Can We Ever Have Technological Security?

Thomas Keenan | October 2013

Strategic Studies Working Group Papers

CIC
Canadian International Council
Conseil International du Canada

CDFAI
Canadian Defence & Foreign Affairs Institute

About The Author

Dr. Thomas P. Keenan is a Professor in the Faculty of Environmental Design, Adjunct Professor of Computer Science and Research Fellow at the Centre for Military and Strategic Studies at the University of Calgary. His research focuses on computer security and the social implications of technology. With a background as a Systems Analyst and Systems Programmer for large mainframe computers, he taught Canada's first computer security course in 1976. He co-wrote and hosted the 1984 CBC IDEAS radio series "Crimes of the Future" and is the author of a forthcoming book on creepiness in technology. He holds a Bachelor's degree in Philosophy, a Master of Science (Engineering) degree in Mathematical Methods and Operations Research and a Master of Arts and a Doctorate in Education, all from Columbia University. He participated in the 1983 Department of Justice consultation that led to Canada's first computer crime law, and has served as an expert witness in several court cases.

A frequent contributor to the media and public discourse about technology, he was awarded the 2012 NSERC Award for Science Promotion. He holds numerous professional designations including Information Systems Professional of Canada (I.S.P.), and Information Technology Certified Professional (ITCP) and is a Fellow of the Canadian Information Processing Society. He received the Queen's Jubilee Commemorative Medal in 2003 and the Order of the University of Calgary in 2007. He currently serves on the boards of the SEEDS Foundation and the Information and Communications Technology Council of Canada, and has served as a Director of the Society for the Policing of Cyberspace and the Calgary Police Museum Interpretive Centre.

If you would like to download a copy of this report please visit **www.cdfai.org** or **www.opencanada.org**.

If you would like to be added to our mailing list or have questions about our publications please contact: contact@cdfai.org or info@opencanada.org.

ISSN 1925-4903

Executive Summary

There is no universally accepted definition of "technological security" though an increasing number of civilian and military personnel have it in their job description. A whole computer security industry, with an estimated 2013 value of $63.34B[1] has arisen to help those who deploy technology do that securely.

There is general agreement that technological security is becoming increasingly important as information and communications technology tools assume a growing role in the operation of all enterprises. The emergence of infowar and cyber warfare widens the scope of threat origination beyond those merely seeking financial gain or the intellectual challenge of hacking.

This paper presents some key aspects of technological security starting with the classic "Infosec Triad" of Confidentiality, Integrity and Availability. These concepts go a long way to providing a baseline level of "technological security." However, there are other factors that are especially relevant in the government and defence contexts.

These include:

- maintaining exclusive control of technology;
- keeping its very existence secret;
- anticipating and attempting to control new and disruptive technologies; and
- dealing with the inevitable failures both of technology and technology security.

Each of these is considered with suggestions for mitigating risks.

Absolute technology security is unattainable as long as humans are part of the system. Someone, or some group of people, must have the physical key, computer "root password" or other authority and that introduces human risk. What we can strive for is "appropriate security" where we use the right protection in the right way for the right information. Recent high profile information security failures in the US, notably the Manning and Snowden disclosures, would appear to indicate that there is much room for improvement.

Recommendations to improve technological security include:

- less reliance on "security through obscurity";
- minimizing exposure to leaks and social engineering through better policies and stronger enforcement;
- increasing the granularity of information classification;
- using "defense in depth" techniques;
- improving cybersecurity education, training, and monitoring;
- making greater use of machine learning, biologically-inspired computing, and related techniques; and
- planning for the inevitable failure both of the technology and the security that protects it.

1 ASDR Reports, Global Cyber Security Market 2013–2023, based on primary and secondary sources. Summary accessed August 12, 2013 at https://www.asdreports.com/shopexd.asp?id=3895.

Sommaire

Il n'existe pas de définition universellement acceptée de la « sécurité technologique » bien qu'un nombre de plus en plus grand d'employés civils et militaire l'aient dans leur description de tâches. Une industrie de sécurité informatique tout entière, avec une valeur estimée, en 2013, de 63,34 milliards de dollars[2] a vu le jour pour aider ceux qui déploient la technologie à le faire de façon sécuritaire.

On s'accorde généralement pour dire que la sécurité technologique est en voie de devenir de plus en plus importante à mesure que les outils de technologie de l'information et des communications assument un rôle croissant dans le fonctionnement de toutes les entreprises. L'émergence de l'infoguerre et de la cyberguerre élargit la portée de la création de la menace au-delà de ceux qui ne font que rechercher un gain financier ou le défi intellectuel du piratage informatique.

La présente communication propose quelques aspects clés de la sécurité technologique à commencer par la classique triade de la sécurité de l'information (infosec) de la confidentialité, de l'intégrité et de la disponibilité. Ces concepts contribuent fortement à établir un niveau de référence de « sécurité technologique ». Cependant, il y a d'autres facteurs qui sont particulièrement pertinents dans les contextes du gouvernement et de la défense.

Ce sont notamment :

- de maintenir le contrôle exclusif de la technologie
- de garder secrète son existence même
- d'anticiper et de tenter de contrôler des technologies nouvelles et perturbatrices
- de traiter avec les échecs inévitables de la technologie elle-même et de la sécurité technologique.

Chacun de ces facteurs est considéré, accompagné de suggestions de mitigation des risques.

La sécurité technologique absolue est impossible à atteindre tant et aussi longtemps que des humains font partie du système. Quelqu'un ou un groupe de personnes doit avoir la clé physique, le « mot de passe racine » de l'ordinateur ou autre autorisation et cela introduit le risque humain. Ce vers quoi nous pouvons viser, c'est une « sécurité appropriée » où nous utilisons la protection juste de la bonne façon pour l'information qu'il faut. Les échecs récents de sécurité de l'information aux États-Unis, notamment les divulgations de Manning et Snowden, sembleraient indiquer qu'il y a encore beaucoup de place pour de l'amélioration.

