Security-Policy
NET Nexus of Emerging Technologies

BRIEFING NOTES

BN-64-Space and Cyberspace-May2021

CYBER DECEPTION - THE ART OF CAMOUFLAGE, STEALTH AND MISDIRECTION

Authors: Dave McMahon, Clairvoyance Cyber Corp

SUMMARY

- Cyber deception has been practiced for decades and electronic deception for a century. While, deception has been central to warfare for millennia. Cyber deception is established as best practice to the extent that it is mandated in policy and standards is supported in domestic and international law. Furthermore, cyber deception is critical to intelligence collection, adversarial management to actively defend, disrupt deter and deter, or creating effects on one’s opponent. A military can employ deception in a decisive engagement then disappear, re-spawn and maneuver within the domain. It is a principal concept of warfare. Any military that has not fully operationalized cyber deception is strategically disadvantaged against pacing threats and foes.

NEED

Pacing threats. The asymmetric nature of cyber technology, places sophisticated offensive cyber capabilities in the hands of most nations and non-state actors. Industrial capability is becoming weaponized. Russia and China are competing aggressively against Canada in the cyber and cognitive domains. Foreign militaries have overrun networks of importance to Canada, purposefully interfered critical infrastructure, attempted to influence and subverted the democratic process. Canada’s adversaries are well practiced in mis-direction and deception in the domain. Western doctrine best follow suit.

A modern military must develop, equip, and train forces to operate in cyberspace in order to preserve freedom of manoeuvre, and the ability to deliver effects against our adversaries in support of national objectives. Actionable, accurate and timely cyber intelligence is critical to situational awareness, as is projecting power and influence in cyberspace. Resilience is important but has focused on hardened static defences. Sometimes it is best not to be in the line-of-fire even if you think you are bulletproof. Increasing emphasis in the future will be placed on anticipatory intelligence, deterrence, deception, persistent engagement, an active forward defence, effects and fires in the cyber domain.

There is a huge benefit to the use of deception in the defence of our digital battle space. Cyber deception in defence is likely to lead to the most interesting development of cyber combat effort and activity.

“I believe that one of our strongest tools for conflict prevention is deterrence, which requires the right mix of military capabilities, credible will to use those capabilities, and clear communication to adversaries.” – Chief of Defence Staff

BACKGROUND

Deception has been central calculus of warfare, diplomacy, business and sport since beginning of recorded history. Electronic deception was used to great effect since WW1 and cyber deception for the past 40 years. The cyber deception technology market is currently estimated to grow to $12 Billion by 2022. Global cyber threat intelligence services use deception infrastructures to: collect malware and fingerprint the Tactics, Techniques and Procedures (TTP) of Advanced Persistent Threats (APT). Deception technology has also proven the most effective means of detecting zero-day exploits. Thus, cyber deception has been established as best practice for cyber security for quite some time.

"*All warfare is based on deception. There is no place where espionage is not used. Offer the enemy bait to lure him*." **—** Sun tzu, The Art of War

Joint Doctrine for Military Deception JP 3-58 says that military deception is applicable at each level-of-war and across the range of military operations including cyber. It is defined as being those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions and operations, thereby causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission. Military deception can be employed during all phases of military operations. Canada has admired the challenge and benefits for quite some time.

The Canadian Forces Information Warfare Conceptual Framework developed by LCdr Robert Garigue, Ph.D., in 1994, as deputy commander of the Canadian Forces Information Operations Group (CFIOG), prophesised of semantic warfare and cyber deception in-depth. The concepts remain valid today. Dr. Garigue went on to become the Chief Security Officer of Bell Canada and one of the highly recognized cyber security visionaries of the time.

The Interdepartmental Committee on Information Warfare was established in 1994.[1] Here, operational concepts and national policy for Canada was drafted for proactive defence, cyber psychological operations and deception. The Treasury Board Secretariat built upon these concepts in the 2009 Canadian Proactive Cyber Security Strategy. Meanwhile, our allies have taken the concepts further.

The United Kingdom established its first research unit focused solely on cyber deception in November 2019, reflecting growing awareness of the importance of deception in this domain. The National Cyber Deception Laboratory (NCDL) is administered by Cranfield University on behalf of the UK MoD and is based at the Ministry of Defence's Cyber School, at the UK Defence Academy.

Deception is a hallmark of military and intelligence operations. - UK Cyber deception lab

On June 7, 2017, the Government of Canada released the Defence Policy - Strong, Secure, Engaged (SSE). The policy established the Government of Canada's defence priorities, which included new investment to support to cyber. The Defence policy emphasized the importance of developing capabilities related cyber threat identification, attribution, response actions, cyber deception and

[1] LCDR Garigue was the military representative and Co-Chair. Other members included CSE, CSIS, PCO, DFAIT, RCMP, DOJ

development of offensive cyber operations.[2] The CDS expanded higher-intent[3] in Directive for Defensive Cyber Operations (DCO) to include cyber deception.

U.S. and NATO doctrine recognizes many enabling aspects and conditions to modern warfare, such as military deception (MILDEC), psychological operations (PO), electronic warfare (EW), information operations (IO), Command and control warfare (C2W)[4] and unconventional warfare (UW).

NATO Best Practices in Computer Network Defence, published in 2014, re-enforced the need for cyber deception, forward-deployed intelligence collection and active defence.[5] The Tallinn Manual International Law Cyber Warfare (Rule 61 – Ruses) permits cyber deception operations during both war and peace as an effective means of defence. Recently, NATO experimented with Deceptive Tactics to Lure Russian cyber operatives. Over a thousand people participated in the exercise.

Russian military doctrine Maskirovka (disguise) covers a broad range of measures for military deception, from camouflage, concealment, imitation, manipulation, decoys, disinformation across all domains, and particularly cyber were Maskirovka is most effective. A goal of military deception is surprise (vnezapnost) so the two are naturally practiced together. Russia has a history of operating with a more complete (hybrid) inclusion of elements of military power and influence than countries like Canada. [Cyber deception] enables Russia's First Offset against the West that gives Russia new leverage on the battlefield.[6]

The Russian State often conducts cyber deception and offensive operations through proxies or with letters-of-mark. Notable Examples include the Russian Business Network (RBN) and the Internet Research Agency (IRA) - known in Russian Internet slang as the Trolls from Olgino. The IRA is a Russian company engaged in online influence operations on behalf of Russian military, political and organized crime. It is linked to Russian oligarch Yevgeny Prigozhin and based in Saint Petersburg, Russia. Both these organizations and advanced persistent threats (APT) linked to Russian State security and military operate aggressively against Canada today.

