THE CANADIAN CYBER SECURITY SITUATION IN 2011

The latest joint research[1] delivers powerful investigative findings[2], views to advanced tradecraft, a blue-print for the next-generation secure networking[3] and the impetus for a national 'clean pipe' strategy[4], effective immediately.

> *"Canada's critical infrastructure consists of the physical and information technology (IT) facilities, networks, services, and assets essential to the health, safety, security, or economic well-being of Canadians, and the effective functioning of government. The real value is that of the transportation and transformation of information. Cyber-attacks have already had measurable adverse economic effects for Canada, totalling in the billions of dollars. The risks to critical infrastructure and <u>info</u>structure are increasingly complex and frequent. The telecommunications sector is the nervous system that binds all other critical sectors and upon which other sectors are most dependent. Communications <u>info</u>structures and <u>infra</u>structures must be protected. E-Security is important to all sectors. More than $174 Billion[5] in electronic funds traverse the*

[1] **Advanced Analytics and Dark Network/Space Analysis for Predictive Indicators of Cyber Threat Activity** provided Evidence-based cyber security research and applied experimentation at a national scale.

[2] Concurrent and Complementary Investigations, which support the findings include: **Pandora, Janissary, Capstone, Ghost Net, Shadows in the Cloud, Stuxnet, Night Dragon, Koobface, Shady Rat**

[3] **The reference architecture for high-performance secure networking, Published 2011, Bell Canada**

[4] Canadian Security Telecommunications Advisory Committee (CSTAC)

[5] Canadian Bankers Association

network core every day. A miniscule disruption in network-throughput results in a direct and measurable financial impact - a 2% loss of network performance is equivalent to Canada's GNP."- The Darkspace Project[6]

KEY FINDINGS

1. Waves of Cyber e-spionage attacks against Canadian interests have become particularly aggressive, sophisticated and successful in the last year. It is reasonable to assume, given the statistical evidence[7], that all critical infrastructure sectors have been penetrated to various degrees.

2. It is abundantly clear that current standards, policies and practices are no match for sophisticated threats. It is therefore also no surprise that traditional paper Threat Risk Assessments (TRA) are ineffective in predicting, interdicting or preventing attacks, as is the procurement of point security solutions based upon lowest price. Incident response is reactive by definition and is a case of too little, too late. Resources should be better used to deploy solutions that have a demonstrated a high protection index and ROI.

3. Enterprises that are running standard network security infrastructures are highly vulnerable to advanced persistent threats and zero day exploitation. This predicament will become more acute with the convergence of disruptive technologies (IPv6, 4G, and Cloud computing) within the next year.

4. Organizations are currently not able to detect or investigate sophisticated cyber attacks nor are they able to share intelligence without multi-source data fusion systems and advanced analytic capabilities.

5. Global (upstream) security and intelligence is necessary for real-time risk management.

6. All-source methods and capabilities are key to developing a predictive cyber threat capability but require significant investment into Joint 'cyber' Information Intelligence Fusion Capabilities.

7. Access to netflow data is a key element to cyber detection tradecraft and determining trending patterns but evoke significant ethical and legal challenges.

8. Security teams must have the ability to sanitize Personal Identifiable Information (PII), employ cloud-based distributed processing and crowd sourcing to a particular problem set.

9. Security audits must demand empirical type 1 evidence.

10. The business of risk assessment must undergo radical transformation to real-time integrated risk management frameworks that are continuous, automated and use quantitative data.

