LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

BACKGROUND PAPER

Cybersecurity and Intelligence: The U.S. Approach

Publication No. 2010-02-E
Revised 15 June 2011

Holly Porteous

International Affairs, Trade and Finance Division
Parliamentary Information and Research Service

Cybersecurity and Intelligence: The U.S. Approach
(Background Paper)

HTML and PDF versions of this publication are available on IntraParl (the parliamentary intranet) and on the Parliament of Canada website.

In the electronic versions, a number of the endnote entries contain hyperlinks to referenced resources.

Ce document est également publié en français.

Library of Parliament ***Background Papers*** present and analyze various aspects of current issues in an objective, impartial manner. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations.

Publication No. 2010-02-E
Ottawa, Canada, Library of Parliament (2011)

CONTENTS

CYBERSECURITY AND INTELLIGENCE: THE U.S. APPROACH

1 INTRODUCTION

Allegations made in January 2010 that China hacked into Google email accounts and the computer systems of at least 33 other U.S. companies highlight an ongoing and increasingly aggressive cyber espionage campaign being waged against U.S. interests and those of its allies.[1] Indeed, China's suspected cyber spying first gained public attention in 2003, when reports emerged that it was behind a massive, coordinated operation in which sensitive government and private-sector computer systems in the United States, the United Kingdom, Australia, New Zealand and Canada had been compromised. Designated "Titan Rain" in the United States, this espionage operation never really ended.[2] It simply morphed into an ongoing assault that leverages a vast shadow infrastructure of compromised systems to attack the United States, its Five Eyes[3] partners (Canada, the United Kingdom, Australia, and New Zealand) and other nations. China is but one of a growing number of states believed to be using the Internet to steal classified or proprietary information and, according to many analysts, to sow the seeds of future acts of sabotage in the event of a conflict.[4]

The United States characterizes cyber espionage and attack as first-order threats and has reformulated its national cybersecurity strategy. Three of its closest (Five Eyes) intelligence partners – Australia, New Zealand and the United Kingdom – have followed suit. Canada also began to draft a national cybersecurity strategy in 2004 but, as of writing, has not yet publicly articulated its position. Because the United States' experience has so deeply informed the strategies of all its allies, this paper will focus on its approach. For reasons that will be explored in this paper, signals intelligence (SIGINT) – the interception of electronic emissions of all types to gather information on a target – has come to play a central role.

2 FRAMING THE ISSUE

The potential for computer-based attacks to wreak havoc on a large scale has been known for some time.[5] Credit for the first automated attack is often given to Robert T. Morris, who unleashed the Morris worm on ARPAnet (the Internet's predecessor) in 1988.[6] Infecting an estimated 60,000 Unix-based computers, the Morris worm prompted the creation of the computer emergency response team at Carnegie Mellon University and netted its creator three years' probation, 400 hours of community service, and a fine of US$10,000. Another decade passed, however, before a concerted attempt to think through cybersecurity on a national level was made in the form of the Clinton administration's Commission on Critical Infrastructure Protection, chaired by retired U.S. Air Force general Robert Marsh. The 1997 Marsh Commission's recommendations on the cyber dimension of critical infrastructure protection formed the basis of Presidential Decision Directive 63 (PDD 63), which in turn framed the cybersecurity issue and the government's intended course of action. Remarkably, despite a series of policy updates by successive administrations – the

2000 National Plan for Information Systems Protection, the 2003 National Strategy to Secure Cyberspace, the 2007 Comprehensive National Cybersecurity Initiative, and the 2009 Cyberspace Policy Review – the fundamental themes established in PDD 63 endure. These themes are as follows:

1. The magnitude of the issue demands executive branch engagement and governance structures to support complex policy and operational coordination.
2. National defence, foreign affairs, intelligence and law enforcement are lead agencies.
3. The interconnectivity of public- and private-sector systems calls for a comprehensive, society-wide approach and public-private partnership.
4. Public- and private-sector understanding of cybersecurity must be addressed through education and awareness.
5. Private-sector operators know best how to secure their systems, and incentives should be favoured over regulation in working with them, but laws and regulation will be used where necessary.
6. Privacy rights must be respected and confidentiality of shared information maintained.
7. Given the global reach and borderless nature of the Internet, successful implementation of the policy requires international cooperation.
8. Multi-year, federally sponsored research and development is needed to address cyber vulnerabilities.
9. The federal government must first secure itself so as to lead the way in establishing best practices.[7]