Canada, for its part, has used electronic deception as part of electronic warfare support and counter-measures in times of war and peace - during exercises on the border of with former Warsaw pact in the 1980's and military operations from Yugoslavia to the Gulf and Afghanistan. Techniques may

[2] SSE Initiative 65. Information operations capabilities and cyber capabilities, situational awareness, cyber threat identification and response, and the development of military-specific information operations and offensive cyber operations capabilities able to target, exploit, influence and attack in support of military operations.
SSE Initiative 87. Protect critical military networks and equipment from cyber-attack by establishing a new Cyber Mission Assurance Program that will incorporate cyber security requirements into the procurement process.
SSE Initiative 88. Develop active cyber capabilities and employ them against potential adversaries in support of government-authorized military missions.
[3] The CDS Initiating Directive for Defensive Cyber Operations (DCO) is to be conducted by clear direction, prioritization and coordination of resources, and informed by accurate, timely and detailed intelligence. It must deliver a sustainable and continuous process that matches resources to the evolving cyber threat".
[4] Command and control warfare (C2W) is the integrated use of operations security (OPSEC), military deception, PSYOP, electronic warfare (EW), and physical destruction, mutually supported by intelligence to deny information to, influence, degrade, or destroy adversary command and control (C2) capabilities while protecting friendly C2 capabilities against such actions.
[5] A number of Canadian representatives co-authored the book
[6] Maskirovka: From Russia, With Deception by By COL JB Vowell Brookings Institution.

include establishing decoys in a theatre-of-operation, masking blue force operations, manipulative and imitative deception, cloaking and camouflage. The doctrinal leap from electronic deception to cyber deception has been made harder than it needs to be.

One would naturally expect the army, navy and air force camouflage platforms from detection across the electromagnetic (EM) spectrum - from visible light, to radio waves. [7] We don't paint army vehicles bright orange. So why do some paint vital cyber infrastructures so obviously? Why is there reluctance, in some quarters, to use deception as a defensive strategy?

All military campaigns require stealth and deception. Cyber is no difference.

Deception is particularly effective in the cyber domain but remains underexploited by defenders [including active defence]. The need for deception should be seen in the context of the nature of cyber conflict. Instead of comparing cyber conflict to warfare, with discrete missile attacks between physically separated physical entities, viewing it as a perpetual set of intimate knife fights between digital proxies.[8] Deception is perhaps more effective in cyberspace because physical use of force is not.

Deception operations are a very effective means of enabling defensive cyber operations and can also support intelligence collection and force protection. A deception operation within cyberspace is not inherently different from a real-world deception operation and similar policies and practices equally apply. Cyber deception can mis-inform, confuse, distract, and delay an adversary. It is also possible to gain intelligence about an adversary based on how they interact with a deliberate deception, which can be immensely useful in the case where a capable adversary is lured into disclosing tools or tactics that have not been previously observed. Actions can also be analyzed to discern the real-world intent and target of that adversary.

Cyber deception imposes additional costs on an adversary increasing the work factor and decreasing ROI. Deception limits their freedom-of-maneuver, undermines their ability to stay hidden and time on target. The loss of their anonymity and the exposure of their tradecraft and technology raise the risk for the attacker. Hence cyber deception and is an excellent deterrent.[9]

One difference between cyber and non-cyber deception is the shifting liability and information incentives that makes defending terrain with unknown vulnerabilities more challenging and the case for deception more compelling. Cyber deception can do much more than intelligence collection and force protection.

Deception activities include both proactive deliberate activities and *Respond-Deceive* actions that occur in response to a particular event or intent. These deception operations may be executed within enterprise networks, platforms and partner infrastructures.

[7] Cyber, by definition includes information and the EM spectrum.
[8] UK National Cyber Deception Lab
[9] CAF Concept of Operations for DCO

The UK National Cyber Deception Lab explains that the *"focus of defensive deception in the cyber domain is likely to shift towards deception that shapes an adversary's understanding of the situation, and thereby alters their behaviour, underlining the focus on deceiving the human adversary, rather than technological solutions."*

The stability and predictability of vulnerability management in an at-risk infrastructure is an ongoing consideration for cyber defence operations. Establishing upstream security with deception-in-depth around a large and potentially vulnerable attack surface has been shown to be an effective means of defence by proactively mis-directing attacks away from the enterprise.

The UK National Cyber Deception Lab recommends *"putting deception at the heart of a layered defence of core networks."*

The cost of a deception capability is substantively lower than the price imposed upon the adversary or the impact of a breach on one's own systems, without the early detection afforded by deception technology. This is particularly true for unstable attack surface and sophisticated attacker – where security management is most challenging. Moreover, deception activities often result in the exposure of the adversary's most-sensitive technology, Tactics, Techniques and Procedures (TTP).

CONCEALMENT AND MISDIRECTION

The Communication Security Establishment (CSE) has provided explicit cyber security guidance, in mandatory standards, to departments on the matter of cyber deception:[10]

The organization employs organization-defined concealment and misdirection techniques to confuse and mislead adversaries. Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber-attacks. For example, virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment/misdirection techniques including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment/misdirection techniques may also provide organizations additional time to successfully perform core missions and business functions.[11]

Similarly the UK National Cyber Deception Lab advises *"Network defenders should take a proactive approach by using military deception tradecraft to effectively defend against and manipulate the activities of attackers operating within their networks. Cyber deception offered a significant asymmetric advantage to the network defender, because they own the terrain and adversaries lack the defenders' situational awareness."*

[10] ITSG-33
[11] ITSG-33 Security Control SC-30

CYBER DECEPTION TECHNOLOGY

The efficacy of deception for defence in the cyber domain is well-established, with modern commercial services focused on detecting adversaries and collecting intelligence on their activities. Cyber deception for cyber security in three verticals: for detecting adversaries, eliciting intelligence and for adversary management.[12]

Deception technology is an established category of cyber security and defence. These systems can detect, analyze, and defend against zero-day and advanced attacks, often in real time. They are automated, highly accurate, and provide unique insight into malicious activity of sophisticated actors, where conventional defence systems fail. Deception technology enables a more proactive security posture by seeking to deceive, detect and defeat threat actors before they can attack.