Les recommandations pour l'amélioration de la sécurité technologique incluent notamment :

- qu'on se fie moins à la « sécurité par l'obscurité »
- qu'on minimise l'exposition aux fuites et à l'ingénierie sociale à travers de meilleures politiques et une application plus vigoureuse de celles-ci
- qu'on augmente la granularité de la classification de l'information
- qu'on utilise des techniques de « défense en profondeur »
- qu'on améliore l'éducation, la formation et la surveillance de la cybersécurité
- qu'on fasse un plus grand usage de l'apprentissage machine (machine learning), de l'informatique d'inspiration biologique et des techniques apparentées
- qu'on planifie en vue de l'inévitable échec de la technologie et de la sécurité qui la protège.

2 ASDR Reports, Global Cyber Security Market 2013-2023, based on primary and secondary sources. Summary accessed August 12, 2013 at https://www.asdreports.com/shopexd.asp?id=3895.

Introduction

The world-wide annual cost of cybercrime has been pegged by an independent industry analyst firm at over $1 trillion.[3] Combating it has given rise to a fast-growing computer security industry that the same report estimates will reach over $80 billion annually by 2017. While businesses and individuals are frequent victims of unauthorized intrusions, in recent years government and military computers and networks have become increasingly attractive targets. Attacks have ranged from highly technical ones such as website hijacking and distributed denial of service packet floods to less technical approaches such as social engineering and spearfishing. Many countries are openly or covertly engaging in cyber-warfare, which frequently involves attacking technological assets of other countries and even quasi-political organizations such as the Office of His Holiness the Dalai Lama, as was revealed in 2009 by the Canadian-based Information Warfare Monitor project.[4]

Our critical reliance on technology for commerce, government and defence is obvious. What is far less clear is how to define an acceptable level of technological security, and what measures governments and others can use to try to achieve it. The 2013 controversy surrounding the disclosures of clandestine surveillance programs such as PRISM show that the public is keenly interested in the intersection between government information gathering and issues of privacy. It is an ongoing challenge to strike the balance between defending technological systems and violating national laws and expectations of privacy. Another balance that must be struck is between stimulating a nation's economy and improving national security. The NATO *Cybersecurity Framework Manual*[5] notes that "there can be an inherent tension between the openness required for innovation and the requirements of public security."

Computer security experts often speak of the "Infosec Triad"—confidentiality, integrity and availability. Techniques for accomplishing these goals are well covered in standard computer security texts such as those related to attaining the Certified Information Systems Security Professional (CISSP) designation.[6] These three dimensions of information security are the bread and butter of corporate, academic and government security departments around the world. They capture the essential baseline of technology security—that we be able to use information reliably, trust it, and be assured that it does not fall into the wrong hands.

Government and defence applications of technology raise additional and important security issues beyond those that are usually of concern in the commercial sector.

These include:

- maintaining exclusive control of technology;
- keeping its very existence secret;
- anticipating and attempting to control disruptive technologies; and
- dealing with the inevitable failures both of technology and technology security.

This paper focuses on the risks that are particularly relevant in the government and defence environments.

3 GIA, Inc., *Global Cyber Security Market to Reach $80.02 Billion by 2017, According to New Report by Global Industry Analysts, Inc.,* accessed August 12, 2013 at http://www.prweb.com/releases/cyber_security/application_content_data/prweb8262390.htm.

4 Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network,* report dated March 29, 2009, accessed August 12, 2013 at http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

5 Alexander Klim, (ed.) *National Cyber Security Framework Manual,* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellent, 2012, accessed August 12, 2013 at http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

6 Steven Hernandez CISSP, Official (ISC)2 Guide to the CISSP CBK, Third Edition, Clearwater, FL: (ISC)2 Press, 2012.

The True Value Of Technology

Technology is a tool to accomplish a specific purpose, not usually an end in itself. Increasingly, our goal is not so much to protect the technology as to protect the information it contains and the functionality it enables. Consider a smartphone left in a taxi by a sales representative on a business trip. The phone itself is worth at most a few hundred dollars. The value of having access to the information stored on it can easily exceed that. The now-missing appointment schedules, contact numbers and other information stored on the phone may have been vital for the success of the trip. An even greater value may be placed on keeping that information out of the hands of a competitor.

There are mitigation strategies (buying a new phone, re-downloading the missing information from a company computer, etc.) that can help to address the first two problems in this scenario. The third risk—information getting into the wrong hands—is far more worrying, since there is usually no way to regain exclusive possession of that information. Strategies such as on-device passwords, encryption, and remote wiping of the phone's contents do not always secure the information in an effective or timely manner.

A great number of technological advances had their origins in the defence industry, and then spread into civilian use. Of course the best known is the Internet that, while primarily implemented in academic research labs during the 1960s and 1970s, clearly benefited from the encouragement and funding of the US Department of Defense. By its very nature, the Internet thrived on connectivity so it was not long before civilian and commercial uses arose, aided significantly by US National Science Foundation funding in the 1980s and the development of the World Wide Web in 1989. While the core technology of the Internet—its robust routing protocol—was made freely available, control of technology was maintained to some extent by the creation of domains such as .MIL and by keeping certain information classified.

Many technological security vulnerabilities are really self-inflicted. People who should know better click on emails offering them a share of an undeserved $10M inheritance and thereby infect their own computers and others on their network. Malefactors use "social engineering" to dupe systems administrators with stories like "I forgot my password and my boss will kill me if I don't finish this report." Highly privileged users log on to bogus "free airport wifi" networks "for just a minute" and wind up infecting entire companies. All of these can, and should be addressed by having strong security policies and rules to enforce compliance, and practicing excellent and regular cyber-education.

There is a deeper level of vulnerability that we bring on ourselves in a more subtle way. It comes from having too much confidence in technology. Canadian software engineering pioneer David Parnas expresses it well, saying, "As a rule, software systems do not work well until they have been used, and have failed repeatedly, in real applications."[7] His advice is reminiscent of the observation of military strategist Helmuth von Moltke who famously wrote "No plan of operations extends with certainty beyond the first encounter with the enemy's main strength"[8] So, in addition to planning for the good times when technology is working well, we need to anticipate its inevitable failure and plan for that too.

The Challenge Of Maintaining Control Of Technology

The so-called "crypto wars" of the 1990s provide an excellent illustration of the difficulty of maintaining exclusive control of a technology. Sensing the value and power of strong cryptographic algorithms, and the danger of them falling into the hands of spies and criminals, various governments took extraordinary measures

7 David Parnas, et. al. "Evaluation of safety-critical software," *Communications of the ACM,* Vol. 33, No. 6, pp. 636–648, New York: Association for Computing Machinery, 1994.