3 STRATEGY IMPLEMENTATION: CHOOSING THE RIGHT TOOL

3.1 LAW ENFORCEMENT TAKES THE LEAD

If the problem statement has changed little since PDD 63 was released in 1998, the instruments used to address it have. Until the 2007 Comprehensive National Cybersecurity Initiative, law enforcement was the "tool of choice." For instance, PDD 63 looked to the fledgling National Infrastructure Protection Center (NIPC) to provide early warning and response. Established by the Department of Justice and the Federal Bureau of Investigation (FBI) in February 1998, NIPC's mission was to work with the private sector, state and local authorities, and other federal leads – including defence and intelligence agencies – to provide threat assessment, warning, vulnerability and law enforcement investigation, and response to cyber incidents affecting critical infrastructure. Though NIPC was staffed primarily by FBI agents, other federal departments and intelligence agencies as well as Canada, Australia and the United Kingdom also provided personnel.[8]

It is telling that the 2003 National Strategy sought to enhance law enforcement's capacity to prevent and prosecute cybercrime. By this time, it was becoming clear

that the NIPC model was not living up to its promise. For example, while praising the Center's investigative, training and awareness efforts, the General Accounting Office (GAO – now the Government Accountability Office) told Congress in 2000 that NIPC suffered from serious shortcomings in its analysis and warning capabilities.[9] As a result, NIPC was only able to issue warning information on the infamous "ILOVEYOU" virus hours after departments and private-sector organizations had began succumbing to the attack.[10] In this connection, the GAO also noted the private sector's reluctance to share incident information with NIPC due to concerns that the FBI was more interested in prosecution than protecting confidentiality. Though NIPC's "fusion centre" approach was intended to provide coordinated response, it was clear that just bringing representatives from different agencies together under one roof was not enough to overcome competing mandates, issues with information sharing, and unclear roles and responsibilities. The National Strategy attempted to finesse the problem by folding NIPC into the newly formed Department of Homeland Security but the underlying issues remained. Cybercrime and cyber warfare can be conducted by states, organized crime groups, corporations and individuals. Law enforcement is equipped to respond to some but not all of these threats.

3.2 INTELLIGENCE JOINS THE MIX

The 2007 Comprehensive National Cybersecurity Initiative (CNCI), issued after a review of the 2003 National Strategy, signalled the end of law enforcement's lead role.[11] Law enforcement would remain an essential player in cybersecurity but it would henceforth be one among many. As the former cybersecurity chief of the U.S. National Security Council, Melissa Hathaway, describes it, "Core to this strategy is the 'bridging' of historically separate cyber defensive missions with law enforcement, intelligence, counterintelligence, and military capabilities to address the full spectrum of cyber threats from remote network intrusions and insider operations to supply chain vulnerabilities."[12]

Simply put, CNCI aims to use the existing cyber defence "tool box" more effectively. Each of these "tools" – law enforcement, the military and intelligence agencies – has a role in protecting U.S. computer systems against cyber threats. The FBI provides the private sector with much-needed security advice. Its investigation and prosecution of cybercrime, including cases of cyber espionage, generates important counter-intelligence information and helps deter other would-be criminals. Military and intelligence agencies bring a different and more operational perspective to cyber defence. For example, under its new Cyber Command (CYBERCOM), the U.S. Department of Defense (DoD) is preparing to engage in full-spectrum computer network operations: from defence, to exploitation, to attack.[13] It is no accident that CYBERCOM will be led by General Keith Alexander, Director of the U.S. National Security Agency (NSA). As will be discussed in greater detail below, the NSA – an agency of DoD – brings considerable capabilities to the table.