"The greater the presence of deceptive assets in the network, the more likely it is that an adversary will fall into the trap." - UK National Cyber Deception Lab

Conventional cyber defence technologies and methods have proven to be ineffective against zero-day exploits and advanced persistent threats. We need better options.

Deception technology is orientated around the adversary's point-of-view and tradecraft. It integrates with existing technologies to provide new visibility, share anticipatory threat intelligence while potentially generating effects against an adversary.

Deception technology may automate the creation of traps, decoys or lures either hidden within existing infrastructure or an entire network can be established as a decoy. Obfuscation of intent, anonymization of communications, ghosting operations, false flag, strategic cloaking of infrastructure while establishing decoy networks, laying tripwires and means of surveillance are just some means of actively defending using cyber deception and misdirection.

Advances in automation may lead to wider use of defensive deception platforms for detection and collection. Automation has the potential to reduce the resource cost of creating and monitoring defensive deceptions, although it is very likely that the most sophisticated deceptions will remain resource-intensive, human-centric operations.[13]

The conventional use of cyber deception technology is the traditional honeypot style bait. However, the potential is to manipulate the attacker's confidence in what is going on, getting them to make error in their understanding of what is occurring and then get them to act on this erroneous understanding. If one puts a burglar alarm on the side of their house, one needs the attacker to see it for it to have a deterrent effect. Likewise, if they now know that there are defensive measures being deployed, the attacker will be expecting them in the future, and this can be used to get them to pause, question or doubt.

[12] UK National Cyber Deception Lab
[13] UK National Cyber Deception Lab

Cyber deception is industry standard.

MARKET SIZE AND ADOPTION

Market Research Media estimates the cumulative deception technology market value at $12 billion (2017–2022) growing at about 19% CAGR. Adoption is being accelerated by aggressive and highly-visible targeted attacks on large enterprises globally by advanced persistent threats. Notwithstanding, only 10 percent of enterprises and 2 percent of government organizations use cyber deception, even through it has been established as best practices for cyber defence and instantiated in official policy and standards. Gartner also noted deception technology as a "*far under-utilized technology that can provide serious advantages over attackers*."

CYBER DECEPTION SOLUTIONS

The following are examples of successful cyber deception solutions in wide use and acceptance:

- Content Delivery Networks (CDN) – Distribute the information flows over multiple geographically and logically dispersed servers, thus making it very difficult to enumerate the infrastructure or interfere with data flows.
- Virtualization and Cloud – Global hyper-cloud instantiations of an infrastructure or operations are highly-robust and agile. Architecture and processes can be replicated, dispersed and rapidly fluxed across data centres around the globe making it very easy to establish decoy networks while hiding real ones. CSE recommends virtualization and cloud as security control SC-29 in ITSG-33.
- Anonymizers – A variety of public anonymization services and purpose built managed (non) attribution Infrastructures as a Service (IaaS) are available commercially which allow one to hide one’s Internet activity or cloak an entire organization. Services like TOR, which provide ofscuscating VPN network for the masses, was originally established by intelligence services, but has provided safe haven for criminals as well as sanctuary for human rights. Many deception technologies are dual use.
- Organizational cloaking – while similar to anoymizers, will hide the existence of an entire organisation or operation while often presenting a decoy addressable infrastructure. The cloaked instance forms part of the deep web and can be covert or clandestine in operation. Stealth is a form of deception.
- Moving Target Defence (MTD) – Rapidly changing organizational infrastructure, using virtualized and cloud environments, can make it very difficult for an adversary to find and target the enterprise of operations. Domains and IPs can be fast-fluxed across global points-of-presence, components and process flows, operating systems and system configurations orchestrated to change over time or in response to threat activity.
- Dark Space – Unassigned IP addresses for an organization are re-routed to a security monitoring network. There is no legitimate traffic expected on these IPs, therefore when an actor (or infected machine) scans, probes or attacks these IPs, they are detected. Often a passive honey net or malware lab will be on the end of these IPs. This has been proven to be

exceptionally effective in catching APTs and reverse engineering zero-day malware. See *APT0 - Study on the Analysis of Dark Space for Predictive Indicators of Cyber Threat Activity*, for a comprehensive example of dark space use in cyber threat intelligence and defence.[14]

- Honeypots - were the first basic form of deception. A honeypot is set up as a decoy to attract adversaries and to deflect their attacks away from the operational systems supporting organizational missions/business function. The notion of honeypots deceiving attackers, perhaps delaying and identifying them, and then ultimately supporting efforts to shut down the attack was a good one.[15] This is a recommended secure control by CSE.[16] The UK National Cyber Deception Lab lists some benefits of having honeypot:

    - Observe threat actors in action and learn about their behaviour
    - Gather intelligence on attack vectors, malware, and exploits. Use that intel to train your IT staff
    - Create profiles of attackers that are trying to gain access to your systems
    - Improve your security posture
    - Waste attackers' time and resources
    - Reduced false positive
    - Cost-effective
    - Introduces a cognitive payload on the attacker
- Honeynet - is a network that is set up to attract potential attackers and distract them from your production network. The gap between legacy honeypots and modern deception technology has diminished over time and will continue to do so. Modern honeypots constitute the low end of the deception technology space today.
    - The Honeynet Project is an international security research organization established in 1999, "dedicated to investigating the latest attacks, developing open source security tools to improve Internet security and learning how attackers operate". The Canadian Honeynet chapter was founded at the University of New Brunswick, Canadian institute for cyber security in April 2008. Note: Telecommunications Carriers and Internet Service Providers (ISP) have run Honey Nets since the 1980s. The public sector has experimented with honey pots and is certainly a recipient of cyber threat intelligence harvested from globally deployed honey nets. Defensive External Interdiction (DEI)[17] relies on commercial deception mechanisms and practices.

    - DND/CAF[18] has sponsored several research projects using forward-deployed honey nets to collect valuable intelligence on adversaries and advanced persistent threats over the past

[14] http://publications.gc.ca/collections/collection_2016/rddc-drdc/D68-3-007-2013-eng.pdf
[15] Wikipedia
[16] ITSG-33 Security Control SC-26
[17] Defensive External Interdiction (DEI) is a category of action that can be requested by the government of a commercial or foreign state third party where that third party takes an action that has defensive value for the government. DEI can be a significant operational enabler for any static or deployed system. It provides a range of possible actions for the DCO planner that cost only the time it takes to reach out to third parties, develop relationships, or add statements into contracts. Actions taken by a third-party leverage that third-party's position within the global telecommunications environment or their national authorities that have the legal ability to block, alter, slow, or redirect elements of malicious communications destined for the government. Cyber threat intelligence services use forward deployed deception networks.