8 Hughes, Daniel, ed. *Moltke on the Art of War: Selected Writings,* New York: Ballantine, 1993.

to try to control them. The US Department of Defense classified certain encryption algorithms as munitions under the International Traffic in Arms Regulations (ITAR) regime and even moved to block publication of academic papers.[9] The restrictions had some bizarre features. For example, a printed copy of the book *Applied Cryptography* could legally be shipped outside of the US, but the same information in machine readable form was restricted. There was also a move to force telecommunications equipment manufacturers to install the "Clipper chip," which would allow government eavesdropping on telephone conversations and other communications. Former Canadian Defence Minister Perrin Beatty came out against the Clipper chip,[10] but it was still likely that if the Clipper was implemented as planned, Canadian firms would be forced to implement it to do business in the US.

Opposition from the public, academics and privacy-minded legislators resulted in the end of US export controls on most forms of cryptography early in 2000. Another major factor was the widespread distribution of encryption programs[11] such as Phil Zimmermann's PGP ('Pretty Good Privacy') that, while different from the ones that were being restricted as munitions, brought strong encryption to the masses. The spread of PGP demonstrates an essential difference between digital information and a physical object such as a night vision scope. Digital data can be copied without leaving a trace, and can be instantly sent anywhere in the world. Once it has escaped, there is no way to call it back. The only way that governments could have tried to crack down on PGP encryption users would have been to monitor the passing around of floppy disks or to attempt to dig into Internet traffic looking for PGP.

The capability to do that, now called Deep Packet Inspection (DPI) was not widely available in the 1990s. Today, commercial vendors such as Cisco Systems, Inc., Allot Communications Ltd. and Procera Networks, Inc. all sell hardware that facilitates digging into Internet traffic to probe its content. Governments believed to have used DPI for law enforcement and/or censorship purposes include China, Korea, Iran, Libya, the Russian Federation, Syria, and the United States.[12] Concerned about the privacy implications of DPI, the Office of the Privacy Commissioner of Canada commissioned a series of papers on the subject in 2009, including an excellent overview by Roger Clarke.[13]

Mandating that Canadian Internet Service Providers install DPI equipment for the benefit of law enforcement agencies was a key feature of the Government of Canada's on-line surveillance legislation Bill C-30, which was withdrawn early in 2013. However, the crypto cat is definitely out of the bag, with an array of very strong encryption programs now widely available from anywhere in the world that doesn't drastically restrict its citizens' access to the Internet.

There are several signs that the ITAR approach of trying to control ICT technology is still being applied. One is the injunction imposed by a UK High Court on Flavio Garcia, a researcher at the University of Birmingham. Garcia had planned to present a paper[14] that would have divulged the secret codes used to secure luxury automobiles "including Porsches, Audis, Bentleys and Lamborghinis." He was ordered not to release the information, which he apparently obtained by "chip slicing," an expensive reverse engineering process that involves examining a chip under a microscope.

Another notable example was the recent temporary take down order relating to plans for "The Liberator"—a plastic gun that can be made on a 3D printer. The distributor of the 3D printable specifications

9 Len Adelman, Professor at University of California. *Contemporaneous Personal Communication.*

10 In a Toronto Sun column, as reported by the Electronic Frontier Foundation, accessed August 12, 2013 at http://w2.eff.org/Privacy/Key_escrow/Clipper/beatty_clipper_051495.statement.

11 Vic Sussman, "Lost in Kafka Territory :The feds go after a man who hoped to protect privacy rights," *US News and World Report,* posted March 26, 1995, accessed August 12, 2013 at http://www.usnews.com/usnews/news/articles/950403/archive_010975.htm.

12 Vivek Krishnamurthy, "The Dark Cloud of Deep Packet Inspection," accessed August 12, 2013 at http://www.csrandthelaw.com/2012/08/the-dark-cloud-of-deep-packet-inspection.

13 Roger Clarke, "Deep Packet Inspection: Its Nature and Implications," accessed August 12, 2013 at http://www.priv.gc.ca/information/research-recherche/2009/clarke_200903_e.asp.

14 Lisa O'Carroll, "Researcher's paper banned for containing luxury car security codes," *The Guardian,* July 26, 2013, accessed August 12, 2013 at http://www.rawstory.com/rs/2013/07/26/researchers-paper-banned-for-containing-luxury-car-security-codes.

file, Texas law student Cody Wilson, operating as Defense Distributed, received a letter in May 2013 from the US State Department ordering that "Defense Distributed should treat the above technical data as ITAR-controlled. This means that all such data should be removed from public access immediately."[15] Wilson complied, but the Sweden-based Pirate Bay website continued to make the plans freely available.[16]

The attempt to control 3D printed guns demonstrates an emerging complexity of trying to separate the virtual and physical worlds. The CAD instruction files that allow the creation of the gun are clearly virtual and have all the characteristics of digital information, notably instant accessibility and the inability to recapture them once they are distributed. After they have been used to make a gun, they become a physical object with all its normal properties. The platform technology (3D printers) to make this transformation are widely available, useful for many other functions, and almost impossible to control, although some legislators apparently want to try.[17]

Maintaining Secrecy

In his prophetic novel *1984,* George Orwell wrote "if you want to keep a secret you must also hide it from yourself. You must know all the while that it is there, but until it is needed you must never let it emerge into your consciousness in any shape that can be given a name." Such a draconian view of security is clearly impractical. The reality is that secrets must be understood and shared for us to go about our business in the real world. In today's world we also need to rely on technology to transmit, store, and organize those secrets.

At one time simply keeping the very existence of something secret could provide adequate security. The Manhattan Project, which led to the successful test of the atomic bomb in the Nevada desert, is an example of the success of "security through obscurity." While there were certainly atomic spies like Klaus Fuchs and Theodore Hall,[18] many of the scientists and soldiers who worked on the Manhattan Project took its secrets to the grave.