While law enforcement, the military and intelligence each have a cyber defence mission, their respective authorities place differing constraints on the scope of their activities. For example, media reports have noted that the FBI's attempts to investigate the Titan Rain attacks was frustrated by China's refusal to cooperate and the U.S. government's reluctance to authorize the FBI to use computer network

exploitation (CNE)[14] to further its investigation. Other entities, such as the U.S. military, have less restrictive rules of engagement with respect to CNE against foreign entities. Here, the main concern is not getting caught in the act.[15]

In a domestic context, however, the U.S. military faces its own set of constraints. This is why DoD officials have stressed the division of labour between military and civilian cyber defence efforts, explaining that CYBERCOM will be responsible for securing the ".mil" Internet domain (the top-level domain used exclusively by the U.S. military), while the Department of Homeland Security will oversee the security of the ".gov" Internet domain (the top-level domain used exclusively by the U.S. government).[16] Nonetheless, Einstein – a network traffic monitoring system being developed to secure the.gov domain – exemplifies some of the complex legal and policy issues raised by mission "bridging." Einstein is operated by the Department of Homeland Security but dependent upon NSA-supplied attack signatures.[17] Einstein is currently proceeding beyond simply monitoring and reporting on potentially harmful Internet traffic coming to and from government departments to actively intercepting such traffic.[18] NSA-supplied attack signatures are essentially triggering the automated "search and seizure" of suspicious traffic, but they are doing so only under the ultimate authority of the Department of Homeland Security.

3.3 More Attention to Governance, Legislation and Policy

One of Barack Obama's first actions as president was to commission a 60-day review of U.S. cybersecurity policy. The resulting May 2009 Cyberspace Policy Review[19] validated CNCI's bridging of previously disparate defence, intelligence and law enforcement missions. But it also set out 10 near-term action items,[20] most of which relate to governance, legislation and policy. If one considers that the United States is moving towards a more operational footing in the face of aggressive cyber operations, this should not be surprising. Near-instantaneous decision-making, in the midst of a fast-moving, multi-jurisdictional attack, demands clear roles and responsibilities and a solid legal and policy framework.

While the broad themes of cybersecurity strategy have not changed much since PDD 63, the sense of urgency has. Cyber threats that seemed somewhat theoretical to many in 1998 have become tangible. Although no "Cyber Pearl Harbour" has materialized, the movement offshore of manufacturing centres for key information technology components over the past decade raises the unsettling possibility that critical systems may have the seeds for self-destruction hidden deep within their software. Real economic loss has occurred as a result of cyber espionage, and the speed, volume and coordinated nature of these intrusions has demonstrated the need for real-time situational awareness to respond effectively. For these reasons, one can discern in CNCI's preoccupation with girding the government against attack a desire to move to an operational footing akin to that needed for battle. The 2009 establishment of CYBERCOM suggests strongly that this is precisely the case.

4 WHY INTELLIGENCE IS TAKING ON A HIGHER PROFILE

As this paper has highlighted, a shift in thinking on the mechanisms of strategy implementation has occurred. Earlier approaches placed law enforcement front and centre. For example, while PDD 63 recognized that some cyber incidents would have a national security dimension requiring involvement of intelligence agencies, it nonetheless pegged the FBI, a law enforcement agency, to head up the national warning and information-sharing system. Moreover, while the United States (as well as Canada) actively pursued diplomatic solutions, it did so primarily in the context of formulating international technical security standards and criminalizing certain computer-based activities through the Council of Europe Convention on Cybercrime.[21]

Law enforcement remains an important instrument of national cybersecurity, but mainly in the context of raising public awareness and prosecuting domestically based cyber criminality or cyber criminality originating from countries willing to assist in the investigation. Despite the 2004 coming into force of the Convention on Cybercrime, prosecution in an international context remains a work in progress. High-profile busts of international child pornography rings are being offset by disappointing results such as the failure to bring to justice all those responsible for a massive flooding attack against Estonia's government and financial systems in 2007. If the angry exchange between China and the United States is any indication, the legal response to the attacks on Google and other U.S. firms is also unlikely to be entirely satisfactory.[22] The threat of prosecution – weak as it is in the face of uncertain attack-source attribution, differences in national legislation and uncooperative behaviours – is no deterrent to state-sponsored computer espionage. The risks are too low and the intelligence payoffs too high. Until reliable attribution can be addressed through identity management regimes, an issue which the Cyberspace Policy Review has identified as requiring near-term action, hackers using the protective havens offered by countries that have not signed the Convention on Cybercrime, such as China and Russia, can operate with relative impunity. Experts agree that, faced with this reality, the essentially reactive mechanism of law enforcement needs to be reinforced by stepped-up preventative measures, including early warning, and the development of a broader range of response options. This is why intelligence, in particular that provided by the NSA, has taken on a higher profile.