[18] DG Cyber, CFIOG and DRDC

ten-years. Certainly, the GC and DND remain a direct benefactor of globally deployed honeynets, through commercial Cyber Threat Intelligence (CTI) subscriptions.

- Tar pits - is a service on computer systems that purposely delays connectivity and processes. The technique was developed as a defense against a computer worm, and the idea is that network abuses such as spamming or broad scanning are less effective, and therefore less attractive. The method forces adversaries to spend more time and resources, cope with greater levels of complexity and uncertainty, and accept greater risks of exposure and detection.[19]
- Randomness – CSE describes how, "randomness introduces increased levels of uncertainty for adversaries regarding the actions organizations take in defending against cyber-attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations supporting critical missions/business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques involving randomness include, for example, performing certain routine actions at different times of day, employing different information technologies (e.g., operating systems, browsers, search engines), using different suppliers, and rotating roles and responsibilities of organizational personnel."[20]
- Change processing / Storage locations – Information Technology Security Guidance provided to the government departments explain that "adversaries target critical organizational missions/business functions and the information resources supporting those missions and functions while at the same time, trying to minimize exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational information systems targeted by adversaries, make such systems more susceptible to cyber-attacks with less adversary cost and effort to be successful. Changing organizational processing and storage locations (sometimes referred to as moving target defence) addresses the advanced persistent threat (APT) using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the information resources (i.e., processing and/or storage) supporting critical missions and business functions. Changing locations of processing activities and/or storage sites introduces uncertainty into the targeting activities by adversaries. This uncertainty increases the work factor of adversaries making compromises or breaches to organizational information systems much more difficult and time-consuming, and increases the chances that adversaries may inadvertently disclose aspects of tradecraft while attempting to locate critical organizational resources."
- Misleading Information – CSE notes that "control enhancement misleads potential adversaries regarding the nature and extent of security safeguards deployed by organizations. As a result, adversaries may employ incorrect (and as a result ineffective) attack techniques. One way of misleading adversaries is for organizations to place misleading information regarding the specific security controls deployed in external information systems that are known to be accessed or targeted by adversaries. Another technique is the use of deception nets (e.g., honeynets, virtualized environments) that mimic actual aspects of organizational information systems but use, for example, out-of-date software configurations."[21]

[19] UK National Cyber Deception Lab
[20] ITSG33
[21] ITSG 33

- Feed material – is real information of lesser value to an organization that is presented to a threat actor as bait to legitimize the deception.
- False flag a threat - a range of areas for the creative deployment of deception to manipulate an attacker's behaviour, such as false flagging the presence of more aggressive attackers already in the network to 'scare off' real attackers - UK National Cyber Deception Lab
- Concealment of system components - By hiding, disguising, or otherwise concealing critical information system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means for organizations to hide and/or conceal information system components include, for example, configuration of routers or the use of honeynets or virtualization techniques.[22]
- Honeyclients – as specified in ITSG-33 Security Control (SC-35) as "the information system includes components that proactively seek to identify malicious websites and/or web-based malicious code. Honeyclients differ from honeypots in that the components actively probe the Internet in search of malicious code (e.g., worms) contained on external websites."
- Black Holing - n networking, a black hole refers to a place in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient. When examining the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic; hence the name.
- Sink holing - A DNS sinkhole, also known as a sinkhole server, Internet sinkhole or Blackhole DNS is a DNS server that is configured to redirect a domain previously used by a bad actor into a monitored security environment in order to enumerate threat command and control infrastructure, study behaviour and protect victims by severing C2 link with vulnerable machines. A common use of a hosts file-based sinkhole is to block ad serving sites.

    - Microsoft took a series of dramatic steps against the recent SolarWinds supply chain attack using sinkholes and other active defence measures. Microsoft's technical and legal actions were broad in speed and scale and effectively obliterates the actions the sophisticated offensive actors attributed to APT29 (Cozy Bear) of the Russian intelligence service, known for the 2016 hack against the Democratic National Committee (DNC). [23]
- Conflict networks – are special honey nets deployed forward in contested environments or adversary space. They can also be real but highly-targeted networks which are heavily monitored and serve a dual purpose as threat intelligence collectors by overwatch programs.
- Circumvention Network – is an infrastructure designed to penetrate national censorship / state firewalls of denied environments. They in themselves become highly targeted by these regimes and then become a means to collecting intelligence on the adversary.
- Counter Censorship – are counter-surveillance systems which in attempting to openly communicate in and out of denied environments are able to reveal state surveillance programs, technology, tradecraft and targeting

[22] ITSG 33

[23] Microsoft unleashes 'Death Star' on SolarWinds hackers in extraordinary response to breach by Christopher Budd on December 16, 2020

- Packer staining – inserts markers within packets to trace the path of communications and identify infrastructure of threat actors. Useful for attribution and traffic management through reputational rating.
- PDNS – *protective* recursive resolver like Canadian Shield[24]. This is a policy-enabled recursive resolver. This means that it performs the functions of a recursive server in looking-up and storing the DNS information - also known as a map of the Internet. Any communicates with a bad domain or IP will be blocked or be rerouted to the correct domain. The incident can be an indication of compromise or phishing attempt.
- Flowspec BGP – Use remote Trigger Blackhole (RTBH) to mitigate DDOS attacks. The actor may not be aware that their DDoS attack has been mitigated.
- Triggered content – Specific content (perhaps a file) is programmed to alarm is anyone tries to access it.
- Beaconing detection – A file or information or media is lowjacked such that it can be tracked as an adversary exfiltrates a copy from the network. Allows security teams to trace the theft back to the actor's computer thus revealing adversary infrastructures, methods and identities.
- Cyber threat intelligence - is analytical product based upon information about threats and actors used for active defence. Cyber threat intelligence sources include open source intelligence, social media intelligence, human Intelligence, technical intelligence or intelligence derived from the deep and dark web. CTI makes extensive use of all the deception technologies and methods mentioned here. It can be:
  - Tactical: technical intelligence (including Indicators of Compromise such as IP addresses, file names, or hashes), which can be used to assist in the identification of threat actors.
  - Operational: details of the capabilities of threat actors, including their Tactics, Techniques, Procedures (TTP)
  - Strategic: anticipatory intelligence covering greater scope of threat motivation, intent and capabilities of a threat.
- Deception technology when integrated with threat hunting, memory and malware analysis can provide dynamic automated attribution of actors and analysis of malware. The process may also identify indicators of compromise (IOC).