---

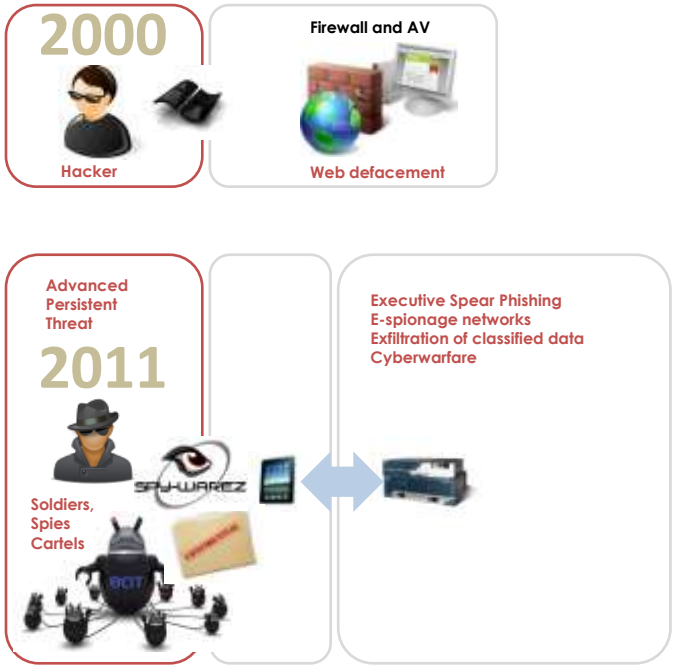
[6] **Study on the Analysis of Darknet Space for Predictive Indicators of Cyber Threat Activity,** Public Safety Technical Program, Centre for Security Science, Defence Research Establishment, Bell Canada, Communications Security Establishment of Canada (CSEC), Royal Canadian Mounted Police (RCMP), Department of National Defence (DND), Canadian Security Intelligence Service (CSIS), Canada Revenue Agency (CRA), and Industry Canada (IC), SecDev, The Munk Centre, SecDev Group and the Canada Center for Global Security, The Citizen Lab , Concordia, McAfee, Cisco, Arcsight, Niksun, Palantir., 31 Mar 2011

[7] **Investigation** as part of the **Darkspace Project** , including **Combating Robot Networks and their controllers** Study, **Night Dragon**, **Aurora**, **Koobface**, **Shadows in the Cloud**, **GhostNet**.

EVIDENCE OF AN CLEAR AND PRESENT THREAT

There is incontrovertible documented evidence[8] of a clear aggressive and sophisticated threat, widespread attacks and measurable losses affecting all critical public and private sectors in Canada.[9]

Cyber threats have evolved from hackers, script kiddies and web defacements, to crime cartels operating sophisticated robot network in tandem with hostile foreign intelligence services (HoIS). Attacks are becoming more bodacious, sophisticated, targeted, dangerous and undetectable by traditional means[10].



> *"Foreign governments preparing sophisticated exploits like Stuxnet, cyberattackers have targeted critical infrastructure. Hostile government infiltration of their networks achieved staggering levels of success."* - **In the Dark - Crucial Industries Confront Cyberattacks**, McAfee's second annual critical infrastructure protection report written with the Center for Strategic and International Studies (CSIS), May 2011.

A year-long investigation[11] uncovered infiltration, penetration, compromise, executive spear phishing, supply chain and traffic shaping with positive attribution to cyber-espionage, organized high-tech crime, hackers, extremists and terrorists.

---

[8] Found in body of the **Darkspace Project** , including **Combating Robot Networks and their controllers** Study, **Night Dragon**, **Aurora**, **Koobface**, **Shadows in the Cloud**, **McAfee Annual threat report** and **GhostNet** et.al.

[9] **Cyber Critical Infrastructure Interdependencies Study** 0D160-063075/A, Public Safety Canada, Bell Canada and the RAND Corporation dated 2006-04-28

[10] Night Dragon Investigation

[11] **Capstone-Janissary Investigation** included as part of the **Darkspace Project** ,Public Safety Technical Program, Centre for Security Science, Defence Research Establishment, Bell Canada, Communications Security Establishment of Canada (CSEC), Royal Canadian Mounted Police (RCMP), Department of National Defence (DND), Canadian Security Intelligence Service (CSIS), Canada Revenue Agency (CRA), and

"There is an overwhelming quantity of empirical data from network sensors that would suggest a high degree of penetration, compromise and loss in all the organizations we investigated. None had the necessary surveillance infrastructure, or tradecraft to detect the majority of penetrations, nor the data-fusion systems and cyber-intelligence analysis capabilities to either process or share data, nor did they possess critical the autonomous command and control security infrastructure to mitigate risks in real-time beyond current levels."[12]

Organizations have large number of covert channels, illicit/untrusted Internet access points and pervasive use of consumer mobile devices handling sensitive communications.

The numbers[13] are staggering:

Over 12% of Internet traffic, including 8,000 North American networks[14], were deliberately redirected through China for what analysts suspect was a templating effort and a precursor to the targeted attacks against Canadian public and private sectors that followed soon thereafter.