Although the public tends to associate the NSA with foreign intelligence collection alone – an association that has not helped assuage fears that its high-profile responsibilities in the new cybersecurity strategy are a threat to privacy rights[23] – the Agency has a long-standing mandate to help defend the United States' most sensitive information and computer networks. SIGINT agencies such as the NSA are well positioned to provide warning, particularly of sophisticated cyber intrusions carried out by states. This is because they are continuously engaged in the same activities themselves. CNE has become an indispensible foreign intelligence collection tool for many SIGINT agencies, including those of the Five Eyes.[24] To succeed at this game, SIGINT agencies expend a lot of time and energy probing and exploiting weak points in their targets' often well-hardened computer systems. This knowledge is also quite useful in spotting when an equally sophisticated entity is trying to return the favour. Detecting and then quietly observing the "tradecraft" of a

state-sponsored cyber intruder attempting to steal or alter data can provide valuable counter-intelligence on capabilities and intentions, all of which can be parlayed into indicators and warning about future targets.

This is not to suggest that the NSA's excellent vantage point on cyber threats is always a comfortable one. There is an obvious tension between its defence and exploitation activities. The same could be said of using exploitation expertise for the purposes of attack. Too much sharing of what the NSA knows about exploitable computer vulnerabilities might just end up closing down valuable foreign intelligence accesses. With so many competing interests at stake among lead agencies, it is understandable why governance has remained a problem to be solved through successive administrations.

5 CONCLUSION

The United States has led the way in identifying cybersecurity as a national security issue and crafting strategies to address the range of associated threats. As the United States increasingly turns to military and intelligence agencies to provide early warning and alternative response options, it stands to reason that its closest allies would do the same. For example, three of the NSA's Five Eyes SIGINT partner agencies – the Government Communications Headquarters in the United Kingdom, the Defence Signals Directorate in Australia and the Government Communications Security Bureau in New Zealand – each hold similar responsibilities in their government's respective cybersecurity strategies.[25] As previously noted, Canada has not yet articulated its strategy but there are reports indicating its imminent release.[26]

While there can be no question as to the capabilities that SIGINT agencies such as the NSA bring to the table, significant issues remain as to how these capabilities can be leveraged to assist cybersecurity beyond the federal level. As China obliquely noted in its riposte to Secretary of State Clinton's public statements on the Google attack, there is also an undeniable (but not insurmountable) contradiction between efforts to engage the international community on cybercrime while pursuing many of these same sorts of activities at the state level.[27] Finally, U.S. efforts to integrate computer network operations, including computer network attack, into its military planning have implications for its private sector and for its allies that need to be explored.[28]

Canada's interests in U.S. cybersecurity strategy are multifold and cross-jurisdictional. Beyond the two countries' close military, intelligence and law enforcement partnerships, Canada and the United States share many critical infrastructures. Sovereignty issues raised by the U.S. government's plans to regulate more aspects of the private sector's cybersecurity-related practices and activities are also worthy of exploration but beyond the scope of this paper.[29]

NOTES

1. For details on the attack and who was targeted, see Ariana Eunjung Cha and Ellen Nakashima, "Google China cyberattack part of vast espionage campaign, experts say," *Washington Post*, 14 January 2010; and Dan Goodwin, "IE zero-day used in Chinese cyber assault on 34 firms," *The Register*, 14 January 2010.

2. *TIME* magazine was among the first to describe Titan Rain in detail. See Nathan Thornburgh, "The Invasion of the Chinese Cyberspies ," *TIME*, 29 August 2005. For more recent reporting on suspected Chinese cyber espionage, see Brian Grow, Keith Epstein and Chi-chu Tschang, "The New E-spionage Threat," *BusinessWeek*, 10 April 2008; and John Markoff, "Vast Spy System Loots Computers in 103 Countries," *New York Times*, 28 March 2009. Markoff's article was based on research conducted by the University of Toronto-based "Citizen Lab" and Ottawa-based SecDev, which can be found in Ron Deibert and Rafal Rohozinski, "Tracking GhostNet: Investigating a Cyber Espionage Network," 29 March 2009. For a complete history of Chinese cyber operations, see Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," US-China Economic and Security Review Commission, 9 October 2009.