The remarkable events surrounding the disclosures by former NSA contractor Edward Snowden and US Army PFC Bradley Manning, and the subsequent outrage in intelligence circles, demonstrate that this approach is far less effective today. A cynic might say that today's intelligence workers lack the integrity of their forebears. Whether that is true or not is debatable, but the entire landscape is completely different from what prevailed in the 1940s. The volume of information being analyzed simply requires more personnel, and each one is a potential Snowden or Manning. General Keith B. Alexander, Commander of US Cyber Command and Director of the US National Security Agency (NSA) has announced that the NSA will be "reducing our system administrators by about 90 percent" in an attempt to cut down on the number of people who have access to sensitive information.[19] System Administrators typically hold the "keys to the kingdom" on computer systems and are charged with keeping them running properly. As a consequence, they are usually able to access any information on the system.

Besides the sheer number of people required by the intelligence apparatus, there is a trend towards using more civilian employees in intelligence functions.[20] The NSA's workforce is now approximately 60% civilian[21] and many of those are, as Snowden was, actually employees of defence contractors. The issuing of security

15 Andy Greenberg, "State Department Demands Takedown Of 3D-Printable Gun Files For Possible Export Control Violations," *Forbes,* May 9, 2013, accessed August 12, 2013 at http://www.forbes.com/sites/andygreenberg/2013/05/09/state-department-demands-takedown-of-3d-printable-gun-for-possible-export-control-violation.

16 Verified at http://thepiratebay.sx/torrent/8516819/DefDist_DEFCAD_Liberator_v1.1_accessed August 12, 2013.

17 Ball, James. *US government attempts to stifle 3D-printer gun designs will ultimately fail,* The Guardian, May 10, 2013, accessed August 12, 2013 at http://www.theguardian.com/commentisfree/2013/may/10/3d-printing-gun-blueprint-state-department-ban.

18 Marian Smith Holmes, Spies Who Spilled Atomic Bomb Secrets, *Smithsonian Magazine,* April 20, 2009, accessed August 12, 2013 at http://www.smithsonianmag.com/history-archaeology/Spies-Who-Spilled-Atomic-Bomb-Secrets.html.

19 Jonathan Allen, "NSA to cut system administrators by 90 percent to limit data access," *Reuters,* August 8, 2013, accessed August 12, 2013 at http://www.reuters.com/article/2013/08/09/us-usa-security-nsa-leaks-idUSBRE97801020130809.

20 Vinh Nguyen, "Current Trends in Intelligence Outsourcing Affect Work Force Stability," *Signal Online,* Fairfax VA: Armed Forces Communications and Electronics Association, December, 2007.

21 National Security Agency, "Inside the NSA," accessed August 12, 2013 at http://science.dodlive.mil/2013/05/16/inside-the-nsa.

clearances is also being outsourced to private contractors. According to blog posts[22] and news reports,[23] 75% of security checks are being done by private contractors, and according to the findings of a Senate subcommittee meeting on homeland security, "87% of those background checks are never fully completed."

Once he had his Top Secret clearance, Snowden had access to a substantial array of information, some of which he has since made public. The Bradley Manning case is an even more spectacular example of a low-ranking intelligence analyst being able to download and smuggle large quantities of information off the base. Manning's own statement at trial, which has not been contradicted by official sources, notes that "as an intelligence analyst, I had unlimited access to the CIDNE-I and CIDNE-A databases and the information contained within them."[24] These Combined Information Data Network Exchange databases contain tactical information collected from troops in Iraq and Afghanistan respectively.

We also know that he was able to access "251,287 diplomatic cables along with 391,000 reports that cover the war in Iraq from 2004 to 2009 and Afghanistan from 2004 to 2009"[25] and provide them to Wikileaks, which then made them publicly available, complete with a user-friendly interface to facilitate access and searching. Most remarkably, as stated in his testimony,[26] Manning was able to download the classified files to a CD-ROM, take them off the base, and copy them to an SD card—demonstrating that he did indeed have access to both read and copy a large quantity of information, not all of which was intimately related to his job function.

To be fair, there is the "needle in a stack of haystacks" argument that says the only way an analyst can find certain patterns is by comparing an incident to vast amounts of baseline data. While this may be true for some types of analysts, and some intelligence queries, it is certainly not true of all of them. In the US Intelligence Community there is already a classification structure, as well as Secure Compartmented Information (SCI), which imposes controls on information beyond the normal classification system. The Snowden and Manning disclosures appear to indicate that a great deal of non-SCI information is available to analysts on much more than a "need to know" basis.

General Alexander defended the NSA's extreme secrecy policies in a talk on July 31, 2013 at the Black Hat USA computer security conference. He noted that information, such as the details of the PRISM program is "not classified to keep it from you, a good person, it's classified because sitting among you are people who wish us harm. If we tell everybody exactly what we are doing then the adversaries will know how to get through our defenses."[27] However, it only took one whistleblower to seriously damage the fragile structure that kept this information from the public.

The editorial writer of the *Washington Post* captured the need for a much better organization and granularity of intelligence information to allow analysts to do their jobs while not being able to carry away an entire database: "Of course there must not be firewalls that prevent senior intelligence analysts and their bosses from seeing and sharing sensitive information. That does not mean a troubled 22-year-old in Baghdad should have access to secret State Department cables from all over the world. Surely there is a way to create a system that can do the former while preventing the latter."[28]

---

22 Gabriel Grand, "Edward Snowden: A Private Contractor Gave Snowden His Security Clearance—and Missed the Red Flags," *Policymic,* June 2013, accessed August 12, 2013 at http://www.policymic.com/articles/50417/edward-snowden-a-private-contractor-gave-snowden-his-security-clearance-and-missed-the-red-flags.

23 David Francis, *Here's How Edward Snowden Got 'Top Secret' Clearance, The Fiscal Times,* June 21, 2013 accessed August 12, 2013 at http://www.thefiscaltimes.com/Articles/2013/06/21/Heres-How-Edward-Snowden-Got-Top-Secret-Clearance.aspx#page1.

24 Alexa O'Brien, alexaobrien.com, posted February 28, 2013, accessed August 12, 2013 at http://www.alexaobrien.com/secondsight/wikileaks/bradley_manning/pfc_bradley_e_manning_providence_hearing_statement.html.

25 Verified at www.wikileaks.org, August 12, 2013.

26 The US Government has, as of this writing, not released official transcripts of the Bradley Manning trial. A public interest organization has paid a professional stenographer to transcribe the proceedings which, though unofficial, are regarded as generally accurate. Accessed August 12, 2013 at https://pressfreedomfoundation.org/bradley-manning-transcripts.