Distributed Denial of Service attacks (DDoS) have spiked upward of 100,000 Mbps[15], against the average business/government Internet connection that is only 10 Mbps[16]. All the organizations we investigated experienced DDoS attacks that shut down on-line business operations.

In what some term as the *'Zombie Apocalypse'*, an estimated 1.5-3.6 Million[17] computers are compromised as part of a criminal/spy robot network; this amounts to 5-12%[18] of the Canadian population. Infections persist despite the 252 million botnet connections (58Gbytes)[19] that ISPs takedown every year.

"*Over half the organizations we investigated had lost networks to foreign control and influence through systematic compromise, quite often facilitated through targeted clandestine attacks against executives. The penetrations and exfiltration of highly sensitive data had persisted undetected for years."*[20]

Industry Canada (IC), SecDev, The Munk Centre, SecDev Group and the Canada Center for Global Security, The Citizen Lab , Concordia, McAfee, Cisco, Arcsight, Niksun, and Palantir., 31 Mar 2011

[12] Ibid **Darkspace Project**

[13] Ibid **Darkspace Project** , and PSTP08-0107eSec **Combating Robot Networks and Their Controllers:** a study for the public security and technical program (PSTP), Bell Canada, RCMP, and the Defence Research Establishment, 06 may 2010

[14] New York Times, et.al

[15] Team Cymru, et. Al.

[16] Canadian Advanced Technology Alliance (CATAAlliance) and the Canadian Association of Internet Providers (CAIP)

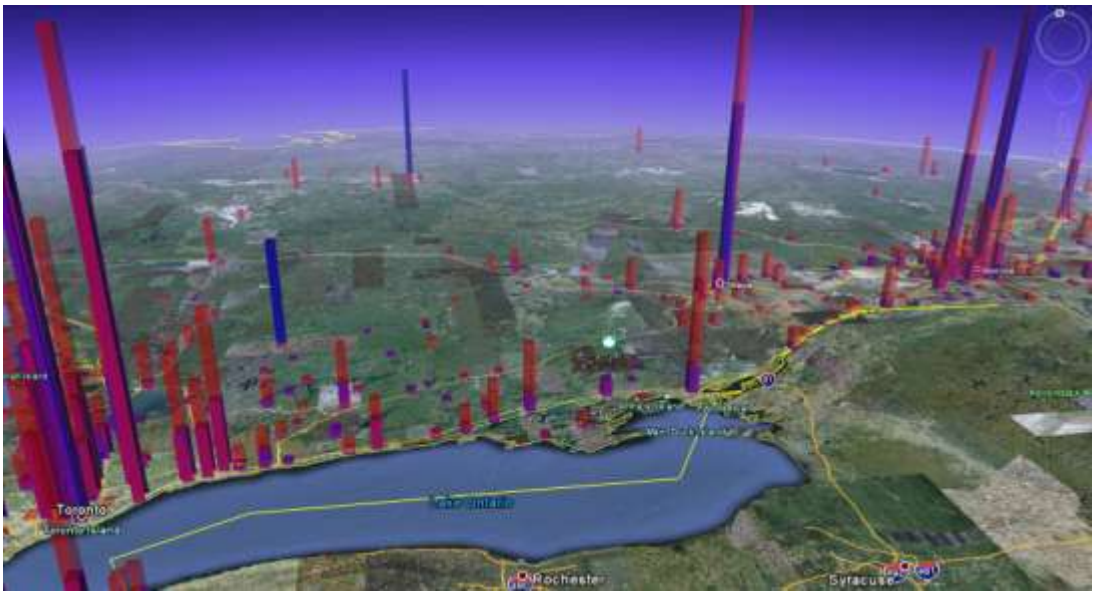
[17] Working figures for the Canadian Security Telecommunications Advisory Committee (CSTAC), International Botnet Task Force, Canadian Telecommunications Cyber Protection (CTCP), GIAIS Global Infrastructure Alliance Internet Safety, CTEPA Canadian Telecommunications Emergency Preparedness Association, National Cyber Forensics Training Alliance and independently verified by Bell Canada as course of the Dark Space Project and Combating Robot Network Study.

[18] Ibid with StatsCan data on the number of computers and internet connections in Canada. Consistent with data published by Canadian Association of Internet Providers (CAIP).

