYES ONLY, only unclassified portions are used and referred to in this paper

systems and teams. The Defence Research and Development Branch could be of enormous technical value to a co-ordinated national effort. In the national interest, DND and the CF should be prepared to offer their expertise and experience to the Privy Council Office and to other government departments in the development of a national strategy and associated plans to improve information systems security. Initially, venues to utilise this expertise and experience should include the Y2K Interdepartmental Planning Group and the Canadian Security and Intelligence Committee Structure. Our close links with Allies, especially those of the intelligence community and of the CF Information Operations Group, should be both valued and utilised.

Building on the experience of dealing with Y2K, the Government of Canada should consider the establishment of a Critical Infrastructure Assurance Agency, which could operate under the control of a department such as Industry Canada.

Conclusion

Canada has entered the Information Age. While this new age promises enormous benefits, it also carries new and significant costs and risks. Our expensive and complex computer systems are vulnerable both to malicious attack and accidental failure. Almost all modern institutions, infrastructure and services are extremely dependent on networked computer-based information systems. This dependence, together with the interdependence of Government, the Armed Forces, the private sector and critical infrastructure, creates vulnerabilities that impact on some of the most important of national considerations – national security, public safety and economic prosperity. The resulting threat to our way of life is real, serious and pervasive. Dealing with the threat will be costly and complicated. But failure to deal with the threat will be more costly and potentially disastrous. In political terms, the confidence of the Canadian people in the ability of the government to protect their way of life is at the very heart of the issue, the "strategic centre of gravity".

Many government departments and agencies and private sector enterprises are making progress in preparing for and dealing with the new threats. But a more concerted national effort

is needed, and this must be co-ordinated from the centre. The looming Year 2000 Millennium Bug must be dealt with urgently. Although not the result of a malicious Information Warfare attack, the consequences of failure would be similar. Y2K is not only a challenge; in a sense it is also an opportunity – a chance to "kick-start" national efforts to address the overall threat to the security of information systems and critical infrastructure.

What is needed is an integrated national approach led by the Government of Canada. An effective national effort will depend on the assumption, at the highest level of government, of responsibility for dealing with the threat to the security of information systems. This responsibility should include the formulation of a national strategy, the establishment and sustainment of a comprehensive strategic partnership and the development of national plans to assure the security of information systems and critical infrastructure. The Privy Council Office, as the organisation responsible for co-ordinating intelligence and security issues at the national level, should co-ordinate inter-departmental efforts relating to security of information systems. The existing interdepartmental Intelligence and Security Committee Structure should be utilised. The formation of a Critical Infrastructure Assurance Agency should be considered.

The Department of National Defence and the Canadian Forces, with their many institutional strengths, including the capabilities of the newly formed CF Information Operations Group and a well-connected military intelligence organisation, are well suited to make valuable contributions to the overall government defensive effort. A pro-active and energetic role for DND and the CF would be in the best interest of both national security and military effectiveness.

Annotated List of Works Cited

Books

Schwartau, Winn. Information Warfare: Chaos on the Information Highway. New York: Thunder's Mouth Press, 1994. A significant work which has been often quoted in other research. Discusses computer security, computer crimes, information warfare and security of information networks.

Sun-Tzu. The Art of Warfare. Trans. Roger T. Ames. New York: Ballantyne Books, 1993. A widely read and much-quoted military classic which has become a seminal work on the philosophy of warfare.

Published Articles

Szafranski, Richard. "A Theory of Information Warfare: Preparing for 2020." Airpower Journal Spring 1995. A discussion of the theory of information warfare, in the broader context of warfare. Proposes ways to wage information warfare at the strategic and operational levels. Explains how attacks on information systems will be prosecuted against knowledge systems and belief systems, aimed at influencing leadership choices.

Internet Sources

Adams, James. "Big problem – Bad Solution: The Crisis in Critical Infrastructure and the Federal Solution." Speech given at Online News Summit '98. Washington, DC: 18 May 1998. (http://206.132.10.154/idmarketsite/jadocs/Online.doc) The CEO of UPI, Adams takes a critical look at the recent US Presidential Decision Directive on Critical Infrastructure Protection. Suggests that the US government policy to protect critical infrastructure is slanted excessively toward the Justice Department and the FBI and largely leaves out the private sector.

Adams, James. "The Enemy Within: A New Paradigm for Managing Disaster." Speech given at Disaster Forum '98 Conference Alberta: 29 June 1998. (http://www.ndu.edu/inss/books/uc/uchome.html) Discusses the potential for breakdown of infrastructure resulting from attacks on information systems, natural disasters and the Y2K problem. Reviews findings of Exercise Eligible Receiver, a simulated Information Warfare attack on government and critical infrastructure. Criticises US political leadership in dealing with the problem.