The emergence of disruptive technologies such as Fifth Generation Mobile Communications, Cloud, Quantum Computing and Artificial Intelligence will expand the capability and need for cyber deception. Deception technology is a proactive layer to a defence-in-depth strategy.

EXAMPLES

The following are examples of the effective use of active defence using deception to: detect, identify, attribute and counter advanced persistent threats against Canada:

[24] First conceived of by Bell Canada and implemented at CIRA.

- The research project *Analysis of Dark Space for Predictive Indicators of Cyber Threat Activity* – by Bell Canada and SecDev for DND, CSE, RCMP, PSC, DFAIT (31 Mar 2011) used forward deployed and carrier based deception networks to successfully detect and attribute advanced persistent threats attacking Canada's. Dark net technology was used extensively to provide early warnings and indicators or zero-day exploits and sophisticated threats, which were able to bypass conventional systems. The project was the first to identify APT0 (Chinese) infiltration of government systems. http://publications.gc.ca/collections/collection_2016/rddc-drdc/D68-3-007-2013-eng.pdf
- The project *Combating Robot Networks and their Controllers* by Bell Canada and Secdev for RCMP and DND investigated and tested the most effective means of detecting advanced threats such as botnets operated by organised criminal groups and nation states. Deception networks and methods were found to have the greatest efficacy. The report included an extensive legal discussion on methods used. PSTP08-0107eSec 06 May 2010 (PSTP) https://www.scribd.com/document/51938416/Botnet-Analysis-Report-Final-Unclassified-v2-0
- GhostNet was a large-scale cyber spying operation discovered in March 2009 through the use of forward deployed networks in contested environment and deception technologies. http://www.nartv.org/mirror/ghostnet.pdf
- Shadows in the Cloud uncovered a complex ecosystem of cyber espionage that systematically targeted and compromised computer systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries, by monitoring highly targeted domains. http://www.nartv.org/mirror/shadows-in-the-cloud.pdf
- Attack Surface Analysis of the Department of National Defence, was completed Bell Canada, Trend Micro and SecDev for (DG Cyber) CAF in 2012. The investigation effectively correlated threat data from forward deployed sensors honeypots and deception networks with global cyber threat intelligence, Advanced OSINT/SOCMINT, DNS analytics, carrier level netflow and security monitoring of internal networks,
- APT1 Exposing One of China's Cyber Espionage Units by Mandiant, 2004 https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
- Operation Aurora - a series of cyber attacks conducted by advanced persistent threats such as the Elderwood Group based in Beijing, China, with ties to the People's Liberation Army. https://en.wikipedia.org/wiki/Operation_Aurora
- Cyber State of Readiness in Canada's Critical Infrastructures Study 0D160-063075/A, by Bell Canada and the RAND Corporation for PSC dated 2006-04-28
- Attribution and Fingerprinting of Advanced Persistent Threats 2015 by Bell Canada for RCMP under PSTP used advanced cyber deception methods.
- McAfee, Night Dragon investigation http://www.mcafee.com/ca/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
- Cyber Attribution of Sophisticated Threat Actors in the Defence of Canada 2019-2021 The Department of National Defence (DND) contracted multiple projects with industry through the IDEaS program to *develop and test innovative approaches to access, interpret, and compare* *all* *available evidence (e.g. technical, all-source intelligence) on how current cyberspace*

activities get attributed. Note: Deception is a key component of cyber intelligence, threat hunting, adversary pursuit and persistent engagement.

OFFENSIVE CYBER DECEPTION

Deceive, Detect, Disrupt and Deter

Canada’s adversaries are adept at offensive cyber deception. We see daily evidence of cyber psychological operations, misinformation, influence and social engineering campaigns against Canadian’s and institutions by foreign intelligence services and militaries. Principally amongst these tactics is social engineering.

Social engineering uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Deception relies heavily on the six principles of influence: reciprocity, commitment and consistency, social proof, authority, liking, scarcity.

All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases, These biases, sometimes called "bugs in the human wetware,” are exploited in various combinations. Phishing tactic has proven to be most effective.

Phishing is one of the most common means of offensive cyber deception. Phishing is the fraudulent attempt to obtain sensitive information, by impersonating a trustworthy entity in a digital communication. Typically the attacker uses a well-crafted e-mail appearing to be sent from a trusted contact, but which contains hidden malware. Nearly all, technical cyber attacks are facilitated through deception in the form of social engineering and phishing in particular.

Phishing is the predominate attack vector for introducing highjacking malware past traditional security systems and circumventing even high-grade crypto-systems. Vishing (via telephone) and Smishing (via SMS) are also used.

Mobile devices are particularly susceptible. In a SIM swap scam (also known as port-out scam, SIM splitting, Smishing and simjacking, or SIM swapping) the attacker uses social engineering to convince the telephone company to port the victim's phone number to the fraudster's SIM. This allows the attacker to intercept any one-time passwords sent via text or telephone calls sent to the victim and thus allows them to circumvent many two-factor authentication methods. Note: exploiting SS7 vulnerabilities and technical deception of the telecommunications provider will achieve much the same result.

Other means of deception can take the form of:

- Trojan horse software or electronic communication can contain a hidden payload just - like the wooden horse from the Trojan war used by the Greeks to enter the city of a Troy and win the war.

- Spoofing an e-mail, domain, IP addresses, phone numbers, URL, or Address Resolution Protocol (ARP) can make the deception more convincing.
- Luring unexpecting victims to a fake web site then triggering the hidden download of a Remote Access Trojan (RAT). Facilitating a man-in-the-middle or man-on-the-side attacks.
- Using click-bate of a trending story, especially in the time of a global pandemic to entice a user to follow a poison link to malware.
- Poisoning of domain name servers to redirect and misdirect traffic to a malicious site.
- Mounting a false flag operation in cyberspace, perhaps to mis-attribute hostile actions, or trap someone into trusting the wrong sort of people.
- Impersonation and fraud of central to most hostile deception operations.
- Meaconing navigational signals such as GPS to lead ships and aircraft off-course to run them aground.
- Deliberate disruption, interference or jamming of a communications signal to force users into the clear (non-encrypted means) or over a more vulnerable route. This is a common attack to force mobile devices to drop down to less secure protocols or deny high-grade systems.

