“Don’t Call Us”

Governments, Cyber Security, and Implications for the Private Sector

Tom Quiggin

Centre for
International and
Defence Policy

Occasional Papers 66

"Don't Call Us"

Governments, Cyber Security, and Implications for the Private Sector

Tom Quiggin

66
April 2012
Occasional Paper Series
Centre for International and Defence Policy
Queen's University

Library and Archives Canada Cataloguing in Publication

Quiggin, Thomas
"Don't call us" : governments, cyber security, and implications for the private sector / Tom Quiggin.

(Occasional paper, 1205-7525 ; 66)
Includes bibliographical references.
ISBN 978-1-55339-356-6

1. Cyberspace—Security measures—Government policy. 2. Computer security—Government policy. 3. Computer networks—Security measures—Government policy. 4. National security. 5. Cyberterrorism—Prevention. 6. Financial institutions—Computer networks—Security measures. 7. Business enterprises—Computer networks—Security measures. I. Queen's University (Kingston, Ont.). Centre for International and Defence Policy II. Title. III. Title: Do not call us. IV. Series: Occasional paper series (Queen's University (Kingston, Ont.). Centre for International and Defence Policy) ; 66

QA76.9.A25Q84 2012 005.8 C2012-902422-8

Table of Contents

Foreword v

The Problems 2

The Critical Issues 3

The Outlook 10

Conclusions 11

Notes 12

Glossary 17

Select Bibliography 19

About the Author 21

Foreword

In the last decade, the rapid and global expansion of digital networks has caused an expansion of the national security agenda in every western developed democracy. The increasing dependence on the internet has created an increasingly vulnerability of these crucial systems to attack. Computer systems that we use without much second thought can be readily and sometimes very easily compromised, and this exposure to exploitation thus poses a significant risk to all those who use these systems—governments, firms, and society at large. Moreover, in a sector where technological change is constant and fast-moving, and where national regulation is challenged by the essentially borderless nature of the internet, governments have been hard-pressed to be at the forefront of this aspect of national defence by putting in place systems of mutual defence against cyber exploitation across all sectors of the economy.

To be sure, governments have laid out their cyber security strategies with the intention of strengthening the capacity of both government and the private sector to deal with cyber exploitation. Certainly the United States, Britain, Australia and Canada have all produced cyber strategies that feature certain common elements. But global agreement on regulating this new digital world has been elusive.

In this Occasional Paper, Tom Quiggin explores the consequences for the private sector—and the financial sector in particular—of these difficulties. An expert in the intelligence field, Quiggin argues that for a number of structural reasons, including the longer-term effects of austerity measures being embraced across the globe, governments have been unable to develop effective cybersecurity systems for all crucial sectors of the economy. While governments continue to work to establish effective cyber defence mechanisms across all sectors of the economy, Quiggin is not optimistic that there will be any quick fix for this threat. For this reason, he suggests that in the short to medium term, the private sector will have to depend on its own resources to mount an effective defence against cyber attacks.

* * *

Occasional Papers published by the Centre for International and Defence Policy at Queen's University are intended to provide both the policy community and the broader public with short analyses of contemporary issues in international and defence policy.

Kim Richard Nossal
Director
Centre for International and Defence Policy
Queen's University
April 2012

“Don’t Call Us”: Governments, Cyber Security, and Implications for the Private Sector

Institutions that depend on computer systems must at present assume they have to depend on their own resources for defence against cyber attacks. As Jason Healey, the former White House Director of Cyber Infrastructure Protection, has admitted, if the United States is engaged in a cyberwar, Americans would be far better served by contacting Microsoft or AT&T rather than the Department of Homeland Security.[1] This high-risk problem is unlikely to be mitigated by government agencies in the short to medium term. A variety of systemic cyber protection weaknesses and increasingly aggressive attackers suggests that the intensity of cyber attacks will continue to increase over the short to medium term. Most Western governments—Sweden and Finland appear to be exceptions[2]—are incapable of deterring or preventing trans-border cyber attacks and do not have the means to effectively retaliate or escalate after an attack or exploitation. Thus without a significant deterrent ability, it is likely that cross-border cyber attacks and exploitation will continue unabated.[3]

The developed world is currently experiencing a period of complexity and uncertainty and is operating without an overarching political framework or ideology.[4] Economic competition for access to scarce resources and markets is producing cooperation at one level (trade) with vicious competition at another (cyber exploitation and attacks). These can occur simultaneously between any number of states. There is a “wild west” element in this competition and conflict, and no sheriff has emerged to enforce any set of rules.[5]

Large financial institutions and national central banks are located at the leading edge of this conflict, with little guidance from national governments on how to act or defend themselves in this environment. As a result, these institutions are left in a defensive mode against aggressive state actors, amorphous transnational hacking groups, organized crime groups and individuals.

Because of information technology (IT) “monolithic ubiquity”—in other words, the commonality of systems across large organizations—large institutions with significant IT infrastructure and security systems are equally, or in many cases even more, vulnerable to intrusion than many small-to-medium IT infrastructures. On the contrary: the large number of IT-oriented security institutions that have been seriously compromised in the last two years[6] suggests that the perception that larger institutions are inherently better protected against IT threats is largely mythical.

Peer-to-peer (P2P) sharing on threat information and protective measures is and will remain a high-value capability when combined with forward-leaning internal monitoring practices supported by open source intelligence collection. The outsourcing of IT capabilities, especially security monitoring, is a high risk option that should be avoided.

The Problems

Cyber attacks and cyber exploitation will continue to constitute a major risk. Governments, typically responsible for protecting public and private assets on the territory of the state from external aggression and from domestic/international criminal activity, are not capable of providing the required protection.

Among the critical areas of weakness related to government policy and/or law and regulations are the following:

- The lack of theory or practical activity in the role of deterrence, retaliation and/or escalation concerning cyber attacks or exploitation originating from foreign states.
- The relatively low priority that most governments attach to cyber defence issues, despite a number of public statements to the contrary.
- The limited knowledge and expertise on the emerging and little-understood role of insider threat and how to counteract it.
- The relatively low investment that software producers devote to improving the security of their product. Unlike providers of other mainstream products or services, software companies are rarely held financially liable for defects in their products.
- The slow response of the United States government to this problem. In most other areas of international competition or conflict, the United States is normally a leading international force. But in the area of

defence against cyber attacks and cyber exploitation, Washington has been slow to move. The first significant responses were in 2009/2010, and those responses tended to focus primarily on military related systems.

- The significant gap that exists between the reality of cyber problems and the ability of most Western governments to adapt to the constantly changing requirements needed to address the issues.
- The limited range of international law enforcement and intelligence-sharing capabilities. While intelligence sharing between states may be increasing, the short to medium term will be dominated by peer-to-peer sharing.
- The outsourcing of a variety of IT capabilities. This outsourcing remains one of the key areas for creating vulnerabilities and exposing systems to attacks and exploitation.
- The monolithic ubiquity of IT equipment and software common among large IT based organizations.
- The mistaken but nonetheless persistent belief (especially in government) that a technological solution exists to the problem of cyber security.

The Critical Issues

There are a number of critical issues that Western countries—governments and the private sector—need to address in the near term.

Deterrence Theory

In general terms, Western governments have not yet come to terms with the concepts of deterrence, escalation and retaliation when malicious cyber activity originates in a foreign state.[7] Until this occurs, transnational cyber exploitation and cyber attacks will continue to increase. Part of the reason for this is that no international norms exist for cyber behaviour, and thus the "rules of the road" are only now being addressed. Formal discussions between the major states concerned—the United States, the Russian Federation and the People's Republic of China—have only been proposed; no meetings have been scheduled.[8] It is thus unlikely that we will see any initial results before 2015.[9]

In the meanwhile, however, cyber vulnerabilities are growing, and cyber attack tools and methodologies are becoming more available. The technical capacity of malicious actors is improving.[10] As a result, various states and large transnational groups can carry out attacks with relative impunity given the lack of international understanding about what constitutes a proper series of responses.

During the Cold War, deterrence was well-developed and normalized. A “ladder of escalation” ranged from conventional responses to biological, chemical, and finally nuclear responses. A series of thresholds were understood by both of the superpowers as well as most other state and non-state actors. [11] These “rules” were initially understood to work within the three main domains of conflict: land, sea and air. In this context, a shared framework existed for understanding how any given confrontation or conflict might develop. These rules were, however, never clearly extended into outer space as it emerged as the fourth domain of conflict.