27 General Keith B. Alexander, keynote speech to Black Hat USA 2013, Las Vegas, July 31, 2013, accessed on August 12, 2013 at http://www.youtube.com/watch?v=4Sg4AtcW0LU.

28 Washington Post, "The Right Response to Wikileaks," *Washington Post,* November 30, 2010 accessed August 12, 2013 at http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112905985.html.

New And Disruptive Technologies

An oft-overlooked aspect of technological security is the inevitable development of new technologies that change the capability of users in a way that threatens security. Some are also disruptive in the sense used by Clayton M. Christensen,[29] i.e. they change existing markets and value networks. Three examples will be considered here to illustrate the changing risk landscape and some mitigation strategies.

Cloud Computing, a recent trend in information systems, has deep roots in the history of computing. In the 1960s and 1970s, when computers were too expensive for a single company to own, "time-sharing firms" would purchase a computer and sell access to fractions of its time to various users. Originally, this was done in a physical environment where users put in decks of punched cards and received their output on large, fan-folded paper printouts in mailbox-like slots. This was a common scenario for smaller oil companies in Calgary in the 1970s. Of course, sometimes an operator, through human error, placed company A's results in company B's slot. Often the information on the printout was highly proprietary data such as seismic or well log results. When this happened, etiquette demanded putting the errant printout in the right box, often with a "you owe me a beer" note attached. The advent of computer terminals reduced the need for this physical access, but people would still occasionally see each other's data in the online environment. Today, organizations that use "the cloud" store their data in distant computers, often not even knowing what country they are in. Employees then download information from the cloud onto laptops and smartphones, and may leave their device in an airport or taxicab. The fundamental risk to information is the same, but the new capabilities vastly increase the threat surface since someone seeking information can attack the cloud provider as well as the data in transit to and from the user, as well as at the endpoint.

Big Data and the associated data analytics tools are another technology that many people "didn't see coming." As demonstrated in two presentations at the 2013 DEFCON conference[30] data that was collected for one purpose can easily be "mined" and analyzed to make inferences and correlations about other subjects.[31] Driving this is the fact that data collection has become virtually ubiquitous. Grocery stores have "frequent buyer cards" that provide discounts but also allow them to track your purchases. Even if you don't join, it has been documented that stores, like the massive retailer Target build "guest profiles" and are even able to guess if a woman has recently become pregnant, and send her offers for baby products, in one case before even her family was aware of her condition![32]

Quantum Computing is one of the most intriguing areas of computer science, as well as a perfect demonstration of how technology risk can change over time. Combining ideas from quantum physics, computing and cryptography, it offers the tantalizing possibility of doing mathematical operations in fundamentally different ways. One of the implications is that many of the cryptographic algorithms currently in use to secure on-line banking, webpages, etc. may be breakable. Many of these are based upon the difficulty of dividing a very large number into factors that are prime numbers (divisible only by themselves and 1). As an example, a 309 digit number called RSA-1024 has not yet been reported to be factored and a $100,000 prize has been offered for doing so. Tackling this type of problem now can require years on large arrays of computers. Quantum computing should be able to greatly accelerate the process, thereby jeopardizing security based on this type of mathematics. D-Wave Systems, Inc. of Burnaby, BC has recently starting selling what they are calling "the first commercial quantum computing system on the market" and Google and NASA are using one in their Quantum Artificial Intelligence Laboratory housed at NASA's Ames Research Center in California.

29 Clayton M. Christensen, *The innovator's dilemma: when new technologies cause great firms to fail,* Boston, Massachusetts: Harvard Business School Press, 1997.

30 Keenan, Tom. "Torturing Open Government Systems for Fun, Profit and Time Travel," presentation at DEFCON 21, Las Vegas, NV, August 2, 2013, to be archived at *defcon.org.*

31 Burroughs, Daniel. "Open Public Sensors, Trend Monitoring and Data Fusion," presentation at DEFCON 21, Las Vegas, NV, August 4, 2013, to be archived at *defcon.org.*

32 Charles Duhigg, "How Companies Learn Your Secrets," New York Times, February 16, 2012, accessed August 12, 2013 at http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=2&hp&.

These three emerging technologies have one major communality—they allow people to do things that were not possible before, thereby putting previously secure information at risk. A further aspect is the "stealthy" aspect of technological intrusions. Unlike a physical attack, which may leave traces such as broken locks or images on surveillance cameras, technological means can be used to surreptitiously steal data over a prolonged period. Indeed this is exactly what happened in the famous case of TJX, Inc., the parent company of a number of stores including TJ Maxx in the US and Winners in Canada. TJX was the victim of a major data breach that was discovered in December 2006, but had apparently been going on for about a year, and affected over 45 million customers' credit card information. According to a detailed *Wall Street Journal* account of the intrusion[33] the data was siphoned off from badly secured wireless connections in stores. The unforeseen technology was as simple as wireless interception devices. In this case there were, in fact, warnings from the company's auditors about the lack of proper security for handling credit cards but TJX did not act on these.

The first mitigation strategy is, of course, to be aware of new technological developments. Fortunately, the same Internet that allows secrets to be leaked worldwide provides analysts a way to keep up with new technology developments. The harder, yet more important, part is to understand the potential impact of a new and/or disruptive technology on existing programs. While this is an ongoing process, there are stages (e.g. when TJX introduced wireless technology into its stores) where a detailed assessment should be done to tease out potential security risks. One approach, used in all of the US military academies as well as Canadian institutions, and, now, we know, in China[34] is to have Cyber War exercises in which teams try to attack and defend the technology. These can help to surface vulnerabilities that system designers never anticipated.

Failures Of Technology And Technological Security

There are two types of failures relevant to the subject of this paper. One is the failure of the technology itself, and the other is a failure of the technology's security protection.

Sooner or later, all technologies will fail. Aircraft designers realize this and build in redundant instrumentation and manual overrides for autopilots. Yet, even in that domain, some of the classic approaches are starting to fail. Cockpit automation is bringing new kinds of errors relating to the pilot's interface with technology[35] and proposed changes to airport landing systems and in flight separation may mean that things will soon happen too fast for a pilot to take over manual control, forcing reliance on technology.