3. The term "Five Eyes" is a reference to the sets of "eyes" permitted to see the intelligence. For example, if a document is classified as "Canadian Eyes Only," this means it cannot be shared with non-Canadians. The Five Eyes intelligence alliance arose from the classified 1948 U.K.–U.S.A. agreement. See Matthew Aid, *The Secret Sentry: The Untold History of the National Security Agency*, Bloomsbury Press, New York, 2009, and Christopher Andrew, "The Making of the Anglo-American SIGINT Alliance," in *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer*, ed. Hayden Peake and Samuel Halpern, NIBC Press, Washington, D.C., 1994, pp. 95–109.

4. In its most recent annual threat assessment presented to the Senate Armed Services Committee, the U.S. Defense Intelligence Agency judged Russia as presenting the "most capable cyber-threat to the U.S." See Lieutenant General Michael D. Maples, U.S. Army Director, Defense Intelligence Agency, "Annual Threat Assessment," statement made before the U.S. Senate Armed Services Committee, 10 March 2009, p. 37.

5. However, the potential for cyber attack in and of itself to bring a nation to its knees is contentious. Long-time observers such as Martin Libicki point out that, because they are based on vulnerabilities created by coding errors, cyber weapons are exquisitely susceptible to countermeasures. Once a vulnerability has been exposed, either through normal IT security vigilance or through its use in a cyber attack, every effort will be made to eliminate it. Martin Libicki, *Cyberdeterrence and Cyberwar*, RAND Project Air Force, RAND Corporation, 2009.

6. The first malicious computer program was the 1982 "Elk Cloner" virus, which was written by ninth grader, Richard Skrenta, targeted Apple II computers and was propagated via infected floppy disks. For further reading on malicious computer programs, see Nicholas Weaver, "A Brief History of the Worm," *Security Focus*, 26 November 2001, and Eugene Spafford, *The Internet Worm Program: An Analysis*, Purdue Technical Report CSD-TR-823, Department of Computer Sciences, Purdue University, 8 December 1988.

7. See "White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," 22 May 1998.

8. See "The GAO Review of the NIPC," testimony of Ronald L Dick, Director, National Infrastructure Protection Center, FBI, before the U.S. Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology and Government Information, 22 May 2001.

9. See General Accounting Office, "Critical Infrastructure Protection: 'ILOVEYOU' Computer Virus Highlights Need for Improved Alert and Coordination Capabilities," testimony before the U.S. Senate Committee on Banking, Housing and Urban Affairs, Subcommittee on Financial Institutions, 18 May 2000.

10. Testifying before a U.S. Senate subcommittee, NIPC director Ronald Dick attributed this analytical shortfall to a reluctance by the Department of Defense and the National Security Agency to second personnel to the Center. See Dick, "The GAO Review of the NIPC" (2001).

11. CNCI was issued in 2007 but officially established only in January 2008, when President Bush signed National Security Presidential Directive 54/Homeland Security Presidential Directive 23. An unclassified version of CNCI was released on 2 March 2010. See The White House, *National Security Council*, "The Comprehensive National Cybersecurity Initiative."

12. See Government of the United States of America, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 29 May 2009, p. 4.

13. See *Quadrennial Defense Review Report*, United States Department of Defense, 1 February 2010, p. 38. There are also reports of instances where the US military has already been authorized to conduct computer network attack. See Shane Harris, "The Cyberwar Plan: It's not just a defensive game; cyber-security includes attack plans too, and the U.S. has already used some of them successfully," *National Journal*, 14 November 2009.

14. "Computer network exploitation" refers to breaking into computer systems and networks to extract but not alter data. "Computer network attack," on the other hand, seeks to "intentionally disrupt, deny, degrade, or destroy adversary computers, computer networks, and/or the information resident on them." See Mélanie Bernier and Joanne Truerniet, *CF Cyber Operations in the Future Cyber Environment Concept*, Department of National Defence, Defence Research and Development Canada, Centre for Operational Research and Analysis, DRDC CORA TM 2009–058, December 2009, p. 7.

15. Thornburgh (2005).

16. "Remarks at the Defense Information Technology Acquisition Summit," Deputy Secretary of Defense William J. Lynn, III, Grand Hyatt, Washington, D.C., 12 November 2009.