Likewise, the emergence of cyberspace as the fifth domain of conflict has not been accompanied by a generally accepted framework of analysis which would produce an internationally shared framework for deterrence and escalation.[12] Moreover, there is no internal consensus on such issues within most governments—including the United States—and nor is one likely to emerge in the immediate future. No ability exists to do axiological targeting in cyber space. Or, as put another way: “As [cyber] offenses improve, thresholds for war in space and especially cyberspace—though not nuclear war—could become perilously low, absent deterrence.”[13]

On top of the inherent complexities and uncertainties involved in the cyber domain, a shared international framework of cyber deterrence would have to bridge cultural divides, force and network structures, national strategies and objectives, national and commercial level decision-making processes as well as concepts of proportionality. While this is not an impossible task, it is complex and the target date recently spoken of in a UK government paper does seem unduly optimistic.

Cyber Issues as a Priority

While many government officials claim that cyber security issues are a top priority,[14] the actual amount of effort, money and coordination going into actual solutions is uneven at best. For instance, the US Department of Homeland Security 2011 report on its Quadrennial Review lists cyber issues as fourth in a list of five priorities (behind terrorism, border security and immigration issues and ahead of ensuing resilience in disasters). The comparable document from Public Safety Canada in 2011 states that cyber issues are a "cornerstone" of national security, but offers little in actual priority setting or a comparison to other threats.[15] The Australian government *appears* to have a stronger interest and has described cyber security as a "top tier national security priority" while identifying the social and economic well being of the state as being "critically dependent" on the integrity of computer systems.[16] The United Kingdom also published a cyber strategy in 2011 and it puts cyber issues as a "Tier One" priority. It clearly identifies problems and potential solutions. However, even this UK report, the strongest of the four, notes that 2015 is a target date for selected solutions and improvements.[17]

The common theme of the Canadian and American documents appears to be well-meaning policy suggestions. Given that DHS in the USA and Public Safety in Canada lack the executive and budgetary control over the relevant intelligence and law enforcement agencies, no capabilities exist to bring the policies into reality. The reports are also making "2011 suggestions" but contain considerable baseline information from 2007 and 2008. By IT standards, this baseline information is questionable due to timeliness issues.

Behind the scenes, however, are two other systemic problems. The first is money. Governments frequently do not pay their staff sufficient money to ensure they are not being poached by private industry. In addition to the issue of compensation, there is the larger and perhaps more important issue of organization. By their nature, many IT workers tend to think in lateral and often non-linear terms. They function best when working in environments where self-emerging structures and solutions are the norm for any given problem set. Rapid adaption is desired and required, often on a daily or weekly basis. By contrast, governments, and other large bureaucracies, tend to be vertically oriented hierarchical structures which do not think in lateral or non-linear terms. Change occurs slowly and with great resistance as bureaucratic norms frequently tend to outweigh operational requirements, even at the cost of failure.

Insider Threat

The insider threat is emerging in both the physical and cyber security worlds. While firm statistics are difficult to come by,[18] the most pessimistic sources suggest that the majority of all cyber attacks have some form of insider activity.[19] This problem is being increasingly compounded by the de-legitimization of the state and its institutions. This enhanced threat is being compounded by the current economic downturn, government sponsored austerity measures and the co-incident inability of the state to deal with emerging structural problems.[20] Democratic states are also experiencing a particularly difficult set of circumstances. Mature Western democracies have developed increasing complex societies as a result of democratic processes. However, the ability of the state to deal with these complexities and the attendant problems has weakened at the same time.[21] As a result, insider threats are increasing and securing against these sorts of problems will be difficult.

Software Makers

With a few notable recent exceptions,[22] it has proven difficult to sue software manufacturers for security or performance defects in their products. Without this ability, software manufactures tend to treat security issues as an afterthought and only react with various patches and upgrades in after-the-fact activities. They also own security companies which then sell "solutions" to their own problems. Legislation to change this situation does not appear to be imminent in Europe, North America or South Asia.

The quality of the software is equally important to security as the defensive measures put around networks. High quality software (such as the quality levels applied to aircraft operating systems) has greater immunity to attacks based on its initial quality.[23] By contrast, lower quality software standards are generally applied, even in the financial industry, so failures and vulnerability to attacks will remain. Major software manufacturers generally only seriously consider security as an afterthought and then apply a "patch" mentality to the issue. Given the state of the industry and the complexity of the problem, it is unlikely that any major Western government will amend legislation in the short to medium future that will encourage software manufacturers to improve the quality of their product by exposing them to greater legal liability.

American Leadership

Despite pressure from both the private sector and its international allies, the United States government undertook limited action on responding to cyber threats from 1998, when the first emergence of serious sustained attacks occurred, to 2008. There appears to have been an increase in interest and activity from 2008 onwards, but even this is uneven and the first efforts were focused on military systems. President Barack Obama declared that digital infrastructure was a "strategic national asset," in 2009, and in June 2009 the US Secretary of Defense, Robert M. Gates, ordered the creation of Cyber Command (USCYBERCOM) within US Strategic Command. The first US Army Cyber Brigade was stood up on 1 December 2011.[24] However, this innovative command should not lead to the assumption that the US government is a leader in the cyber defence field. US cyber defences for non-military systems are no better than that of any other Western country, and arguably worse than countries such as Sweden, Finland and Israel.[25] A recent series of major foreign attacks against US government systems and corporations has demonstrated these weaknesses. As of early 2012, the American government has not even entered into formal talks with other states on issues concerning cyber security and the potential for cyber war. Talks in this area are at the proposal stage.[26]

Some American officials have recognized this weakness. Jason Healey's admission that Americans should not call the Department of Homeland Security in the event of a cyberwar has already been quoted. Healey, who is now the director of the cyber statecraft initiative at the Atlantic Council, went on to say that "If we do ever have a cyberwar, it will be won or lost in the private sector." He also admitted that he had little faith in the National Cybersecurity and Communications Integration Center, which is intended to be the lead agency for dealing with large-scale cyber-attacks.[27]

While no major example of cyber war exists,[28] it is increasingly clear that any such "war" would be won or lost in the private sector, as most governments have no ability to defend their own systems let alone the private sector. Western governments (and others) are not yet in the defensive fight. Indeed, at present it is not even clear who would have responsibility in the United States in the event of a major cyber incident. Legislation making its way through the US House of Representatives—HR 3674[29]— would give the Secretary of Homeland Security a leading role in cyber security, even though the National Security Agency has greater skills and personnel in this area. The working theory appears to be that a civilian-led agency should have control over a problem that will have an effect on mostly privately owned networks.[30] How this works in practice has not been made clear and the legislation has not yet passed; moreover, competing legislation may eventually award the lead to the NSA.

Gaps between Reality and Government Knowledge and Efforts

Government-based analysis tends to lag behind, rather than lead, knowledge creation efforts concerning cyber attacks. For instance, policy prescriptions contained in a series of government reports published in 2011 were based on 2007 and 2008 statistics.[31] Given that problems in the cyber world tend to evolve in periods of weeks and months, a government response based in an assessment cycle of years is not likely to be effective.

International Law Enforcement and Intelligence Sharing

Despite public comments to the contrary, the amount of domestic and international sharing and cooperation in IT security and criminal investigations is not encouraging. One particular area of concern is the sharing between national government agencies and the private sector. As the former White House Director of Cyber Infrastructure Protection stated in January 2012, "Government only inhales, it never exhales. It will take all the information, but it will find any excuse not to share."[32]

Internationally, the situation is not encouraging either. Jurisdictional disputes, complex legal requirements and a general lack of will on the part of some major governments have greatly restricted international investigations. As with deterrence and other issues, there are no immediate fixes in sight and no reason to be optimistic that this problem will be fixed in the near future.[33]

Outsourcing

Who writes your code that is in your security software and what do you know about it? "Not much" is the likeliest answer today. Many companies, including software security companies, are outsourcing their code-writing to sub- and to sub-sub contractors.[34] Frequently, this code-writing work is being done in the People's Republic of China, India, South Korea and even Libya. For the end user, there is no means of identifying the source of the code, and no way of knowing whether vulnerabilities have been built into the code at its point of origin. There is no legislation pending by major governments that may force software writers to disclose who wrote their software and where it was created.