Even our workhorse personal computers are susceptible to transient and undetected hardware memory errors. While this fascinating IBM Research paper[36] refers to an older generation of memory technology, and errors caused by stray cosmic rays, the possibility remains that any given piece of hardware can fail unpredictably, at any moment. Of course software is generally even more susceptible to errors. Evidence of this comes from the fact that even at the end of its lifecycle, Microsoft is still issuing regular "patches" for the Windows XP system it released in 2001. It is worth noting that these corrections themselves sometimes open up new vulnerabilities, so the term "Exploit Wednesday" has been coined to refer to the exploitation of new vulnerabilities released on the preceding "Patch Tuesday."

Recognizing the importance of anticipating and planning for technology failure, General C. Robert Kehler, Commander, US Strategic Command, Offutt AFB, Nebraska, writing in the context of space defence[37] stated "to enhance deterrence we have committed ourselves to prepar-ing our forces to 'fight through' any possible degradations or disruptions to our space capabilities."

33 Joseph Pereira, "Breaking the code: How Credit-Card Data Went Out the Wireless Door," *Wall Street Journal,* May 4, 2007, accessed August 12, 2013 (subscription may be required) at http://online.wsj.com/article/SB117824446226991797.html.

34 Graeme McMillan, "Chinese Military to Launch Cyber War Games Next Month," *Digital Trends,* May 30, 2013, accessed August 12, 2013 at http://www.digitaltrends.com/international/chinese-military-to-launch-cyber-war-games-next-month.

35 Kuo Kuang Liu, "The Highly-Automated Airplane: Its Impact on Aviation Safety and an Analysis of Training Philsophy," Air Force Institute of Technology thesis AFIT/GSM/LAC/97J- 1, 1997, Accessed August 12, 2013 at: http://www.dtic.mil/dtic/tr/fulltext/u2/a327119.pdf.

36 T. J. O'Gorman, et. al. , "Field testing for cosmic ray soft errors in semiconductor memories," *IBM Journal of Research and Development,* 40:41–50, Jan. 1996.

37 C. Robert Kehler, "Implementing the National Security Space Strategy." *Strategic Studies Quarterly,* Vol. 6.1, 2012.

The second category of failure we must address is the failure of the security measures designed to protect the technology. This could be through human actions such as espionage agents or whistleblowers, or through a lapse in technology, human error, or a lapse in protocol. Like technology failure, technological security failure is inevitable in most situations.

In one of the most terrifying novels about computerized military technology, published during the 1962 Cuban Missile Crisis, Eugene Burdick and Harvey Wheeler explain how things can go horribly wrong. *Fail-Safe* took its name from the engineering paradigm that systems should be designed so that, if something did go wrong, either no harm, or the least possible harm would occur.

Today, a new engineering model is being promoted called "Safe to Fail." University of Massachusetts professor Jack F. Ahearn writes[38] that:

> More recent thinking about change, disturbance, uncertainty, and adaptability is fundamental to the emerging science of resilience, the capacity of systems to reorganize and recover from change and disturbance without changing to other states—in other words, systems that are 'safe to fail.'

An excellent example of this type of reasoning is the new approach to flooding being pursued by the government of the Netherlands. The program, called *Planologische Kernbeslissing Ruimte voor de Rivie* (Room for the River) acknowledges the inevitability of annual flooding of the Rhine Delta and, through measures such as relocating dikes instead of building them ever higher, attempts to prepare the country physically and intellectually for the inevitable flooding.

Can I Just Hack The Bad Guys Right Back?

Active defence, or "hacking back" is an extremely thorny area of technology security. It often arises in cases where computers are being attacked from a known or unknown source via the Internet. Examples include website defacing, denial of service attacks, and malicious re-rerouting of traffic. A common sense notion of fairness and natural justice would seem to suggest that the victim of a technology-driven cyber-attack is justified in taking measures against the attacker, at least to "stop the pain." However, legal experts advise caution. Attempts to sabotage another organization's computers, even for self-defence, may well open the retaliator to charges under various computer hacking laws.

Consider, for example, the case where A's private and confidential files have been stolen by B and are being made available on a server owned by C. Assuming that it is technologically possible, is A justified in deleting the files, which are his stolen property, from C's server? Generally not, says Robert Clark, a lawyer and former CyberSecurity Compliance Officer in the US Department of Homeland Security. He told attendees at the Black Hat USA 2013 and DEFCON conferences that the common law doctrine of "trespass to chattel" provides some limited protection for someone who is trying to protest their property, including digital property. However, legal tests for this involve the action being "necessary to protect property" and "reasonable in relation to the harm threatened." An especially important factor is "previous and ongoing coordination with law enforcement agencies." In the defence context, political and diplomatic issues take the place of legal ones, but Clark's advice is the same—"proceed with caution."

Canadian Ronald J. Deibert was a principal investigator in the GhostNet investigation that disclosed Chinese hacking of high value targets such as embassies and office of the Tibetan Government in Exile. He bristles at the suggestion made by US lawyer Harvey Rishikof, chair of the Advisory Committee for the American Bar Association Standing Committee on Law and National Security, that Deibert's group hacked into foreign

38 Jack F. Ahearn, "From fail-safe to safe-to-fail: sustainability and resilience in the new urban world," unpublished paper, accessed August 12, 2013 at http://works.bepress.com/ahern_jack/2.

computers to carry out their investigations. "I insist that the Citizen Lab did not trespass or violate anything, and certainly not 'computers in foreign jurisdictions.' We simply browsed computers already connected to the public Internet, and did not force our way into them," Deibert writes in *Black Code*.[39] It is, however, clear from the results published in the GhostNet report[40] that these researchers set up a "honey pot" computer that could be infected with the ghOstRAT Trojan to lure foreign hackers into divulging the details of their *modus operandi*. The legal, moral and ethical limits pertaining to active defence are still being worked out in academic discussions and in courtrooms around the world.