Adversaries have routinely used social engineering to obtain personal data, hijack accounts, steal identities, initiate illegitimate payments etc of Canadians at scale. As technology becomes more complex, criminals will seen the path of least resistance and seek to compromise the individual through manipulative and imitative deception. Social media pretexting will remain a primary attack vector.

LAW, ETHICS AND RISK

In this section we examine prohibition and prescription for cyber defence in the Canadian context[25] and international cyber norms.

It is worth noting that, Cyber deception and authorities are similar to the manner in which law-enforcement uses bait cars to catch thieves or on-line profiles to catch child predators.

An organization is authorized to effectively and actively defend its own networks and systems from adversaries. There are five considerations that we will examine:

1. There are statutory/regulatory authorizations for an organization to conduct all forms of cyber defence operations;

2. There are no statutory restrictions/prohibitions/court rulings that prohibit or restrict an organization from actively defending its networks;

[25] The hierarchy of direction starts with the Canadian Charter of Rights and Freedoms, followed by Legislation, Regulations, Crown prerogative for defence, Treaties, Judicial interpretation binding to the party and persuasive to other parties, Government Policy, Security Guidance Procedures and Standards. For the military the Queens Regulations and Orders, Chief of Defence Staff orders and Use-of-Force Directives, and Operational Guidance or Directives pursuant to authoritative bodies apply.

3. There are explicit procedures/authorizations which compel an organization to take conduct active cyber defence;

4. There are relevant international agreements which permit and obligate the department to protect and defence not only its own networks but critical information infrastructures of Canada;[26] and

5. There are policy/legislative changes that need to be made to achieve the desired outcomes.

Under Canadian law, all cyber defence actions are permitted unless explicitly forbidden. Restrictions of activities, like the intercept of private communications, are clearly specified in the Criminal Code of Canada while obligations to defence information systems are identified in Privacy legislation and Regulations for industry or the Financial Administration Act and policy promulgated from TBS and CSE for government.

The Financial Administration Act (FAA), Criminal Code of Canada (CC) and The National Defence Act and Telecommunications Act and Privacy Legislation all allow for an employee acting in an official capacity, to take reasonable measures to protect computer systems, including the interception of private communications. Furthermore, this legislation, government IT Security policy released by Treasury Board Secretariat (TBS) and official Guidance by the Governments Lead Security Agency (CSE) compel system owners in departments to defend computer systems.

> Financial Administration Act: *Management or protection of computer systems Gestion et protection des ordinateurs 161 (1) The appropriate Minister, any public servant employed in a department, any employee of a Crown corporation or any person acting on behalf of a department or Crown corporation who performs duties relating to the management or protection of computer systems of the department or the Crown corporation may take reasonable measures for such purposes, including the interception of private communications in circumstances specified in paragraph 184(2)(e) of the Criminal Code.*

Note: Deception networks such as honeypots constitute part of the organization network and are protected under law.

Canadian Government Information Technology Security Policy, states "*departments must adopt an active defence*[27] *strategy. Department must continuously monitor threats and vulnerabilities, and where required, take proactive*[28] *countermeasures.*"

[26] NATO Charter Article 3, Tallinn Manual on the International Law Applicable to Cyber Warfare, ITU et.al.

[27] Active Cyber Operations as defined in the CSE Act as "activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security."

[28] Proactive cyber defence is defined as Proactive cyber defence means acting in anticipation to oppose an attack through cyber and cognitive domains. It represents the thermocline between purely offensive and defensive action; interdicting, disrupting or deterring an attack or a threat's preparation to attack, either pre-emptively or in self-defence. Common methods include cyber deception, attribution, threat hunting and adversarial pursuit. The mission of the pre-emptive proactive operations is to conduct aggressive interdiction and disruption activities against an adversary using: Psychological operations, Managed Information Dissemination, Precision Targeting, Information Warfare Operations and computer network exploitation and other active threat reduction measures. The proactive defense strategy is meant to improves information

The Federal Government Information Technology Security Guidance (ITSG-33), which all departments are required to follow, requires concealment and misdirection (Cyber deception) for sensitive networks and specifies a number of security controls including specifying the use of honeynets, honeypots, honeyclients, randomness, change processing / storage locations, misleading information, concealment of system components. The standard further states that:

Attribution is a critical component of a security concept of operations. The ability to detect source and destination points for information flowing in information systems allows for forensic reconstruction of events when required an encourages policy compliance.

Precedence has been established by the federal court [29] and upheld by the Supreme Court of Canada for organizations to use cyber deception technology and methods to manage their networks or to collect intelligence.

In 1995, the Information Technology Security Working Group[30] published *A Survey of Legal Issues Relating to Security of Electronic Information*. The group considered a comprehensive spectrum of cyber security issues that are equally relevant today. Federal government legal teams affirmed the need to secure information systems to best practices, which include deploying surveillance and deception systems.

The following are principal observations and findings with respect to legal use of active cyber deception in the Canadian context:

1. Cyber Deception Technologies have been operating for half-a-century without court challenges.

2. There is no express prohibition on cyber deception, or active cyber defence including attribution, threat hunting or adversary pursuit domestically or internationally. Neither is there exclusivity to any parties or agencies.

3. A department not only has the authority to conduct cyber deception, threat hunting, attribution, forensics and active cyber defence to protect their networks and assure the mission, they are

collection by stimulating reactions of the threat agents, provide strike options and to enhance operational preparation of the real or virtual battlespace. A measure for detecting or obtaining information as to a cyber attack, or impending cyber operation or for determining the origin of an operation that involves launching a pre-emptive, preventive, or cyber counter-operation against the source. Proactive cyber defence operations pre-emptively engage the adversary. The offensive capacity includes the manipulation or disruption of networks and systems with the purpose of limiting or eliminating the adversary's operational capability. This capability can be required to guarantee one's freedom of action in the cyber domain. Cyber-attacks can be launched to repel an attack (active defence) or to support the operational action. Proactive cyber defence differs from active defence in that it is pre-emptive (not waiting for an attack to occur). The distinction between active cyber defence and offensive cyber operations (OCO) is that the later requires legislative exceptions or executive prerogative to undertake. Hence, offensive cyber capabilities may be developed in collaboration with industry, or facilitated by private sector but operations are often led by nation states. There are some exceptions, notably in self-defence or with judicial authority (civil warrants) or assisting law enforcement. https://en.wikipedia.org/wiki/Proactive_cyber_defence

[29] Ministerial authorizations

[30] The signatories on the group consisted of the legal representatives and chief security officers from CSIS, CSE, DND, CSS, DFAIT, HC, IC, PWGSC, RC, RCMP, TBS, PCO, DoJ

explicit obligated to do so in official security guidance.