Monolithic Ubiquity and the IT Vulnerability of Large Information Based Institutions

Despite their seeming outward differences, most large institutions with substantial IT infrastructures have many commonalities in servers, routers, software, power supplies and backup systems. They use many of the same types of software (such as Microsoft or Adobe) and the same kinds of security methods (appliances etc.). Consequently, once would-be attackers can determine vulnerability in one large institution, they can adapt that knowledge to be equally successful in attacking another. Additionally, large organizations tend to develop a sense of security based purely on their size and influence. Unfortunately, there is no correlation in the cyber world between the size of an IT infrastructure and its security. On the contrary: a small to medium size organization may present a more difficult target due to its lack of complexity, its small size and the likelihood that updates and patches will be applied automatically, unlike larger institutions.

In this case, a contrast exists between the physical world and the cyber world in security terms. There is a significant security difference between the cyber world and the physical world. In the physical world, a large bank or cash centre is less vulnerable to robberies than a corner convenience store because of its resources. In a convenience store, a determined robber will be able to defeat locked doors, basic alarms and a small safe. Those same skills would not allow a determined robber to attack a cash centre or major bank. In the cyber world, however, the size of an organization and its complexity do not make it less vulnerable—in fact the opposite appears to be occurring.

Complexity

Large complex systems increase the probability of flaws. Complexity and interdependency are known to be their own forms of weakness in computer systems, power grids and many other complex systems as well.[35] The constant addition of more technology has exacerbated the problem by adding complexity, more implicit assumptions and more vulnerability. The result is problematic, with new examples emerging such as the increased use of VOIP (voice over internet protocol) communications systems, virtualization on servers and the channelling of more information systems over the world wide web. The resulting complexity is—by itself—an emerging concern for IT systems vulnerability. Some governments are introducing the concept of having one government department responsible for all IT services and one portal for all Internet traffic. This may cause an increased level of complexity and interdependency which will render government more, rather than less, vulnerable to catastrophic failures.

Technological Solutions Sought by States and Corporations

There is a near total consensus of opinion among hackers (both "black hats" and "white hats") and among those in the computer security industry that the human factor is both the greatest strength and weakness in IT security.[36] This view has been validated by a recent series of major attack in 2011 and early 2012, most of which featured significant human elements. The belief that technological solutions or software fixes will emerge is an illusion and this has been clear since the early 2000s. While there are those who are still hoping for such as fix, it is unlikely to occur in the short to medium term.[37] This point of views appears, anecdotally, to be more pervasive in government than it is in the private sector.

The Outlook

The outlook for the short to medium term—until 2015—is not positive. Barring a catastrophic unanticipated attack like Pearl Harbor or 9/11, there does not appear to be either the political will or ability to tackle many of the major issues. Even when issues are known (such as the lack of deterrence), it will be years before the knowledge and skills are developed to initiate a solution.

In general, the "black hats" are getting better, and they are increasingly using social engineering techniques and targeted attacks to gain the advantage. In short, they can operate more effectively and are constantly developing new ideas such as brokerage houses for hackers as well as modularized software for hacking. Poorly written software with extensive zero day vulnerabilities assists them.

Complexity is a serious adversary by itself. Combined with interdependence, it may prove to be the Achilles Heel of infrastructure. The current trend is moving us towards systems which are creating more "single points of failure." This greatly enhances the motives and capabilities of attackers.

On a more positive front, however, the concept of P2P sharing among like minded institutions is growing. This will allow for a more immediate response to ongoing and/or potential problems. Anecdotal evidence to date shows response times in a P2P situation of hours, as opposed to days or weeks when done through official government channels.[38]

Conclusions

Large financial institutions and central banks should assume that, in the short to medium term, government efforts in cyber defence (especially from foreign threats) will be modest. Governments lack the theoretical framework for the necessary cyberspace deterrence and retaliatory capabilities and the "rules of the road" for determining international norms of behaviour have not been developed. The ability to prosecute criminals across state borders is limited and the threat of retaliation against state actors and criminals is minimally effective, if at all.

Institutions needing—or wanting—an effective cyber defence against attacks and exploitations will have to create their own localized defensive capabilities while developing their own intelligence sharing P2P networks to support these operations. Those institutions will need to provide their defensive IT workers with a flexible working environment where lateral thinking and creativity are actually allowed. This will include the ability to buy not only the latest "toys," but also access to information and methods that allow for the necessary validation of threat information to occur. Above all, the skills and capabilities need to be internal. Outsourcing in this case is an open invitation to fatal attacks. P2P sharing with like-minded institutions will provide the best information advantage and defensive capabilities for ongoing or impending events. Government capabilities in this area are limited and often untimely.

An optimistic view of when governments may take a leading role in defence against attackers or criminal prosecutions is 2015. Anecdotal evidence suggests a much later date due to the increasing rate of change in the cyber world and the limited rate of adaptation in government compounded by current government pre-occupation with economic issues.

Notes

1. “Former W.H. official: in the event of a cyberwar, don’t call DHS,” *National Defense*, 30 January 2012; available at http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=654.

2. Mark Clayton, “Is the cyberwarfare arms race for real? Survey of world experts says that it is,” *Christian Science Monitor*, 31 January 2012; available at http://www.csmonitor.com/USA/2012/0131/Is-the-cyberwarfare-arms-race-for-real-Survey-of-world-experts-says-it-is.

3. Richard L. Kugler, “Deterrence of Cyber Attacks,” in Franklin Kramer, Stuart Starr and Larry Wentz, eds., *Cyberpower and National Security* (Washington, DC: Potomac Books, 2009), 309-40.

4. For example, Pierre Lizée, *A Whole New World: Reinventing International Studies for the Post-Western World* (New York: Palgrave Macmillan, 2010); Ulrich Beck, Power in the Global Age (Cambridge: Polity Press, 2005).

5. United Kingdom, Cabinet Office, *Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London: November 2011); available at http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy.

6. Among the most glaring and damaging attacks were those on RSA/SecurID, supposedly a leader in the IT security field; the US government’s research labs at Oak Ridge; STRATFOR; Symantec/Norton Utilities; HB Gary, the Central Intelligence Agency and Visa.

7. Vincent Manzo, *Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?* INSS Strategic Forum 272 (Washington, DC: National Defense University, December 2011); available at http://www.ndu.edu/inss/docUploaded/SF%20272_Manzo%20.pdf.

8. David Gompert and Michael Koffmann, *Raising Our Sights: Russian-American Strategic Restraint in an Age of Vulnerability*, INSS Strategic Forum 274 (Washington, DC: National Defense University, January 2012); available at http://www.ndu.edu/press/lib/pdf/StrForum/SF-274.pdf.

9. For more on the “rules of the road” issue, see UK Cabinet Office, *Cyber Security Strategy*, 26–27. While this report addresses the issues and suggests 2015 as a target date for improvements, details on how this will happen are unclear and hence, overly optimistic.

10. Franklin Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in Franklin, Starr and Wentz, eds., *Cyberpower and National Security*, 15–17.

11. Kugler, "Deterrence of Cyber Attacks," 320–25.

12. Manzo, *Deterrence and Escalation*.

13. Gompert and Koffmann, *Raising Our Sights*, 7.

14. Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation, *Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism*, Washington, DC, 12 April 2011; available at: http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism. See also the briefing of the Marcella Hawkes, Director, Cyber Security Policy, Australian Government Attorney-General's Department, available at: http://aimp.apec.org/Documents/2011/TEL/TEL43-SPSG-WKSP/11_tel43_spsg_wksp_005.pdf.

15. Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: 2010), 1; available at http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf.

16. Australian Government, *Cyber Security Strategy* (Canberra, 2009), v; available at: http://www.ag.gov.au/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

17. UK Cabinet Office, *Cyber Security Strategy*.

18. Reliable statistics are impossible to obtain as the financial industry does not maintain a central database of such issues. Moreover, many institutions prefer not to report such losses for reputational reasons. As one senior insider stated: "Anecdotally it is a huge issue and often involves members of affinity groups responsible for much of the industry's fraud. Most security people in the banking industry expect a cyber crime attack on the banking industry over a physical attack."

19. Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (New York: Wiley, 2000); Kevin D. Mitnick and William Simon, *The Art of Deception: Controlling the Human Element of Security* (New York: Wiley, 2003); Joseph Menn, *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet* (PublicAffairs, 2010); Kevin D. Mitnick and William L. Simon, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (New York: Wiley, 2005). See also Verizon RISK Team, *2011 Data Breach Investigations Report,* available at http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

20. See, for example, *2012 EVT: Budget Deficit and Liquidity (The Chronicles of Everstate)*; available at http://www.redanalysis.org/2012/01/29/everstates-deepening-budget-deficit-and-increasing-need-for-liquidity-c-5230-c-5235/.