Protecting The Right Assets The Right Way

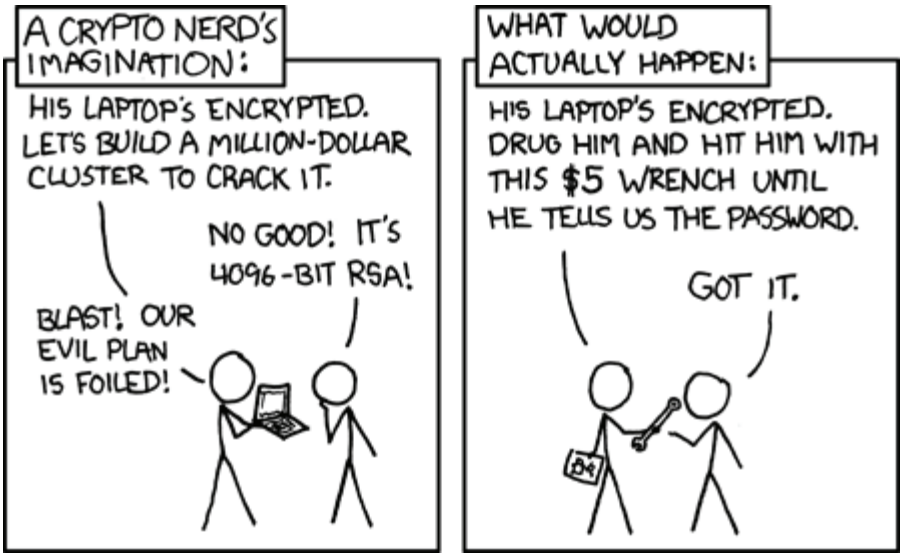
People giving technology security briefings often show this xkcd comic strip[41]

It concisely illustrates the consequences of failing to properly identify and protect what is truly valuable. Even the best technological measures are ineffective unless the sensitivity of information is properly understood and the right things are protected. A cynic might say that the recent embarrassing disclosures by Manning and Snowden fit the shoebox model.

In a fascinating presentation at Black Hat USA 2013 on "insider threats", Patrick Reidy—Chief Information Security Office of the Federal Bureau of Investigation—joked that he receives several emails a day from security vendors offering to "Snowden-proof" his system. He said he rebuffs them all since the threats he fears most are from people who are already inside the FBI's firewall and have all the access they need to steal the Bureau's information.

39 Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace,* Toronto: McClelland & Stewart, 2013.
40 Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network, March 29, 2009, p. 30, accessed August 12, 2013* at http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.
41 permission to reproduce for non-commercial use granted under Creative Commons License at http://xkcd.com/916/, accessed August 12, 2013.

The further limitations of technical safeguards in the face of human frailty are well captured by this xkcd comic.[42]



Encryption is certainly an important tool that can be used to protect data communications in transit and, to some extent, data stored on devices such as computers and smart phones. However, the data must eventually be decrypted (converted to plain text) so it can be viewed by humans or acted upon by computer programs. At this stage non-technical vulnerabilities enter into the picture.

The risk alluded to in the second comic strip, coercion, is just one of a vast array of "social engineering" techniques that prey on human weaknesses. Chief among them is phishing (sending false emails with an attractive incentive to lure people into clicking on it and thereby infecting their computers) and spear phishing (the same concept, but targeted to specific people based on their position or level of access.) Spearfishing is a growing vulnerability because it preys on human nature and lax policies. Indeed the technique has been tested on cadets at the United States Military Academy at West Point, NY. In an experiment conducted in 2004, 500 cadets there were sent an email from a fictitious Col. Robert Melville and 80% were tricked into clicking on a link contained in it.[43]

As for the right way to protect assets, most experts recommend a multi-layered approach, based on Defense in Depth—a military strategy that stretches back at least to Roman times. It was employed by Hannibal at the Battle of Carnae to encircle and destroy ten Roman legions, who outnumbered his army. In the computer security context it is a strategy promoted by the National Security Agency[44] involving multiple layers of security so that, even if an intruder breaches one, the others will prevent unauthorized access or tampering. Typically these layers are implemented as controls on the network boundaries (such as firewalls), authentication/access control measures (passwords, access control lists) and detection functionality (antivirus software, intrusion detection systems).

42 permission to reproduce for non-commercial use granted under Creative Commons License at http://xkcd.com/538/, accessed August 12, 2013.
43 David Bank, "'Spear Phishing' Tests Educate People About Online Scams," *Wall Street Journal,* August 17, 2005.
44 National Security Agency "Defense in Depth," accessed August 12, 2013 at http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

It is perhaps instructive to apply the Defense in Depth principle to defending your car in a parking lot. Locking your valuables in the trunk minimizes the attractiveness of your vehicle to thieves. So does parking in a well lit area. Then, of course you want to lock your doors and possibly have a car alarm system. If you are unlucky enough to be a victim, the operator of the lot might have security video footage that will help you make a police report and possibly even catch the perpetrators.

It's important to realize that even Defense in Depth can be thwarted. Car thieves can now buy a device that intercepts the signal between your car and the key fob. You push the lock button; it intercepts the signal and tells the car to emit a satisfying honk of the horn or flash of the lights. Yet your car is not really locked, and the thief can ransack it at leisure. A variant of this allows the interceptor to capture the lock/unlock codes and use them at will. So technological security is not something we can achieve, it is something we must continually strive for. We also need to establish reasonable limits on how far we will go for the sake of security. Encasing your car completely in a concrete slab is a great way to keep it secure, but totally impractical.

One major difference between technological crime and physical crime is that the former often leaves no meaningful traces. Officials of TJX did not realize that their customers' data was being stolen, though their auditors flagged it as a potential vulnerability. While General Alexander, in his BlackHat speech, spoke of the extensive audit trails in place at the NSA, it is not at all obvious that the data exfilitrations by Snowden and Manning would have come to light if they had not disclosed them themselves.

Other technological security vulnerabilities include supply chain tampering and sabotage, such as the widely discussed Stuxnet computer worm that targeted Iranian organizations[45] and "DNS poisoning" which causes computers to look in the wrong place for trusted webpages. Details of these are beyond the scope of this paper but it is worth noting that a Defense in Depth strategy may be effective against them.

There are some laudable efforts to completely re-engineer computer security. One is the US DARPA-funded Clean Slate Design of Resilient, Adaptive, Secure Hosts (CRASH) project announced in 2010.[46] The goal is to make a fresh start in hardware, software and network design to build systems that are inherently more resistant to cyber attack. Taking inspiration from human biology, the project's design document talks about modeling computer networks on the two types of immunity (innate and active) exhibited by biological systems. One of the technical areas to be studied is "Machine-Learning, Self-Adaptation, Diagnosis, Recovery and Repair" with the goal of building self-repairing technological systems that are even more robust than current ones.