17. An attack signature is an action, or a series of actions, indicating an attempt to exploit a vulnerability.

18. Ellen Nakashima, "Cybersecurity Plan to Involve NSA, Telecoms," *Washington Post*, 3 July 2009.

19. Government of the United States of America, *Cyberspace Policy Review* (2009).

20. To demonstrate "leadership from the top" and move these and other medium-term action items along, Obama appointed former eBay and Microsoft executive Howard Schmidt as his cybersecurity coordinator on 22 December 2009. Schmidt will report regularly to the President and work as a key member of his National Security Council. "Introducing the New Cybersecurity Coordinator," *The White House Blog*, 22 December 2009.

21. See Council of Europe, *Convention on Cybercrime*. The Convention came into force on 1 August 2004. The United States deposited its instrument of ratification for this treaty on 29 September 2006, while Canada remains only a signatory. See Council of Europe, *Convention on Cybercrime*, "What do you want to know about this treaty?" for the list of signatures and ratifications.

22. In this connection, it is noteworthy that Google has reportedly asked the NSA for assistance in defending itself against future attacks. Media reports indicate that the collaborative effort will not attempt to determine who was behind the attack because such attribution is "nearly impossible." Ellen Nakashima, "Google to enlist NSA to help it ward off cyberattacks," *Washington Post*, 4 February 2010.

23. For example, President Obama has come under fire for allowing the NSA to continue its involvement in the Einstein intrusion detection and prevention system. See Jesselyn Radack, "NSA's cyber overkill," *Los Angeles Times*, 14 July 2009. The U.S. Office of the General Legal Counsel has concluded that Einstein does "not … [run] afoul of state wiretapping or communication privacy laws." See Memorandum Opinion for an Associate Deputy Attorney General, "Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch," United States Department of Justice, 14 August 2009.

24. Each of the Five Eyes partner countries has publicly alluded to its use of computer network exploitation to collect foreign intelligence. For example, speaking before the Canadian Standing Senate Committee on National Security and Defence in 2007, John Adams, Chief of the Communications Security Establishment Canada (CSEC), said his organization shared his U.S. counterpart's goal to "master the Internet" and drew the committee's attention to the growing number of Africa- and Middle East-based Internet users. Describing why CSEC's foreign intelligence collection mandate was updated in 2001 to enable collection of foreign communications where one end begins or ends in Canada, Adams noted that "The problem with today's communication is that it is not fixed. With the Internet, we do not know at any given time who is talking to whom. We target foreigners, but we do not know necessarily that they will be talking to foreigners. When the Internet became the mode of choice for communications, we were effectively muted because we could not target a foreigner because we did not know whether that target might speak to a Canadian. We were euchred." Standing Senate Committee on National Security and Defence, *Evidence*, 1st Session, 39th Parliament, 30 April 2007.

25. For the governments' cybersecurity strategies, see United Kingdom, Cabinet Office, *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, June 2009; Australian Government, *Cyber Security*; and New Zealand, Ministry of Economic Development, *Digital Strategy 2.0*.

26. Karen Fournier, "Feds working on a broad national digital strategy; could be released in budget, experts say," *The Wire Report*, 25 January 2010.

27. Michael Wines, "China Issues Sharp Rebuke to U.S. Calls for an Investigation on Google Attacks," *New York Times*, 25 January 2010.

28. Though the United States established a Cyber Command in June 2009 and is currently reviewing existing strategy and policy "to develop a comprehensive approach" to cyber operations, computer network attack remains a contentious activity for some of its allies. See Jason Sherman, "Defense Department Launches Cyber Strategy and Policy Review," *Inside the Pentagon*, Vol. 26, No. 1, 7 January 2010. Though he was writing in 2001, Andrew Rathmell provides an insightful analysis of U.S. and European thinking on computer network operations. See Andrew Rathmell, "Controlling Computer Network Operations," *Information & Security*, Vol. 7, 2001. For a more recent review of the ongoing doctrinal discussion in the Canadian Forces, see Bernier and Truerniet (2009).

29. See, for example, Ian Macleod, "U.S. plans to secure power grid worry producers," *Ottawa Citizen*, 22 November 2009.