21. For a broader analysis of the structural problems in democratic states, see *Rising Discontent (The Chronicles of Everstate)*; available online at http://www.redanalysis.org/2012/01/15/starting-the-chronicles-of-everstate/; http://www.redanalysis.org/2012/01/22/the-chronicles-of-everstate-c-5230-c-5235-seeking-security/.

22. For a rare example of where a UK court held a software company liable for its product performance, see "High Court rules software liability clause not 'reasonable,'" available online at http://www.out-law.com/page-11011. High Court decision [2010] EWHC 965 (TCC), (2010) 26 Const LJ 542, available online at http://www.bailii.org/ew/cases/EWHC/TCC/2010/965.html.

23. For more on this issue, see, for example, Jintao Pan, "Software Reliability," Carnegie Mellon University, 1999, available online at http://www.ece.cmu.edu/~koopman/des_s99/sw_reliability/.

24. "Army activates first-of-its-kind Cyber Brigade," 9 December 2011, available at http://www.army.mil/article/70611/.

25. Clayton, "Is the cyberwarfare arms race for real?"

26. Gompert and Koffmann, *Raising Our Sights*.

27. "Former W.H. official: in the event of a cyberwar, don't call DHS," *National Defense*, 30 January 2012; available at http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=654.

28. The Russian cyber attacks on Estonia in 2007 and on Georgia and Lithuania in 2008 possible exceptions, depending on the definition of cyber war and how any one chosen definition relates to the more traditional form of kinetic warfare. For discussion of the definitional issues, "Real cyberwar: A taxonomy," available at http://www.infosecisland.com/blogview/19445-Real-Cyberwar-A-Taxonomy.html; "Marching off to cyberwar," *The Economist*, 4 December 2008; available at: http://www.economist.com/node/12673385.

29. Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act, or the PRECISE Act 2011, available at http://www.gpo.gov/fdsys/pkg/BILLS-112hr3674ih/pdf/BILLS-112hr3674ih.pdf.

30. See, for example, Paul Rosenzweig, "Promoting cybersecurity through the PRECISE Act," *The Heritage Foundation*, 6 February 2012; available at http://www.heritage.org/research/reports/2012/02/promoting-cybersecurity-through-the-precise-act.

31. See, among others, *Canada's Cyber Security Strategy.*

32. "Report: US tied for 4th among 23 countries in cyber defense," *Defense News*, 31 January 2012; available at http://www.defensenews.com/article/20120131/DEFREG02/301310002/Report-U-S-Tied-4th-Among-23-Countries-Cyber-Defense.

33. Menn, *Hunt for the New Crime Lords*.

34. Interview with software developer and marketer, 14 January 2012.

35. On these infrastructure vulnerabilities, see Charles P. Pfleeger and Shari Lawrence Pfleeger, *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach* (Englewood Cliffs, NJ: Prentice Hall, 2011), esp. xxv, 444; Amory B. Lovins and Hunter Lovins, *Brittle Power: Energy Strategy for National Security* (Amherst, NH: Brick House, 1982).

36. For more on the issue of the interplay between humans and technology in computer security, see Christopher Hadnagy, *Social Engineering: The Art of Human Hacking* (New York: Wiley, 2010); also Schneier, *Secrets and Lies*; Mitnick, *Art of Deception*; Mitnick, *Art of Intrusion*; and Menn, *Fatal System Error*.

37. Hadnagy, *Social Engineering*; Pfleeger and Pfleeger, *Analyzing Computer Security*, xxv.

38. The hacking of STRATFOR in December 2011 caused significant concerns for a number of institutions which were customers and had their information exposed. P2P sharing resulted in information being passed among the sharing partners on the same day, while the first official notification from a government agency of the problem did not occur for five days, long after defensive and remedial action had already been taken. Other governments responded in seven to thirteen days.

Glossary

Axiological targeting: A theory of target selection based on two Greek words *axios* (worthy) and *logos* (reason or theory). It is the study or theory of values—what targets are required to be attacked and what the value is of attacking them. Currently, there is only the weakest of information and theory available about how to attack cyber targets within the context of deterrence, escalation or retaliation.

Cyber exploitation: The process of removing information from computers and networks without authorization. This information can take any form including financial, technical, diplomatic or security related matters.

Cyber attacks: Destroying, altering or degrading computers and networks with a malicious intent.

Cyber war: No generally accepted definition of cyber warfare exists. Richard A. Clarke, in *Cyber War* (2010) defines it as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." Despite the (over)use of the term, it is arguable that there has only been one case of "cyber" as the fifth domain of warfare actually being used—the use of cyber attacks by the Russians during their partial invasion of Georgia in 2008.

Deterrence: The ability to demonstrate that you have the ability to stop your adversary from attacking as they believe that the cost of the attack/exploitation will outweigh the benefits. Deterrence threats have to be credible, timely, and proportional as well as being connected to the actions they are intended to deter. There has to be a direct connection between action and response to eliminate the possibility of the deterrence activity as being seen as coincidental by the adversary.

Escalation: The willingness to broaden the nature of the conflict or confrontation by shifting the nature of the retaliation targets or increasing the intensity or cost of the reaction.

Select Bibliography

Government Documents

Australian Government, *Cyber Security Strategy* (Canberra, 2009), v; available at http://www.ag.gov.au/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: 2010), 1; available at http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf.

United Kingdom, Cabinet Office, *Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London: November 2011); available at http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy

United States, Department of Homeland Security, *Quadrennial Homeland Security Review* (QHSR), February 2010: available at http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

Secondary Sources

Andress, Jason and Steve Winterfeld. 2011. *Cyberwarfare, Techniques, Tactics and Tools for Security Practitioners*. Waltham, MA: Syngress Publishers.

Conference Board. 2010. *Security as a Critical Component of Corporate Defense*. New York: The Conference Board.

Hadnagy, Christopher. 2010. *Social Engineering: The Art of Human Hacking*. New York: Wiley.

Kramer, Franklin, Stuart Starr and Larry Wentz, eds. 2009. *Cyberpower and National Security*. Washington, DC: Potomac Books.

Manzo, Vincent. 2011. *Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?* INSS Strategic Forum 272. Washington, DC: National Defense University, December; available at http://www.ndu.edu/inss/docUploaded/SF%20272_Manzo%20.pdf

Menn, Joseph. 2010. *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet.* New York: PublicAffairs Books.

Mitnick, Kevin D. and William Simon. 2003. *The Art of Deception: Controlling the Human Element of Security*. New York: Wiley.

________. 2005. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. New York: Wiley.

Pan, Jintao. 1999. "Software Reliability," Carnegie Mellon University; available at http://www.ece.cmu.edu/~koopman/des_s99/sw_reliability/.

Pfleeger, Charles P., and Shari Lawrence Pfleeger. 2011. *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach.* Englewood Cliffs, NJ: Prentice Hall

Schneier, Bruce. 2000. *Secrets and Lies: Digital Security in a Networked World.* New York: Wiley.

About the Author

Tom Quiggin is a Senior Researcher at the Canadian Centre of Intelligence and Security Studies at Carleton University. A court qualified expert on terrorism, he has 20 years of practical experience in a variety of intelligence positions. He has worked in an intelligence capacity for the Royal Canadian Mounted Police, the Canadian Armed Forces, the United Nations Protection Force in Yugoslavia, Citizen and Immigration Canada (War Crimes), the International War Crimes Tribunal for the former Yugoslavia (The Hague), and the Privy Council Office of Canada. He was also a qualified arms control inspector for the Conventional Forces in Europe Treaty and the Vienna Document. he is also the author of *Seeing the Invisible: National Security Intelligence in an Uncertain Age* (2007).

Centre for International and Defence Policy
Published in association with the
School of Policy Studies

The Centre for International and Defence Policy (CIDP) at Queen's University was established in 1975 to provide a focal point for research, publication and education on Canadian foreign and defence policy, and other aspects of international relations. We support a range of activities in the field of security and defence. Through publications and events, CIDP and its Fellows contribute to public debate on foreign and defence policy, and on issues of international peace and security. The Centre's purpose is to help shape a distinctive Canadian view of the world, and of Canada's role in global affairs.