INTERNATIONAL LAW

The Tallinn Manual International Law Cyber Warfare outlines cyber deception in Rule 61 – Ruses. Ruses of war are acts intended to mislead the enemy or to induce enemy forces to act recklessly, but do not violate the law of armed conflict. They are not perfidious because they do not invite the confidence of the enemy with respect to protected status. Cyber operations that qualify as ruses of war, are permitted in time of peace and war. The following are permitted:

- Creation of a dummy or decoy computer systems simulating non-existent forces
- Transmission of false information causing an opponent to believe operations are about to occur or underway
- Use of false computer identifiers, computer networks (eh., honeynets or honeypots), or computer transmissions
- Feigned cyber attacks
- Bogus orders purported to be issued by the enemy commander (or friendly forces)
- Psychological warfare activities
- Transmitting false intelligence information intended for interception; and
- Use of enemy code, signals and passwords
- Military cyber operations may blend into civilian infrastructure [ie., managed (non) attribution networks]
- There is a “Do no harm" principle in using deceptive technique outside of warfare with respect to civilian populations

CAF AUTHORITIES, RESPONSIBILITIES, ACCOUNTABILITY AND OBLIGATIONS

The CAF cyber defence operational concept and campaign plan envision being capable of defending the CAF’s freedom of action and interests in cyberspace, and delivering military effects in and through a contested cyber environment in support of CAF missions and those regions of the global cyberspace used by Canada’s allies and partners. Intelligence is recognised as an essential component to DCO, CMA, DCO-RA and ACO. Cyber deception[31], threat hunting and attribution are fundamental to cyber intelligence production.

The Department of National Defence (DND) and the Canadian Armed Forces (CAF) have all the necessary legislative, judicial and executive authorities to unilaterally[32] carry out defensive cyber operations (DCO), active cyber operations (ACO) and offensive cyber operations (OCO). In fact, they are also obligated to do so by policy and law in the defence of Canada.

The Financial Administration Act (FAA), the Government Security Policy (GSP), Treasury Board Secretariat (TBS) Management of Information Technology Security (MITS), and Information

[31] A cyber dominance and deception concept is to be completed by 2022.
[32] The CSE Act, does not give CSE exclusivity for DCO or ADO. Any individual or organization may conduct ACO provided they do not contravene the Charter or Criminal Code, or have an exception.

Technology Security Guidelines ITSG-33 compel DND/CAF to actively defend networks using cyber deception, to gather intelligence and to attribute and counter threat actors.

The Criminal Code of Canada (CCC) and Privacy Act (PA) provide necessary exemptions for DND/CAF to conduct including deception, as do International Telecommunications Law and the Law of Armed Conflict (LOAC).

The National Defence Act (NDA) provides legislative authority to conduct military operations across all domains and prescribes intelligence and ACO/OCO. Ministerial Authority and Directives provide further explicit authorities for ACO/OCO under executive prerogative with the requirement to report to the minster annually.

Canada's National Defence Policy, *Strong, Secure, Engaged*, recognizes that cyberspace is essential for the conduct of modern military operations. It also acknowledges that a purely defensive cyber posture is no longer sufficient and must be accompanied by active and offensive cyber operations, a capability that Canada commits to develop and employ against potential adversaries. Subsequent executive direction has been given in Defence Policy to perform active defence in the defence of Canada. Specific initiatives specified in defence policy which are directly benefited from cyber deception and intelligence are:

- SSE Initiative 65. Information operations capabilities and cyber capabilities, situational awareness, cyber threat identification and response, and the development of military-specific information operations and offensive cyber operations capabilities able to target, exploit, influence and attack in support of military operations.

- SSE Initiative 87. Protect critical military networks and equipment from cyber-attack by establishing a new Cyber Mission Assurance Program that will incorporate cyber security requirements into the procurement process.

- SSE Initiative 88. Develop active cyber capabilities and employ them against potential adversaries in support of government-authorized military missions.

The defence policy also has stated the objective to build Canadian Forces Intelligence Command's (CFINTCOM's) capacity and infrastructure to provide more advanced intelligence support to operations, including through an enhanced ability to forecast flashpoints and emerging threats, better support next generation platforms and understand rapid developments in cyber. Attribution and deception are most often mentioned by policy in context with the intelligence mandate.

HIGHER INTENT

"But deterrence is more than presence and a show of force. It has to be credible, and it has to be grounded in strong offensive capabilities that would be capable of denying an adversary the ability to achieve success through their own offensive actions, before they have been taken. Deterrence is also

owned by more than just the military. It requires a coordinated approach from all sources of national power and Allies, and must be applied in a coordinated manner throughout all domains to achieve the effect.” – Chief of Defence Staff

OVERSIGHT AND REVIEW

DND mandate to unilaterally conduct active cyber defence and offensive cyber operations,which necessaility includes cyber deception, is recognized by intelligence review and oversight bodies (OCSEC, SIRC, and NSIRA).

SOCIAL CONTRACT AND OBLIGATIONS

The military is mandated to conduct the full-spectrum military operations including the use of lethal force across all domains, of which cyber is recognized to be one. The state, as the national guarantor of Peace, Order and Good Government (POGG) is expected and obligated to defence Canada from cyber attacks.[33]

RESIDUAL RISK

The common straw-man argument against deception technologies is to raise the remote possibility that a deception technology (like a honeypot) could be compromised and be used as a launching platform to attack third parties.

Firstly, the argument is not unique to a deception network. The 3rd party liability argument applies to all networks, computers or mobile devices[34]. The difference is that deception networks are much more carefully monitored and controlled than your average network. For example, many deception nets are engineered to throttle outbound traffic and prevent attacks. Secondly, they are designed to catch threat activity early, and hence are far more vigilant and secure than a conventional network. Thirdly, there are no established trust relationships or shared credentials between a deception net and regular users, thus preventing an attacker from moving laterally. Fourthly, deception systems do not handle Sensitive information, Personal Identifiable Information (PII) or Private Communications and have low false positive rate (demonstrating that only threat actors attempt to communicate with the system) hence that are no security or privacy concerns. Finally, cyber deception also does not constitute fraud or entrapment under any legal interpretation. Research has not found case law or civil liability involving cyber deception.