[19] Messaging Anti-Abuse Working Group (MAAWG), National Cyber Forensics Training Alliance and the International Botnet Task Force. Consistent with and verified by Bell Canada statistics when extrapolated from market share.

[20] Ibid **Darkspace Project**

Canadian carriers detect over 125 million attacks per hour[21] on Canadian's, comprising 80,000[22] new zero-day exploits identified every day. The vast majority of attacks are undetectable by traditional security software/hardware.



The research counted 528 Billion illicit/malicious e-mails last year[23], or 98% of all e-mails sent[24]. Over 60% of DNS Traffic[25] is attributable to malevolent sites (botnet controllers). It adds up to a whopping 200 Petabytes[26] of malicious traffic, causing an estimated $100B[27] damage to the Canadian economy. To put this in perspective, 50 petabytes represents the entire works of humankind, from the beginning of recorded history, in all languages.

---

[21] Based upon a summary of reporting logs from the largest Arcsight Security Information Event Management (SIEM) system within a Canadian Tier 1 carrier and scaled based upon market share. Order of magnitude verified by other Carriers through the Telecom Information Sharing and Analysis Center (ISAC)

[22] Average based upon Trend Micro, Symantec and McAfee Annual threat reports. Symantec states that, in 2009, a total of 2,895,802 new signatures for the detection of malware were created, 51% of all the signatures ever created by them. Kaspersky identified about 15 million unique samples of malware specimens in 2009, which means that one unknown sample was discovered roughly every 2 seconds. In 2010, McAfee Labs identified more than 20 million new pieces of malware. [McAfee Threats Report: Fourth Quarter 2010, By McAfee Labs]

[23] Bell Canada message analytics as reported to in Corporate Responsibility Report and to the Canadian Security Telecommunications Advisory Committee (CSTAC), Be Web Aware and Stop Spam Here education campaigns, Messaging Anti-Abuse Working Group (MAAWG), Federal Anti-Spam Task Force (FAST-F), Global Infrastructure Alliance on Internet Safety (GIAIS), OECD's Internet Governance Forum, Digital PhishNet (DPN).

[24] Inbid. 94-98% of email is spam is a widely quoted figure from Microsoft, McAfee, Symantec, Trend Micro et.al. Independently verified by Bell Canada through message analytics in the course of this study.

[25] Observation from the Dark Space Project analytics based upon the specific root DNS that was sampled. Degrees of correlation with Team Cymru and Defence Intelligence DNS monitoring.

[26] Based upon a net aggregation of Bell Canada primary data sources. Figures and analytical methodology is explained with the Dark Space Project and Combating Robot Networks and Their Controllers Study. Data reported within the National Clean Pipes Strategy to the Canadian Security Telecommunications Advisory Committee (CSTAC), and as evidence presented by the Information Technology Association of Canada to the Standing Senate Committee on Legal and Constitutional Affairs (cyber crime and identity theft). There is also oversight of Deep Packet Inspection (DPI) and P2P traffic shaping by CRTC as a matter of regulatory compliance.

[27] Ibid

"On any given day, 30% of overall bandwidth is consumed by illicit activity."[28]

Such empirical evidence has led us to the conclusion that "*anyone who contests that their network is not penetrated, is simply not looking hard enough."*

[28] Ibid.

SYSTEMIC VULNERABILITIES

The threat is sophisticated, aggressive and real. Organizations only see glimpses as to the degree to which they are compromised and have little to no visibility into the threat ecosystem beyond the walls of their buildings. The notion of the network perimeter is an illusion and the entire supply chain is under some degree of global risk.

> *"If you can't deal with a zero-day attack coming from a thumb drive," says former* ***Director of Central Intelligence*** *Jim Woolsey, "you have nothing."*

Traditional security has been shown to be ineffective at either detecting or mitigating advanced persistent threats. It is reactive and episodic. Furthermore, there is very weak correlation between compliance audits, standards, certification & accreditation and the volume of malicious activity measured on a given network.

Reacting to an incident, raising a trouble ticket and performing post-mortem disaster recovery is an untenable strategy for cloaked attacks arriving at a speed-of-light.