To receive a list of the Centre's publications, or to order copies, please contact

Centre for International and Defence Policy
Robert Sutherland Hall 403
Queen's University
Kingston, ON K7L 3N6
CANADA

+1 (613) 533-2381

cidp@queensu.ca
www.queensu.ca/cidp

ISSN: 1205-7525
ISBN-13: 978-1-55339-356-6

“Don’t Call Us”

Governments, Cyber Security, and Implications for the Private Sector

Tom Quiggin

66
April 2012
Occasional Paper Series
Centre for International and Defence Policy
Queen's University

Library and Archives Canada Cataloguing in Publication

Quiggin, Thomas
"Don't call us" : governments, cyber security, and implications for the private sector / Tom Quiggin.

(Occasional paper, 1205-7525 ; 66)
Includes bibliographical references.
ISBN 978-1-55339-356-6

1. Cyberspace—Security measures—Government policy. 2. Computer security—Government policy. 3. Computer networks—Security measures—Government policy. 4. National security. 5. Cyberterrorism—Prevention. 6. Financial institutions—Computer networks—Security measures. 7. Business enterprises—Computer networks—Security measures. I. Queen's University (Kingston, Ont.). Centre for International and Defence Policy II. Title. III. Title: Do not call us. IV. Series: Occasional paper series (Queen's University (Kingston, Ont.). Centre for International and Defence Policy) ; 66

QA76.9.A25Q84 2012 005.8 C2012-902422-8

Table of Contents

Foreword v

The Problems 2

The Critical Issues 3

The Outlook 10

Conclusions 11

Notes 12

Glossary 17

Select Bibliography 19

About the Author 21

Foreword

In the last decade, the rapid and global expansion of digital networks has caused an expansion of the national security agenda in every western developed democracy. The increasing dependence on the internet has created an increasingly vulnerability of these crucial systems to attack. Computer systems that we use without much second thought can be readily and sometimes very easily compromised, and this exposure to exploitation thus poses a significant risk to all those who use these systems—governments, firms, and society at large. Moreover, in a sector where technological change is constant and fast-moving, and where national regulation is challenged by the essentially borderless nature of the internet, governments have been hard-pressed to be at the forefront of this aspect of national defence by putting in place systems of mutual defence against cyber exploitation across all sectors of the economy.

To be sure, governments have laid out their cyber security strategies with the intention of strengthening the capacity of both government and the private sector to deal with cyber exploitation. Certainly the United States, Britain, Australia and Canada have all produced cyber strategies that feature certain common elements. But global agreement on regulating this new digital world has been elusive.

In this Occasional Paper, Tom Quiggin explores the consequences for the private sector—and the financial sector in particular—of these difficulties. An expert in the intelligence field, Quiggin argues that for a number of structural reasons, including the longer-term effects of austerity measures being embraced across the globe, governments have been unable to develop effective cybersecurity systems for all crucial sectors of the economy. While governments continue to work to establish effective cyber defence mechanisms across all sectors of the economy, Quiggin is not optimistic that there will be any quick fix for this threat. For this reason, he suggests that in the short to medium term, the private sector will have to depend on its own resources to mount an effective defence against cyber attacks.

* * *

Occasional Papers published by the Centre for International and Defence Policy at Queen’s University are intended to provide both the policy community and the broader public with short analyses of contemporary issues in international and defence policy.

Kim Richard Nossal
Director
Centre for International and Defence Policy
Queen’s University
April 2012

"Don't Call Us": Governments, Cyber Security, and Implications for the Private Sector

Institutions that depend on computer systems must at present assume they have to depend on their own resources for defence against cyber attacks. As Jason Healey, the former White House Director of Cyber Infrastructure Protection, has admitted, if the United States is engaged in a cyberwar, Americans would be far better served by contacting Microsoft or AT&T rather than the Department of Homeland Security.[1] This high-risk problem is unlikely to be mitigated by government agencies in the short to medium term. A variety of systemic cyber protection weaknesses and increasingly aggressive attackers suggests that the intensity of cyber attacks will continue to increase over the short to medium term. Most Western governments—Sweden and Finland appear to be exceptions[2]—are incapable of deterring or preventing trans-border cyber attacks and do not have the means to effectively retaliate or escalate after an attack or exploitation. Thus without a significant deterrent ability, it is likely that cross-border cyber attacks and exploitation will continue unabated.[3]

The developed world is currently experiencing a period of complexity and uncertainty and is operating without an overarching political framework or ideology.[4] Economic competition for access to scarce resources and markets is producing cooperation at one level (trade) with vicious competition at another (cyber exploitation and attacks). These can occur simultaneously between any number of states. There is a "wild west" element in this competition and conflict, and no sheriff has emerged to enforce any set of rules.[5]

Large financial institutions and national central banks are located at the leading edge of this conflict, with little guidance from national governments on how to act or defend themselves in this environment. As a result, these institutions are left in a defensive mode against aggressive state actors, amorphous transnational hacking groups, organized crime groups and individuals.

Because of information technology (IT) “monolithic ubiquity”—in other words, the commonality of systems across large organizations—large institutions with significant IT infrastructure and security systems are equally, or in many cases even more, vulnerable to intrusion than many small-to-medium IT infrastructures. On the contrary: the large number of IT-oriented security institutions that have been seriously compromised in the last two years[6] suggests that the perception that larger institutions are inherently better protected against IT threats is largely mythical.

Peer-to-peer (P2P) sharing on threat information and protective measures is and will remain a high-value capability when combined with forward-leaning internal monitoring practices supported by open source intelligence collection. The outsourcing of IT capabilities, especially security monitoring, is a high risk option that should be avoided.

The Problems

Cyber attacks and cyber exploitation will continue to constitute a major risk. Governments, typically responsible for protecting public and private assets on the territory of the state from external aggression and from domestic/international criminal activity, are not capable of providing the required protection.

Among the critical areas of weakness related to government policy and/or law and regulations are the following:

- The lack of theory or practical activity in the role of deterrence, retaliation and/or escalation concerning cyber attacks or exploitation originating from foreign states.
- The relatively low priority that most governments attach to cyber defence issues, despite a number of public statements to the contrary.
- The limited knowledge and expertise on the emerging and little-understood role of insider threat and how to counteract it.
- The relatively low investment that software producers devote to improving the security of their product. Unlike providers of other mainstream products or services, software companies are rarely held financially liable for defects in their products.
- The slow response of the United States government to this problem. In most other areas of international competition or conflict, the United States is normally a leading international force. But in the area of

defence against cyber attacks and cyber exploitation, Washington has been slow to move. The first significant responses were in 2009/2010, and those responses tended to focus primarily on military related systems.

- The significant gap that exists between the reality of cyber problems and the ability of most Western governments to adapt to the constantly changing requirements needed to address the issues.
- The limited range of international law enforcement and intelligence-sharing capabilities. While intelligence sharing between states may be increasing, the short to medium term will be dominated by peer-to-peer sharing.
- The outsourcing of a variety of IT capabilities. This outsourcing remains one of the key areas for creating vulnerabilities and exposing systems to attacks and exploitation.
- The monolithic ubiquity of IT equipment and software common among large IT based organizations.
- The mistaken but nonetheless persistent belief (especially in government) that a technological solution exists to the problem of cyber security.

The Critical Issues

There are a number of critical issues that Western countries—governments and the private sector—need to address in the near term.

Deterrence Theory

In general terms, Western governments have not yet come to terms with the concepts of deterrence, escalation and retaliation when malicious cyber activity originates in a foreign state.[7] Until this occurs, transnational cyber exploitation and cyber attacks will continue to increase. Part of the reason for this is that no international norms exist for cyber behaviour, and thus the "rules of the road" are only now being addressed. Formal discussions between the major states concerned—the United States, the Russian Federation and the People's Republic of China—have only been proposed; no meetings have been scheduled.[8] It is thus unlikely that we will see any initial results before 2015.[9]

In the meanwhile, however, cyber vulnerabilities are growing, and cyber attack tools and methodologies are becoming more available. The technical capacity of malicious actors is improving.[10] As a result, various states and large transnational groups can carry out attacks with relative impunity given the lack of international understanding about what constitutes a proper series of responses.

During the Cold War, deterrence was well-developed and normalized. A "ladder of escalation" ranged from conventional responses to biological, chemical, and finally nuclear responses. A series of thresholds were understood by both of the superpowers as well as most other state and non-state actors. [11] These "rules" were initially understood to work within the three main domains of conflict: land, sea and air. In this context, a shared framework existed for understanding how any given confrontation or conflict might develop. These rules were, however, never clearly extended into outer space as it emerged as the fourth domain of conflict.