Alberts, D.S. Defensive Information Warfare. NDU Press Book. National Defence University: August 1996. (http://www.ndu.edu:80/ndu/inss/books/diw/index.html) An online book, which reviews the potential for, attacks on decision-makers, the information-based processes they rely on and the means of communicating their decisions.

Anderson, Kent E. "Intelligence-Based Threat Assessments for Information Networks and Infrastructures: A White Paper." Global Technology Research, Inc: 11 March 1998.

(http://www.aracnet.com/~kea/Papers/threat_white_paper.shtml) A paper which proposes an intelligence-based threat assessment model. Identifies potential threats to networks and information infrastructures which cross organisational and national boundaries and where responsibilities for protection are unclear.

Arquilla, John J. and Ronfeldt, David F. "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict." Rand Research Review: Fall,1995. (http://www.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html) A short but useful paper which discusses ways in which information-related conflicts will change the nature and organisation of warfare, crossing economic, political and social boundaries. Suggests that conflicts in the Information Age will not be limited to nations, but will include non-state groups. Discusses concepts such as "netwar" - information-related conflict at a grand scale between nations or societies, and "cyberwar" - the conduct of military operations according to information-related principles.

Brewin, Bob. and Harreld, Heather. "U.S. Sitting Duck, DOD Panel Predicts." Federal Computer Week: 11 November 1996 (http://www.fcw.com/pubs/fcw/1111/duck.htm) A short article which comments on the US Defence Science Board's 1996 report on information warfare defence. Discusses the role of the Defence Information Systems Agency and predicts conflicts with the private sector in monitoring threats to infrastructure.

Browning, Graeme. "Infowar." Government Executive Magazine-GovExec.Com: 21 April 1997. (http://www.govexec.com/dailyfed/0497/042297b1.htm) A discussion of several Information Warfare scenarios and capabilities, including the possibility of devastating attacks on military and public infrastructures.

Canadian Security Intelligence Service. 1997 Public Report. Ottawa: 1998. (http://www.csis-scrs.gc.ca/eng/pub1997e.html) An annual report that informs the Canadian public regarding the security environment and security programmes undertaken by CSIS. Includes a small section on Information Warfare as an aspect of counter-intelligence, including the role of CSIS in assessing the threat and Canadian vulnerabilities.

Canadian Defence Research and Development Branch. "R&D Programmes – Command and Control Information Systems." (http://www.crad.dnd.ca/program/cgccis_e.html) CRAD's Internet home page explains their roles, organisation and research programmes in support of the Department of National Defence and the Canadian Forces.

Devost, Matthew G. "National Security in the Information Age." Submitted in fulfilment of a Masters degree. University of Vermont: May 1995. (http://www.terrorism.com/documents/devostthesis.html) A well-written and in-depth look at Information Warfare and the vulnerability of key US infrastructures. Discusses attractions and deterrents to the use of Information Warfare and considers the political dimension.

Fast, William R. "Knowledge Strategies: Balancing Ends, Ways and Means in the Information Age." Sun Tzu Art of War in Information Warfare Compendium. Institute of National Strategic Studies. National Defence University: 1997. (http://www.ndu.edu/ndu/inss/siws/ch1.html) An

excellent and thought-provoking paper, which discusses how the Information Age profoundly affects how we think about and act on national strategic interests. Fast analyses an information-based society in terms of ends (national objectives), ways (actions) and means (methods). Examines key elements necessary to redefine US national interests and military defensive requirements.

Foran, Brian "Information Warfare: Attacks on Personal Information." Address to the 91st Annual Canadian Association of Chiefs of Police Conference. Ottawa: 26 August 1996. (http://www.magi.com/~privcan/pubs/cacp91.html) From a security and law-enforcement point of view, discusses issues of privacy, security and confidentiality as they relate to attacks on information systems. Relates several examples of significant computer-related losses suffered by North American companies. Concludes the threat means that separate constituencies, public and private sectors, dealing with privacy, security, law enforcement and technology must work together to find suitable compromises.

Fowler, Bruce W. and Peterson, Donald R. "Induced Fragility in Information Age Warfare." OR/MS Today Vol 24, No 2. April 1997. (http://lionhrtpub.com/orms/orms-4-97/warfare.html) Discusses new risks, vulnerabilities and increased potential for losses when information age technology, combined with standard military operations, crosses both civilian and military boundaries.