> "The security properties of confidentiality and integrity can often be overlooked because their loss is less easily measured and most Canadians (consumers and businesses) are preoccupied by availability and price. But nearly all attack-vectors are against confidentiality and integrity." – Briefing note - **National Clean Pipes Strategy,** Canadian Strategic Telecommunications Advisory Committee (CSTAC).

> *"We have moved from an Internet of implicit trust to an Internet of pervasive distrust."* **- Service Provider Solutions DDoS Protection Solution Enabling "Clean Pipes" Capabilities**, CISCO 2005

THE SOLUTION

Tackling modern cyber-threats requires next generation security architectures that are consistent with the tenets of 5th dimension (netcentric) warfare; notably the doctrine of Battle Command[29] and defence-in-depth[30].

Proactive cyber defence[31] is the only effective strategy within a real-time risk integrated risk framework. Next-generation reference architectures for high-performance secure networking pave the way to deter, detect, and defend against sophisticated threats. The bulk of malicious traffic (toxic content) can be stopped before it reaches an organization by invoking upstream (cloud) security services. It far safer for an organization not to handle toxic content themselves, and carrier-grade solutions are more cost-effective. This frees the organization to divert security budget towards tackling unique problem sets, insider threats and mopping-up what attacks actually get through.

> *"Persistently changing and evolving threats and threat agents are driving up risks and elevating the need for new security capabilities to counter new risks. Forms of upstream security intelligence [clean pipes] are deployed to substantial benefit"*[32]

The concept of next-gen security network engineering can summarized as follows:

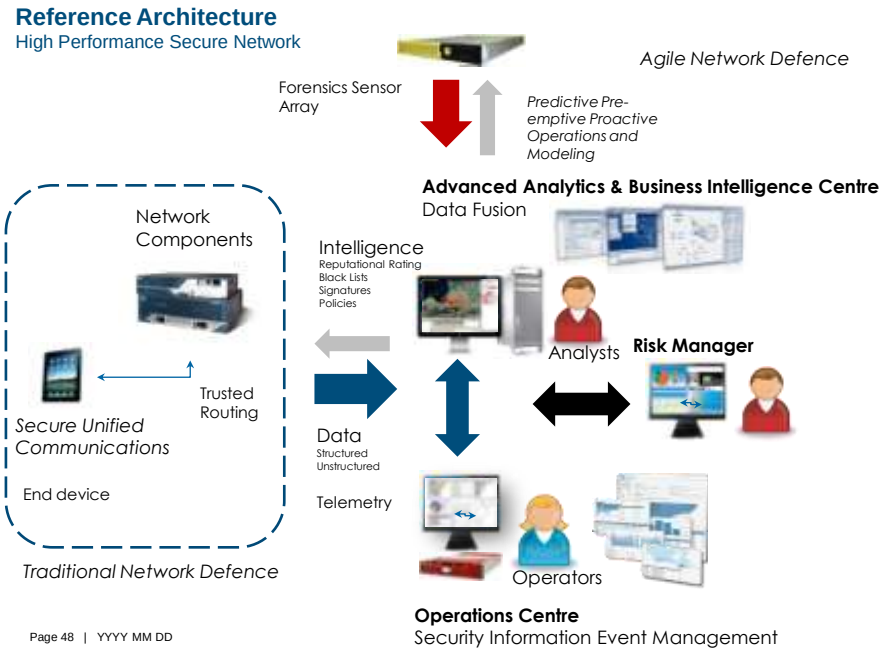
---

[29] **Cyber Battle Command (BC)** is the art and science of visualizing, describing, directing, and leading forces in cyber operations against a hostile, thinking, and adaptive enemy. The concept of battle command applies leadership to translate decision into actions, by synchronizing forces and war-fighting functions of computer network operations (CNO) in time, space, and purpose, to accomplish missions. It refers both to processes triggered by commanders and executed by people and to the system of systems (SoS) that directly enables those processes. This refers to critical cyber systems such as a Joint Information and Intelligence Fusion Capability (JIIFC) and the processes Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance Architectural Framework (C4ISR AF) is integrated into the Department of Defense Architecture Framework (DoDAF). The proactive cyber defence systems-of-systems is manifested in the reference architecture for next-generation high performance secure networking.

[30] **Defence-in-depth strategy** means engaging with and maintaining contact the threat at a distance starting with the notion of "clean-pipes" and upstream security.