Likewise, the emergence of cyberspace as the fifth domain of conflict has not been accompanied by a generally accepted framework of analysis which would produce an internationally shared framework for deterrence and escalation.[12] Moreover, there is no internal consensus on such issues within most governments—including the United States—and nor is one likely to emerge in the immediate future. No ability exists to do axiological targeting in cyber space. Or, as put another way: "As [cyber] offenses improve, thresholds for war in space and especially cyberspace—though not nuclear war—could become perilously low, absent deterrence."[13]

On top of the inherent complexities and uncertainties involved in the cyber domain, a shared international framework of cyber deterrence would have to bridge cultural divides, force and network structures, national strategies and objectives, national and commercial level decision-making processes as well as concepts of proportionality. While this is not an impossible task, it is complex and the target date recently spoken of in a UK government paper does seem unduly optimistic.

Cyber Issues as a Priority

While many government officials claim that cyber security issues are a top priority,[14] the actual amount of effort, money and coordination going into actual solutions is uneven at best. For instance, the US Department of Homeland Security 2011 report on its Quadrennial Review lists cyber issues as fourth in a list of five priorities (behind terrorism, border security and immigration issues and ahead of ensuing resilience in disasters). The comparable document from Public Safety Canada in 2011 states that cyber issues are a "cornerstone" of national security, but offers little in actual priority setting or a comparison to other threats.[15] The Australian government *appears* to have a stronger interest and has described cyber security as a "top tier national security priority" while identifying the social and economic well being of the state as being "critically dependent" on the integrity of computer systems.[16] The United Kingdom also published a cyber strategy in 2011 and it puts cyber issues as a "Tier One" priority. It clearly identifies problems and potential solutions. However, even this UK report, the strongest of the four, notes that 2015 is a target date for selected solutions and improvements.[17]

The common theme of the Canadian and American documents appears to be well-meaning policy suggestions. Given that DHS in the USA and Public Safety in Canada lack the executive and budgetary control over the relevant intelligence and law enforcement agencies, no capabilities exist to bring the policies into reality. The reports are also making "2011 suggestions" but contain considerable baseline information from 2007 and 2008. By IT standards, this baseline information is questionable due to timeliness issues.

Behind the scenes, however, are two other systemic problems. The first is money. Governments frequently do not pay their staff sufficient money to ensure they are not being poached by private industry. In addition to the issue of compensation, there is the larger and perhaps more important issue of organization. By their nature, many IT workers tend to think in lateral and often non-linear terms. They function best when working in environments where self-emerging structures and solutions are the norm for any given problem set. Rapid adaption is desired and required, often on a daily or weekly basis. By contrast, governments, and other large bureaucracies, tend to be vertically oriented hierarchical structures which do not think in lateral or non-linear terms. Change occurs slowly and with great resistance as bureaucratic norms frequently tend to outweigh operational requirements, even at the cost of failure.

Insider Threat

The insider threat is emerging in both the physical and cyber security worlds. While firm statistics are difficult to come by,[18] the most pessimistic sources suggest that the majority of all cyber attacks have some form of insider activity.[19] This problem is being increasingly compounded by the de-legitimization of the state and its institutions. This enhanced threat is being compounded by the current economic downturn, government sponsored austerity measures and the co-incident inability of the state to deal with emerging structural problems.[20] Democratic states are also experiencing a particularly difficult set of circumstances. Mature Western democracies have developed increasing complex societies as a result of democratic processes. However, the ability of the state to deal with these complexities and the attendant problems has weakened at the same time.[21] As a result, insider threats are increasing and securing against these sorts of problems will be difficult.

Software Makers

With a few notable recent exceptions,[22] it has proven difficult to sue software manufacturers for security or performance defects in their products. Without this ability, software manufactures tend to treat security issues as an afterthought and only react with various patches and upgrades in after-the-fact activities. They also own security companies which then sell "solutions" to their own problems. Legislation to change this situation does not appear to be imminent in Europe, North America or South Asia.

The quality of the software is equally important to security as the defensive measures put around networks. High quality software (such as the quality levels applied to aircraft operating systems) has greater immunity to attacks based on its initial quality.[23] By contrast, lower quality software standards are generally applied, even in the financial industry, so failures and vulnerability to attacks will remain. Major software manufacturers generally only seriously consider security as an afterthought and then apply a "patch" mentality to the issue. Given the state of the industry and the complexity of the problem, it is unlikely that any major Western government will amend legislation in the short to medium future that will encourage software manufacturers to improve the quality of their product by exposing them to greater legal liability.

American Leadership

Despite pressure from both the private sector and its international allies, the United States government undertook limited action on responding to cyber threats from 1998, when the first emergence of serious sustained attacks occurred, to 2008. There appears to have been an increase in interest and activity from 2008 onwards, but even this is uneven and the first efforts were focused on military systems. President Barack Obama declared that digital infrastructure was a "strategic national asset," in 2009, and in June 2009 the US Secretary of Defense, Robert M. Gates, ordered the creation of Cyber Command (USCYBERCOM) within US Strategic Command. The first US Army Cyber Brigade was stood up on 1 December 2011.[24] However, this innovative command should not lead to the assumption that the US government is a leader in the cyber defence field. US cyber defences for non-military systems are no better than that of any other Western country, and arguably worse than countries such as Sweden, Finland and Israel.[25] A recent series of major foreign attacks against US government systems and corporations has demonstrated these weaknesses. As of early 2012, the American government has not even entered into formal talks with other states on issues concerning cyber security and the potential for cyber war. Talks in this area are at the proposal stage.[26]

Some American officials have recognized this weakness. Jason Healey's admission that Americans should not call the Department of Homeland Security in the event of a cyberwar has already been quoted. Healey, who is now the director of the cyber statecraft initiative at the Atlantic Council, went on to say that "If we do ever have a cyberwar, it will be won or lost in the private sector." He also admitted that he had little faith in the National Cybersecurity and Communications Integration Center, which is intended to be the lead agency for dealing with large-scale cyber-attacks.[27]

While no major example of cyber war exists,[28] it is increasingly clear that any such "war" would be won or lost in the private sector, as most governments have no ability to defend their own systems let alone the private sector. Western governments (and others) are not yet in the defensive fight. Indeed, at present it is not even clear who would have responsibility in the United States in the event of a major cyber incident. Legislation making its way through the US House of Representatives—HR 3674[29]— would give the Secretary of Homeland Security a leading role in cyber security, even though the National Security Agency has greater skills and personnel in this area. The working theory appears to be that a civilian-led agency should have control over a problem that will have an effect on mostly privately owned networks.[30] How this works in practice has not been made clear and the legislation has not yet passed; moreover, competing legislation may eventually award the lead to the NSA.

Gaps between Reality and Government Knowledge and Efforts

Government-based analysis tends to lag behind, rather than lead, knowledge creation efforts concerning cyber attacks. For instance, policy prescriptions contained in a series of government reports published in 2011 were based on 2007 and 2008 statistics.[31] Given that problems in the cyber world tend to evolve in periods of weeks and months, a government response based in an assessment cycle of years is not likely to be effective.

International Law Enforcement and Intelligence Sharing

Despite public comments to the contrary, the amount of domestic and international sharing and cooperation in IT security and criminal investigations is not encouraging. One particular area of concern is the sharing between national government agencies and the private sector. As the former White House Director of Cyber Infrastructure Protection stated in January 2012, "Government only inhales, it never exhales. It will take all the information, but it will find any excuse not to share."[32]

Internationally, the situation is not encouraging either. Jurisdictional disputes, complex legal requirements and a general lack of will on the part of some major governments have greatly restricted international investigations. As with deterrence and other issues, there are no immediate fixes in sight and no reason to be optimistic that this problem will be fixed in the near future.[33]

Outsourcing

Who writes your code that is in your security software and what do you know about it? "Not much" is the likeliest answer today. Many companies, including software security companies, are outsourcing their code-writing to sub- and to sub-sub contractors.[34] Frequently, this code-writing work is being done in the People's Republic of China, India, South Korea and even Libya. For the end user, there is no means of identifying the source of the code, and no way of knowing whether vulnerabilities have been built into the code at its point of origin. There is no legislation pending by major governments that may force software writers to disclose who wrote their software and where it was created.

Monolithic Ubiquity and the IT Vulnerability of Large Information Based Institutions

Despite their seeming outward differences, most large institutions with substantial IT infrastructures have many commonalities in servers, routers, software, power supplies and backup systems. They use many of the same types of software (such as Microsoft or Adobe) and the same kinds of security methods (appliances etc.). Consequently, once would-be attackers can determine vulnerability in one large institution, they can adapt that knowledge to be equally successful in attacking another. Additionally, large organizations tend to develop a sense of security based purely on their size and influence. Unfortunately, there is no correlation in the cyber world between the size of an IT infrastructure and its security. On the contrary: a small to medium size organization may present a more difficult target due to its lack of complexity, its small size and the likelihood that updates and patches will be applied automatically, unlike larger institutions.