There is negligible legal risk associated with the use of deception technologies, but there is liability to public and private organizations not actively defending their networks. An organization is highly-exposed to both compromise and liability should they not comply with best practices or standards,

[33] Failure to defend Canadians has legal implications (eg.,Mandamus Prerogative Writ) which will see Industry and civil society taking a lead role in ACD.
[34] Note: It is common for attacks on Canadians to be launched from compromised government systems. Yet there has never been a civil or criminal liability case against the Crown.

which shall include cyber deception.

Re-shaping people's risk perception is important, so that they are willing to explore the art-of-the-possible with cyber deception solutions.

CONCLUSION

We have established that there is no prohibition on the use of cyber deception activities. To the contrary, it can be successful argued that cyber deception controls are mandatory given that they are well established as best practices and explicitly written into standards. They also make good business sense because cyber deception lowers threat risk and liability, while offering the best Return-on-Investment (ROI) for cyber defence. Moreover, cyber deception and intelligence are found to be very closely coupled.

REFERENCES

1. Strong, Secure, Engaged, Canada's Defence Policy, June 2017
2. Cyber Ops FD Campaign Plan 2020-2035, 09 Dec 20
3. CAF Concept Defensive Cyber Ops 14 Jan 2020
4. UK Cyber Deception Lab
5. Cyber Defence Futures, DG Cyber, 08 Oct 2019
6. Future Security Environment, DG Cyber, 28 Mar 2018
7. 2018 Security Outlook Potential Risks and Threats Canadian Security Intelligence Service
8. Annual report to congress Military and Security Developments Involving the People's Republic of China
9. APT0 Study on the Analysis of Darknet Space for Predictive Indicators of Cyber Threat Activity –Communication Security Establishment, Bell Canada and SecDev Cyber Corp, 31 Mar 2011 http://publications.gc.ca/collections/collection_2016/rddc-drdc/D68-3-007-2013-eng.pdf
10. APT1 Exposing One of China's Cyber Espionage Units, Mandiant, 2004 https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
11. Army 2040 The global security environment: emerging trends and potential challenges Prepared for the Annual Meeting of the Canadian Political Science Association, Carleton University Ottawa, Canada 27 May 2009 Peter J. Gizewski
12. Aurora, https://en.wikipedia.org/wiki/Operation_Aurora
13. Bell Canada, Capstone-Janissary Forensic Investigation of systemic cyber infiltration of Canadian's critical infrastructures by criminal and state sponsored actors.
14. Bell Canada, Combating Robot Networks and Their Controllers: PSTP08-0107eSec 06 May 2010 (PSTP) https://www.scribd.com/document/51938416/Botnet-Analysis-Report-Final-Unclassified-v2-0
15. Bell Canada, RAND Corp, Cyber State of Readiness in Canada's Critical Infrastructures Study 0D160-063075/A, Public Safety Canada, Bell Canada and the RAND Corporation dated 2006-04-28

16. Bell Canada, RCMP, Attribution and Fingerprinting of Advanced Persistent Threats 2015
17. Bell Canada, SecDev, Communication Security Establishment, DRDC, APT0 Study on the Analysis of Darknet Space for Predictive Indicators of Cyber Threat Activity – A comprehensive report on advanced cyber security tradecraft and issues affecting Canada, 31 Mar 2011 http://publications.gc.ca/collections/collection_2016/rddc-drdc/D68-3-007-2013-eng.pdf
18. Best Practices in Computer Network Defense: Incident Detection and Response http://www.iospress.nl/book/best-practices-in-computer-network-defense-incident-detection-and-response/
19. CSE ITSG-33
20. CCCS - National Cyber Threat Assessment 2018 - Communications Security Establishment (CSE), the Canadian Centre for Cyber Security (Cyber Centre)
21. Clairvoyance Cyber Corp, Cyber Forechecking, Frontline magazine, 2017
22. Clairvoyance Cyber Corp, Information Warfare 2.0, Cyber 2017 https://www.linkedin.com/pulse/information-warfare-20-dave-mcmahon/
23. Collings, Deirdre., Rohozinski, Rafal. Bullets and Blogs. New media and the warfighter - An analytical synthesis and workshop report
24. Combating Robot Networks and Their Controllers: PSTP08-0107eSec 06 May 2010 (PSTP) https://www.scribd.com/document/51938416/Botnet-Analysis-Report-Final-Unclassified-v2-0
25. Consolidated Industry response to Public Safety Canada's: Working Towards a National strategy and Action Plan for Critical Infrastructure, 2008
26. Cyber Critical Infrastructure Interdependencies Study 0D160-063075/A, Public Safety Canada, Bell Canada and the RAND Corporation dated 2006-04-28
27. Garigue, Robert, Canadian Forces Information Warfare- Developing a Conceptual Framework 1994
28. GhostNet http://www.nartv.org/mirror/ghostnet.pdf
29. McAfee, Night Dragon investigation http://www.mcafee.com/ca/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
30. McMahon, Dave, IPK and Cyberterrorism3.0 2015 Understanding Wetware Attacks And Countermeasures To The Hacking Of Belief Systems.
31. McMahon, Dave, Think Big on SecDev Cyber Corp 2014 https://new.Secdev.com/wp-content/uploads/2014/05/Think-Big-on-Cyber.pdf
32. McMahon, David, Cyber Threat: Internet Security for Home and Business, Hardcover – Oct 1 2000
33. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare 2013
34. NATO, Best Practices in Computer Network Defense: Incident Detection and Response http://www.iospress.nl/book/best-practices-in-computer-network-defense-incident-detection-and-response/
35. Night Dragon investigation http://www.mcafee.com/ca/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
36. Omand, Sir David, Jamie Bartlett & Carl Miller, "Introducing Social Media Intelligence (SOCMINT)" published: 28 Sep 2012.

37. Overview of the Future Security Environment, RAND Corp
38. SecDev, “GhostNet” was a large-scale cyber spying operation discovered in March 2009 http://www.nartv.org/mirror/ghostnet.pdf
39. SecDev, “Shadows in the Cloud”. A complex ecosystem of cyber espionage that systematically targeted and compromised computer systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries. http://www.nartv.org/mirror/shadows-in-the-cloud.pdf
40. Stuxnet and the Future of Cyber War DRDC deep in-field investigation supported by technical and open source network intelligence
41. The DCDC Global Strategic Trends 2007-2023
42. The Future Security Environment 2013-2040 Chief of Force Development
43. Treasury board of Canada, Canadian National Proactive Cyber