Will CRASH succeed in creating new paradigms for secure computing? It's too early to tell, but a meeting of the Principal Investigators was held in San Diego on November 13–15, 2012. In a delightfully revealing message on the conference registration page, the organizers note that "we are currently experiencing compatibility issues with the Google Chrome and Opera browers (sic) and the payment processing system. Please DO NOT use these browsers when registering/paying on this website." So even the best minds in computer security can't use a spell checker, or get their website to properly take our money online! Then again, this certainly supports their notion that much work remains to be done.

Conclusions And Policy Recommendations

Absolute technology security is less attainable than ever for a number of reasons. The weakest link is still usually the human component of the system. Brigadier-General Greg Loos served as Director General, Cyber, Canadian Forces, from 2011 to 2013. He notes that "everyone in the department, military and civilian; they are sitting at a keyboard and they have to understand the consequences of their actions."[47]

45 David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum,* February 26, 2013, accessed August 12, 2013 at http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

46 DARPA, Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH,) Broad Agency Announcement DARPA-BAA-10-7, June 1, 2010, accessed August 12, 2013 at https://www.fbo.gov/utils/view?id=82f6068978da5339752c89d2f65d89ca.

47 Chris Thatcher, "Operationalizing the Cyber Domain," Vanguard, June/July 2013, accessed August 12, 2013 at http://vanguardcanada.com/operationalizing-the-cyber-domain.

On the civilian site, blogger Mark Collins[48] writes that the news is "not exactly encouraging about the (Canadian) government's (Cyber Security) capabilities." Another commentator[49] writes that "inside Public Safety Canada, the Canadian Cyber Incident Response Centre (CCIRC) evaluates the seriousness of cyber-threats against Canadian systems and provides advice to average Canadians and businesses on how and what to protect themselves against. But CCIRC is only able to act on information it is provided from private companies; it does not monitor their networks for cyber incidents."

A further controversy concerns the CCIRC's operating hours which, according to their 2010–2015 *Action Plan* will be increasing to 15 hours per day.[50] While that may be a laudable goal, the fact is that every major CERT (Computer Emergency Response Team) in the world already operates on a 24/7 basis. Cyberthreats come in from all over the globe, at all hours of the day and night, and some emergencies can't wait for business hours. The inadequate operating hours of the CCIRC were flagged by Canada's auditor general who wrote in his Fall 2012 report, "As CCIRC is not operating around the clock, there is a risk that there will be a delay in the sharing of critical information linked to newly discovered vulnerabilities or active cyber events reported to CCIRC after operating hours."[51]

Modern technology systems are orders of magnitude more complex than, say, tattooing a secret message on the head of a messenger and waiting for the hair to grow in (an ancient form of encryption technology.) It has been said that no single person can fully understand major software products such as the Windows operating system. The environment in which they operate is also more complex, international and populated by criminals, state-sponsored terrorists and even "script kiddies," all targeting our assets. An intruder only needs to find one unpatched vulnerability; the defenders must guard against all attacks. Technological security is a challenging battle, and the endpoint keeps receding as new technologies, and new ways to attack them, emerge on a daily basis.

To summarize the policy recommendations in this paper, in order to enhance cybersecurity the Government of Canada, and others, should:

1. Not rely on security through obscurity;
2. Minimize exposure to social engineering and related attacks through good policies and strict adherence;
3. Increase the granularity of information classification;
3. Use Defense in Depth to put multiple barriers in the way of an adversary;
4. Plan carefully for failure both of technology and of technology security using the "safe to fail" approach;
5. Apply machine learning, self-repairing technologies, bio- and neuro-morphic computing;
6. Institute continuous cybersecurity awareness and training programs; and
7. Actively model threats through cybersecurity exercises, hackathons, and red team exercises.

48 Mark Collins, Canadian Government's Cyber Security Action Plan, 3DS Blog, accessed August 12, 2013 at http://cdfai3ds.wordpress.com/2013/04/15/mark-collins-canadian-governments-cyber-security-action-plan.

49 Milnews.ca, "What's Canada Buying? — April 13, 2013", accessed August 12, 2013 at http://milnewsca.wordpress.com/2013/04/13/wcb-131700utc-apr-13.

50 Public Safety Canada, "Action Plan 2010–2015 for Canada's Cyber Security Strategy," accessed August 21, 2013 at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx.

51 Auditor General of Canada, *2012 Fall Report of the Auditor General of Canada,* section 3.44, accessed August 12, 2013 at http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html#hd4c.

Bibliography

Araya, D. Et al. (eds.) *Nexus: New Intersections in Internet Research.* New York, NY: Peter Lang, 2011.

Bamford, J. *The Shadow Factory.* New York, NY: Doubleday, 2008.

Batra, N.D. *Digital Freedom: How Much Can You Handle?* Lanham, MD: Rowman & Littlefield, 2008.

Campen, A. *The First Information War: The Story of communications, computers, and intelligence systems in the Persian Gulf War,* Fairfax, VA: AFCEA Press, 1992.

Deibert, R. et.al. (eds.) *Access Controlled: The Shaping of Power, Right and Rule in Cyberspace,* Cambridge, MA: The MIT Press, 2010.

Gardner, D. Risk: *The Science and Politics of Fear,* Toronto, ON: McClelland & Stewart, 2008.

McGrath, J. *Loving Big Brother: Performance, Privacy and Surveillance Space,* London, UK: Routledge, 2004.

Monahan, T. *Surveillance and Security: Technological Politics and Power in Everyday Life,* New York, NY: Routledge, 2006.

Prensky, M. *Brain Gain,* New York, NY: Palgrave Macmillian, 2012.

Tipton, Harold F. *Guide to the CISSP CBK, Third Edition,* Clearwater, FL: ISC2 Publishing. 2012.

Winterfield, S., Andress, J. *The Basics of Cyber Warfare,* Waltham, MA: Elsevier, 2013.

Zalewski, Michal. *Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks,* San Francisco: No Starch Press, Inc., 2005.

Strategic Studies Working Group

The Strategic Studies Working Group (SSWG)is a partnership between the Canadian International Council (CIC) and the Canadian Defence and Foreign Affairs Institute (CDFAI). The CIC absorbed the former Canadian Institute of Strategic Studies (CISS) upon the CIC's formation in 2008, and the CISS's original focus is now executed by the SSWG.