In this case, a contrast exists between the physical world and the cyber world in security terms. There is a significant security difference between the cyber world and the physical world. In the physical world, a large bank or cash centre is less vulnerable to robberies than a corner convenience store because of its resources. In a convenience store, a determined robber will be able to defeat locked doors, basic alarms and a small safe. Those same skills would not allow a determined robber to attack a cash centre or major bank. In the cyber world, however, the size of an organization and its complexity do not make it less vulnerable—in fact the opposite appears to be occurring.

Complexity

Large complex systems increase the probability of flaws. Complexity and interdependency are known to be their own forms of weakness in computer systems, power grids and many other complex systems as well.[35] The constant addition of more technology has exacerbated the problem by adding complexity, more implicit assumptions and more vulnerability. The result is problematic, with new examples emerging such as the increased use of VOIP (voice over internet protocol) communications systems, virtualization on servers and the channelling of more information systems over the world wide web. The resulting complexity is—by itself—an emerging concern for IT systems vulnerability. Some governments are introducing the concept of having one government department responsible for all IT services and one portal for all Internet traffic. This may cause an increased level of complexity and interdependency which will render government more, rather than less, vulnerable to catastrophic failures.

Technological Solutions Sought by States and Corporations

There is a near total consensus of opinion among hackers (both "black hats" and "white hats") and among those in the computer security industry that the human factor is both the greatest strength and weakness in IT security.[36] This view has been validated by a recent series of major attack in 2011 and early 2012, most of which featured significant human elements. The belief that technological solutions or software fixes will emerge is an illusion and this has been clear since the early 2000s. While there are those who are still hoping for such as fix, it is unlikely to occur in the short to medium term.[37] This point of views appears, anecdotally, to be more pervasive in government than it is in the private sector.

The Outlook

The outlook for the short to medium term—until 2015—is not positive. Barring a catastrophic unanticipated attack like Pearl Harbor or 9/11, there does not appear to be either the political will or ability to tackle many of the major issues. Even when issues are known (such as the lack of deterrence), it will be years before the knowledge and skills are developed to initiate a solution.

In general, the "black hats" are getting better, and they are increasingly using social engineering techniques and targeted attacks to gain the advantage. In short, they can operate more effectively and are constantly developing new ideas such as brokerage houses for hackers as well as modularized software for hacking. Poorly written software with extensive zero day vulnerabilities assists them.

Complexity is a serious adversary by itself. Combined with interdependence, it may prove to be the Achilles Heel of infrastructure. The current trend is moving us towards systems which are creating more "single points of failure." This greatly enhances the motives and capabilities of attackers.

On a more positive front, however, the concept of P2P sharing among like minded institutions is growing. This will allow for a more immediate response to ongoing and/or potential problems. Anecdotal evidence to date shows response times in a P2P situation of hours, as opposed to days or weeks when done through official government channels.[38]

Conclusions

Large financial institutions and central banks should assume that, in the short to medium term, government efforts in cyber defence (especially from foreign threats) will be modest. Governments lack the theoretical framework for the necessary cyberspace deterrence and retaliatory capabilities and the "rules of the road" for determining international norms of behaviour have not been developed. The ability to prosecute criminals across state borders is limited and the threat of retaliation against state actors and criminals is minimally effective, if at all.

Institutions needing—or wanting—an effective cyber defence against attacks and exploitations will have to create their own localized defensive capabilities while developing their own intelligence sharing P2P networks to support these operations. Those institutions will need to provide their defensive IT workers with a flexible working environment where lateral thinking and creativity are actually allowed. This will include the ability to buy not only the latest "toys," but also access to information and methods that allow for the necessary validation of threat information to occur. Above all, the skills and capabilities need to be internal. Outsourcing in this case is an open invitation to fatal attacks. P2P sharing with like-minded institutions will provide the best information advantage and defensive capabilities for ongoing or impending events. Government capabilities in this area are limited and often untimely.

An optimistic view of when governments may take a leading role in defence against attackers or criminal prosecutions is 2015. Anecdotal evidence suggests a much later date due to the increasing rate of change in the cyber world and the limited rate of adaptation in government compounded by current government pre-occupation with economic issues.

Notes

1. “Former W.H. official: in the event of a cyberwar, don’t call DHS,” *National Defense*, 30 January 2012; available at http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=654.

2. Mark Clayton, “Is the cyberwarfare arms race for real? Survey of world experts says that it is,” *Christian Science Monitor*, 31 January 2012; available at http://www.csmonitor.com/USA/2012/0131/Is-the-cyberwarfare-arms-race-for-real-Survey-of-world-experts-says-it-is.

3. Richard L. Kugler, “Deterrence of Cyber Attacks,” in Franklin Kramer, Stuart Starr and Larry Wentz, eds., *Cyberpower and National Security* (Washington, DC: Potomac Books, 2009), 309-40.

4. For example, Pierre Lizée, *A Whole New World: Reinventing International Studies for the Post-Western World* (New York: Palgrave Macmillan, 2010); Ulrich Beck, Power in the Global Age (Cambridge: Polity Press, 2005).

5. United Kingdom, Cabinet Office, *Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London: November 2011); available at http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy.

6. Among the most glaring and damaging attacks were those on RSA/SecurID, supposedly a leader in the IT security field; the US government’s research labs at Oak Ridge; STRATFOR; Symantec/Norton Utilities; HB Gary, the Central Intelligence Agency and Visa.

7. Vincent Manzo, *Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?* INSS Strategic Forum 272 (Washington, DC: National Defense University, December 2011); available at http://www.ndu.edu/inss/docUploaded/SF%20272_Manzo%20.pdf.

8. David Gompert and Michael Koffmann, *Raising Our Sights: Russian-American Strategic Restraint in an Age of Vulnerability*, INSS Strategic Forum 274 (Washington, DC: National Defense University, January 2012); available at http://www.ndu.edu/press/lib/pdf/StrForum/SF-274.pdf.

9. For more on the “rules of the road” issue, see UK Cabinet Office, *Cyber Security Strategy*, 26–27. While this report addresses the issues and suggests 2015 as a target date for improvements, details on how this will happen are unclear and hence, overly optimistic.

10. Franklin Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in Franklin, Starr and Wentz, eds., *Cyberpower and National Security*, 15–17.

11. Kugler, "Deterrence of Cyber Attacks," 320–25.

12. Manzo, *Deterrence and Escalation*.

13. Gompert and Koffmann, *Raising Our Sights*, 7.

14. Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation, *Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism*, Washington, DC, 12 April 2011; available at: http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism. See also the briefing of the Marcella Hawkes, Director, Cyber Security Policy, Australian Government Attorney-General's Department, available at: http://aimp.apec.org/Documents/2011/TEL/TEL43-SPSG-WKSP/11_tel43_spsg_wksp_005.pdf.

15. Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: 2010), 1; available at http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf.

16. Australian Government, *Cyber Security Strategy* (Canberra, 2009), v; available at: http://www.ag.gov.au/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

17. UK Cabinet Office, *Cyber Security Strategy*.

18. Reliable statistics are impossible to obtain as the financial industry does not maintain a central database of such issues. Moreover, many institutions prefer not to report such losses for reputational reasons. As one senior insider stated: "Anecdotally it is a huge issue and often involves members of affinity groups responsible for much of the industry's fraud. Most security people in the banking industry expect a cyber crime attack on the banking industry over a physical attack."

19. Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (New York: Wiley, 2000); Kevin D. Mitnick and William Simon, *The Art of Deception: Controlling the Human Element of Security* (New York: Wiley, 2003); Joseph Menn, *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet* (PublicAffairs, 2010); Kevin D. Mitnick and William L. Simon, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (New York: Wiley, 2005). See also Verizon RISK Team, *2011 Data Breach Investigations Report,* available at http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

20. See, for example, Helene Lavoix, *2012 EVT: Budget Deficit and Liquidity (The Chronicles of Everstate)*; available at http://www.redanalysis.org/2012/01/29/everstates-deepening-budget-deficit-and-increasing-need-for-liquidity-c-5230-c-5235/.