Fredericks, Brian. "Information Warfare: The Organisational Dimension." Sun Tzu Art of War in Information Warfare Compendium. Institute for National Strategic Studies. National Defence University: 1997. (http://www.edu/ndu/inss/siws/ch4.html) A thoughtful and comprehensive paper which addresses the role of organisations in the US as an essential element in developing and implementing a viable Information Warfare strategy. Discusses inter-agency challenges and makes recommendations regarding how to better organise the US Information Warfare effort as a decisive element of national security strategy.

Gertz, Bill. "Eligible Receiver." The Washington Times. 16 April 1998. (http://csel.cs.colorado.edu/~ife/114/EligibleReceiver.html) A newspaper article which reports on Exercise Eligible Receiver, a US Government Information Warfare exercise which simulated an orchestrated and large-scale attack on US military information systems and civil infrastructure.

Rand Organisation. "Information Warfare: A Two-Edged Sword." Rand Research Review Fall, 1995. (http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html) A short paper that presents the results of a series of simulated attacks on US information systems. Provides a short summary of the main lessons learned from the exercises.

Lewis, Brian C. "Information Warfare." A Proceeding from the U.S. Policy Conference, Intelligence Reform from Outside the Beltway. Princeton University: January 1997. (http://www.fas.org/irp/eprint/snyder/infowarfare.htm) Discusses the role of the US intelligence community, using both offensive and defensive information warfare, in advancing US foreign policy interests and protecting national security. Makes a number of recommendations to better prepare the US to defend against information warfare attacks.

U.S. Presidential Directives and Executive Orders. "The Clinton Administration's Policy on Critical Infrastructure Protection." Presidential Decision Directive 63: 22 May 1998. (http://www.fas.org/irp/offdocs/paper598.htm) Explains the key elements of the Clinton Administration's policy and direction on critical infrastructure protection.

U.S. Department of Transportation. "Emerging Issues in Transportation Information Infrastructure Security." Presented at the Emerging Issues in Transportation Infrastructure Security Conference: 21May 1996. (http://www.volpe.dot.gov/pubs/series1.html) A study of threats relating specifically to US transportation infrastructure and makes recommendations for protection, including national level standards and procedures for information security.

Rathmell, Andrew, et al. "The IW Threat from Sub-State Groups: An Interdisciplinary Approach." Paper presented at the Third International Symposium on Command and Control Research and Technology. Institute for National Strategic Studies. National Defence University: 17 June 1997. (http://www.kcl.ac.uk/orgs/icsa/terrori.htm) A paper which discusses the potential uses by terrorists of Information Warfare techniques, and recommends an interdisciplinary approach which combines computer science strategic, studies and political science to facilitate open-source threat assessments.

Robinson, Clarence A. "Western Infrastructures Face Rogue Data Stream Onslaught." Signal Magazine January, 1997. (http://www.us.net/signal/Archive/Jan97/Western-jan.html) A short but very useful article which describes the reorganisation of the US Defence Information Systems Agency to improve the protection of Department of Defence networks and to align Defence efforts with the protection of other information infrastructures.

Tenet, George J. "Current and Projected National Security Threats." Testimony before the U.S. Select Committee on Intelligence Hearing on Current and Projected Security Threats: 28 January 1998. (http://www.odci.gov/cia/public_affairs/speeches/dci_speech_012898.html) Outlines the growing dependence of the US on information systems, highlights technology issues as they affect other areas of national security and discusses terrorist threats.

Ware, W.H. The Cyber-Posture of the National Information Infrastructure. Rand Report No MR-976-OSTP: 1997. (http://info.rand.org/publications/MR/MR976/mr976.html) Discusses the vulnerability of US national information infrastructure to disruptions and external attack. Assesses ways to assess the threat and discusses steps that the government and the private sector could take to reduce national vulnerability.

Briefings

Alward, Colonel R. "Information Operations in Canada." J6 Information Operations Briefing. National Defence Headquarters, Ottawa: May 1998. An unclassified briefing which outlines the activities currently under way in the Canadian Forces to deal with Information Warfare. Discusses Canadian doctrine and outlines the development of the new CF Information Operations Group.

Personal Interviews

Forand, Major-General Alain. Canadian Forces member of the Y2K Interdepartmental Planning Group. Interviewed at Canadian Forces College Toronto: 16 Oct 1998.

Other Sources

Canadian Forces Publication. B-GL-300-005/FP-000 Information Operations. Draft version 0.1. Ottawa: 1998. Army doctrine published under the authority of the Chief of Defence Staff. Describes the Canadian Forces' concept of Information Operations as a combat function, outlines how IO relates to other combat functions and contributes to battlefi