[31] **National Proactive Cyber Defence Strategy**, Published 23 Oct 2008, Bell Canada

[32] **Upstream Intelligence and Security Series: Delivery Options for Upstream Intelligence, Upstream Intelligence in the World of Legal Compliance and Liability, Upstream Intelligence: A New Layer of Cybersecurity, Anatomy of Upstream Intelligence, Business Models of Upstream Intelligence Management and Distribution,** published by the Information Assurance Technology Analysis Center (IATAC), Department of Defense (DoD) managed by the Defense Technical Information Center (DTIC), and Director, Defense Research and Engineering (DDR&E), Co-authors Tyson Macaulay (Bell Canada), Dave McMahon (Bell Canada) and Chris Mac-Stoker (Niksun Corporation).



Every network component has three purposes:

- a primary function like routing,
- an ability to produce logs, and
- a capacity to accept intelligence in the form of reputational ratings/filters, signatures, black/white lists, rules etc., and enforce rules/policies.

Unfortunately, most networks install a network component once, program static security policies, and never look at the logs, don't measure effectiveness nor use intelligence.

The intelligence needs to be put into a network to be effective against agile threats like double-fast flux IPv6 robot networks, operated by hostile powers.

The solution necessarily involves the consolidation of all available internal sources into a Security Information Event Management System (SIEM) and made simultaneously available to a multi-source Data Fusion platform supported by an advanced analytical team. This team would have at their disposal specialized forensic sensoring, tools and sources for collection, deep investigation and mitigation such as dark-nets, recursive DNS, honey-nets, DPI, and message statistics (SPAM) etc. Global Threat Intelligence feeds and upstream security and intelligence services combine with the parochial (enterprise) view to create enriched actionable intelligence, which is disseminated through a C2 infrastructure to decision makers, the SOC and individual components for real-time mitigation. Technology/market forecasting and research is needed to get ahead of the threat and shape future solutions.

The Government of Canada will be *"imposing contractual commitments on suppliers that provide some assurance of the integrity, availability and confidentiality of Canada's networks and data and mitigate the threats and vulnerabilities associated with potentially vulnerable or shaped technologies."* - **Technology Supply Chain Guidelines (TSCG) contracting clauses for telecommunications equipment and services,** Communications Security Establishment of Canada, TSCG-01\G October 2010

The official guidance has force under Management Accountability Framework (MAF), the National Security Policy and the Financial Administration Act (FAA). Similarly, there is an evolving audit requirement for verifiable continuous compliance using quantitative metrics and real-time quantitative (Type 1) evidence.

The National Clean Pipe standard developed by the Canadian Strategic Telecommunications Advisory Committee (CSTAC) will remain non-mandatory and will be published in two releases:

Release 1 - Q42011- Telcos seeking a Clean Pipe certification would be required to:

- Comply with requirements on physical security, personnel security, access control, etc. in line with the objectives of ISO 27011.
- Provide basic cyber security protection services including spam filtering, blocking of known botnet communications and limited DDOS protection. Most Telcos already offer these services in one form or another. The objective will be to arrive at a common practice based on what is currently done by each company.
- Be audited.

Release 2 - includes more advanced cyber protection services. Telcos already certified under Release 1 will be able to seek additional certifications for some or all of the following advanced cyber protection services:

- Upstream Cyber Security Intelligence Services (monitoring, detection and cleaning);
- Deep Packet Inspection and Advanced Analytics of client traffic;
- Message Traffic analysis and provision of logs;
- Provision of advanced malware protection services (e.g., APT, fast flux DNS attacks, etc.)
- Data loss protection services
- Forensic Investigations
- Real-Time Integrated Risk Management, etc.

Based on the CSTAC recommendations, advanced upstream security services, capable of detecting sophisticated attacks will be offered only to those companies and governments who negotiate a contract with Telcos (i.e., Telcos will not clean the entire Internet cloud).

SUMMARY OF RECOMMENDATIONS

The recommended solution begins with upstream security services that 'clean the pipe' of toxic content at a safe distance; before reaching the enterprise network perimeter. Next-generation secure networks will be based upon the Reference Architecture[33] and should include the deployment of multi-source collation, data Fusion and analysis capability using real-time global cyber threat intelligence.

[33] Ibid DarkSpace Project