21. For a broader analysis of the structural problems in democratic states, see Helene Lavoix, *Rising Discontent (The Chronicles of Everstate)*; available online at http://www.redanalysis.org/2012/01/15/starting-the-chronicles-of-everstate/; http://www.redanalysis.org/2012/01/22/the-chronicles-of-everstate-c-5230-c-5235-seeking-security/.

22. For a rare example of where a UK court held a software company liable for its product performance, see “High Court rules software liability clause not ‘reasonable,’” available online at http://www.out-law.com/page-11011. High Court decision [2010] EWHC 965 (TCC), (2010) 26 Const LJ 542, available online at http://www.bailii.org/ew/cases/EWHC/TCC/2010/965.html.

23. For more on this issue, see, for example, Jintao Pan, “Software Reliability,” Carnegie Mellon University, 1999, available online at http://www.ece.cmu.edu/~koopman/des_s99/sw_reliability/.

24. “Army activates first-of-its-kind Cyber Brigade,” 9 December 2011, available at http://www.army.mil/article/70611/.

25. Clayton, “Is the cyberwarfare arms race for real?”

26. Gompert and Koffmann, *Raising Our Sights*.

27. “Former W.H. official: in the event of a cyberwar, don’t call DHS,” *National Defense*, 30 January 2012; available at http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=654.

28. The Russian cyber attacks on Estonia in 2007 and on Georgia and Lithuania in 2008 possible exceptions, depending on the definition of cyber war and how any one chosen definition relates to the more traditional form of kinetic warfare. For discussion of the definitional issues, “Real cyberwar: A taxonomy,” available at http://www.infosecisland.com/blogview/19445-Real-Cyberwar-A-Taxonomy.html; “Marching off to cyberwar,” *The Economist*, 4 December 2008; available at: http://www.economist.com/node/12673385.

29. Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act, or the PRECISE Act 2011, available at http://www.gpo.gov/fdsys/pkg/BILLS-112hr3674ih/pdf/BILLS-112hr3674ih.pdf.

30. See, for example, Paul Rosenzweig, “Promoting cybersecurity through the PRECISE Act,” *The Heritage Foundation*, 6 February 2012; available at http://www.heritage.org/research/reports/2012/02/promoting-cybersecurity-through-the-precise-act.

31. See, among others, *Canada’s Cyber Security Strategy.*

32. “Report: US tied for 4th among 23 countries in cyber defense,” *Defense News*, 31 January 2012; available at http://www.defensenews.com/article/20120131/DEFREG02/301310002/Report-U-S-Tied-4th-Among-23-Countries-Cyber-Defense.

33. Menn, *Hunt for the New Crime Lords*.

34. Interview with software developer and marketer, 14 January 2012.

35. On these infrastructure vulnerabilities, see Charles P. Pfleeger and Shari Lawrence Pfleeger, *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach* (Englewood Cliffs, NJ: Prentice Hall, 2011), esp. xxv, 444; Amory B. Lovins and Hunter Lovins, *Brittle Power: Energy Strategy for National Security* (Amherst, NH: Brick House, 1982).

36. For more on the issue of the interplay between humans and technology in computer security, see Christopher Hadnagy, *Social Engineering: The Art of Human Hacking* (New York: Wiley, 2010); also Schneier, *Secrets and Lies*; Mitnick, *Art of Deception*; Mitnick, *Art of Intrusion*; and Menn, *Fatal System Error*.

37. Hadnagy, *Social Engineering*; Pfleeger and Pfleeger, *Analyzing Computer Security*, xxv.

38. The hacking of STRATFOR in December 2011 caused significant concerns for a number of institutions which were customers and had their information exposed. P2P sharing resulted in information being passed among the sharing partners on the same day, while the first official notification from a government agency of the problem did not occur for five days, long after defensive and remedial action had already been taken. Other governments responded in seven to thirteen days.

Glossary

Axiological targeting: A theory of target selection based on two Greek words *axios* (worthy) and *logos* (reason or theory). It is the study or theory of values—what targets are required to be attacked and what the value is of attacking them. Currently, there is only the weakest of information and theory available about how to attack cyber targets within the context of deterrence, escalation or retaliation.

Cyber exploitation: The process of removing information from computers and networks without authorization. This information can take any form including financial, technical, diplomatic or security related matters.

Cyber attacks: Destroying, altering or degrading computers and networks with a malicious intent.

Cyber war: No generally accepted definition of cyber warfare exists. Richard A. Clarke, in *Cyber War* (2010) defines it as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." Despite the (over)use of the term, it is arguable that there has only been one case of "cyber" as the fifth domain of warfare actually being used—the use of cyber attacks by the Russians during their partial invasion of Georgia in 2008.

Deterrence: The ability to demonstrate that you have the ability to stop your adversary from attacking as they believe that the cost of the attack/exploitation will outweigh the benefits. Deterrence threats have to be credible, timely, and proportional as well as being connected to the actions they are intended to deter. There has to be a direct connection between action and response to eliminate the possibility of the deterrence activity as being seen as coincidental by the adversary.

Escalation: The willingness to broaden the nature of the conflict or confrontation by shifting the nature of the retaliation targets or increasing the intensity or cost of the reaction.

Select Bibliography

Government Documents

Australian Government, *Cyber Security Strategy* (Canberra, 2009), v; available at http://www.ag.gov.au/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: 2010), 1; available at http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf.

United Kingdom, Cabinet Office, *Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London: November 2011); available at http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy

United States, Department of Homeland Security, *Quadrennial Homeland Security Review* (QHSR), February 2010: available at http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

Secondary Sources

Andress, Jason and Steve Winterfeld. 2011. *Cyberwarfare, Techniques, Tactics and Tools for Security Practitioners*. Waltham, MA: Syngress Publishers.

Conference Board. 2010. *Security as a Critical Component of Corporate Defense*. New York: The Conference Board.

Hadnagy, Christopher. 2010. *Social Engineering: The Art of Human Hacking*. New York: Wiley.

Kramer, Franklin, Stuart Starr and Larry Wentz, eds. 2009. *Cyberpower and National Security*. Washington, DC: Potomac Books.

Manzo, Vincent. 2011. *Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?* INSS Strategic Forum 272. Washington, DC: National Defense University, December; available at http://www.ndu.edu/inss/docUploaded/SF%20272_Manzo%20.pdf

Menn, Joseph. 2010. *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet.* New York: PublicAffairs Books.

Mitnick, Kevin D. and William Simon. 2003. *The Art of Deception: Controlling the Human Element of Security*. New York: Wiley.

________. 2005. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. New York: Wiley.

Pan, Jintao. 1999. "Software Reliability," Carnegie Mellon University; available at http://www.ece.cmu.edu/~koopman/des_s99/sw_reliability/.

Pfleeger, Charles P., and Shari Lawrence Pfleeger. 2011. *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach.* Englewood Cliffs, NJ: Prentice Hall

Schneier, Bruce. 2000. *Secrets and Lies: Digital Security in a Networked World.* New York: Wiley.

About the Author

Tom Quiggin is a Senior Researcher at the Canadian Centre of Intelligence and Security Studies at Carleton University. A court qualified expert on terrorism, he has 20 years of practical experience in a variety of intelligence positions. He has worked in an intelligence capacity for the Royal Canadian Mounted Police, the Canadian Armed Forces, the United Nations Protection Force in Yugoslavia, Citizen and Immigration Canada (War Crimes), the International War Crimes Tribunal for the former Yugoslavia (The Hague), and the Privy Council Office of Canada. He was also a qualified arms control inspector for the Conventional Forces in Europe Treaty and the Vienna Document. he is also the author of *Seeing the Invisible: National Security Intelligence in an Uncertain Age* (2007).

Centre for International and Defence Policy
Published in association with the
School of Policy Studies

The Centre for International and Defence Policy (CIDP) at Queen's University was established in 1975 to provide a focal point for research, publication and education on Canadian foreign and defence policy, and other aspects of international relations. We support a range of activities in the field of security and defence. Through publications and events, CIDP and its Fellows contribute to public debate on foreign and defence policy, and on issues of international peace and security. The Centre's purpose is to help shape a distinctive Canadian view of the world, and of Canada's role in global affairs.

To receive a list of the Centre's publications, or to order copies, please contact

Centre for International and Defence Policy
Robert Sutherland Hall 403
Queen's University
Kingston, ON K7L 3N6
CANADA

+1 (613) 533-2381

cidp@queensu.ca
www.queensu.ca/cidp

ISSN: 1205-7525
ISBN-13: 978-1-55339-356-6