Defence Research and Development Canada
Recherche et développement pour la défense Canada

The Dark Space Project

Dave McMahon
Rafal Rohozinski
Bell Canada

Scientific Authority
Rodney Howes
DRDC Centre for Security Science

Defence R&D Canada – Centre for Security Science

Contractor Report
DRDC CSS CR 2013-007
July 2013

Canada

The Dark Space Project

Dave McMahon
Rafal Rohozinski
Bell Canada

Scientific Authority
Rodney Howes
DRDC Centre for Security Science

Defence R&D Canada – Centre for Security Science

Contractor Report
DRDC CSS CR 2013-007
July 2013

Scientific Authority

Rodney Howes

Rodney Howes

eSecurity Portfolio Manager

Approved by

Original signed by Andrew Vallerand

DRDC Centre for Security Science
Director S&T Public Security

Approved for release by

Dr. Mark Williamson

DRDC Centre for Security Science

DRP Chair

THE Dark Space Project

Privacy and Ethics Statement

The methodology used in this research was based on guidance and precedence provided by the Privacy Commissioner of Canada and Auditor General of Canada for conducting cyber security research from primary data sources.

No personal information has been used in this project. The research was conducted on aggregate data only no personally identifiable information (PII) was collected.

In addition, all research activities related to this project complied with applicable laws and regulations in Canada and the following policies and procedures: the Bell Canada Code of Business Conduct, Bell Canada Corporate Policies and Ethics, the Bell Competition Law Compliance Handbook, the Bell Code of Fair Information Practices and the Privacy Statement and Ethical Principles Regarding Cyber Security Research at the Citizen Lab, Munk School of Global Affairs, University of Toronto. All such documents are publicly available.

Bell Canada research, including this project, was subject to an independent audit under Sarbanes–Oxley Act, regulatory oversight by the Canadian Radio-television and Telecommunications Commission (CRTC), and review by privacy organizations and law enforcement agencies.

This report is derived exclusively from commercial and open sources. No public sector information was used or consulted. In the interests of academic independence, no government information or intellectual property was used in the study, nor has the Canadian government influenced the scientific findings of this report in any way.

TABLE OF CONTENTS

Contents

PREFACE

HISTORICAL CONTEXT

The story began around 2005 with the first demonstrations of live takedowns involving a substantial criminal robot network. At the time, very few security professionals had heard of a botnet or the use of dark space as a means to detect zero-day threat activity.

The demonstration opened discussions on the topic of 'Clean Pipes' and a lecture series on advanced security tradecraft pertaining to Botnet defence including upstream security services. It became apparent to all those involved that a whole World of malevolent activity had been escaping detection for years and was compromising existing security controls with impunity. Traditional security science had been overtaken by the ingenuity of modern threat agents, and the gap was considerable.

A series of projects was subsequently launched around cyber-futures that was meant to study service-provider-level clean-pipes initiatives specifically proactive cyber defence, security sensoring, botnet detection and mitigation, without impacting the privacy of those affected.

One of the important outcomes of the cyber-futures program was the design of an enterprise-wide solution that could feed an advanced Malcode Analysis Treatment and Handling facility. The idea sat dormant for a number of years, as policy, legal and privacy issues[1] were resolved, and the arrival of a compelling cyber events.

Meanwhile, Botnets were behind nearly everything evil in cyberspace. So, it was generally accepted that, to understand botnets, their technology, and the contemporary threat agents who run them, was, in essence, to appreciate the crux of the overall security problem facing public and private sectors.

The first e-security project funded by the Government under the Public Safety Technical Program, through the Centre for Security Science, focused on botnets.

The year-long research project *Defence against Botnets and their Controllers*, published 2010, by Bell Canada for the Government of Canada became a cornerstone research document on estimating the real threat, sophistication of tradecraft, defining effective defence strategies, creating the necessary business case for action and clarifying legal and policy imperatives.

This report used upstream security intelligence, from nascent 'clean pipes' programs, for the first time and demonstrated the efficacy of dark space[2] analysis and proactive defence against advanced persistent threats (APT). It provided the first real hard evidence of wide-spread

[1] Initial legal-privacy-policy interpretations that all IP addresses are private, effectively stalled the use of Intrusion Detection and Deep Packet Inspection Systems in many Canadian organization, which was indirectly responsible for compromises of Canadian computer systems.

[2] Darkspace consists of unassigned IP addresses that are monitored for anomalous activity.

infection/compromises across private/public sectors; showing illicit internet connectivity, the universal erosion of the network perimeter, dispelled the notion of a 'closed system' and ineffectiveness of traditional enterprise security architecture.

The keystone document spawned or accelerated a number of parallel initiatives including a national proactive cyber defence strategy, network consolidation initiatives and the reawakening of centralized advanced threat monitoring designs from the cyber futures program five years earlier.

THE GENESIS OF THE DARK SPACE PROJECT

The e-security cluster, consisting of lead federal government departments, re-established Scientific and Technology (S&T) priorities for 2009/10. The Communications Security Establishment of Canada championed the Public Security Technical Program (PSTP) study for Advanced Analytics and Dark Space Analysis for Predictive Indicators of Cyber Threat Activity. The general requirements stipulated in the RFP, contract SOW, Project Plan and Charter covered a wide spectrum of cyber security issues under the auspices of 'dark space' that looked something like this:

Bell Canada led the DarkSpace Study (PSTP02-359ESEC) with a team consisted of resources, partners and sponsorship from the Centre for Security Science, Research Establishment, Communications Security Establishment of Canada (CSEC), Royal Canadian Mounted Police (RCMP), Department of National Defence (DND), Canada Revenue Agency (CRA), and Industry Canada (IC). The study had major academic partnerships the Munk Centre, SecDev Group and the Canada Center for Global Security, the Citizen Lab, and University of Toronto. The research also included input from the RAND Corporation from previous work on Critical Infrastructure Protection and consultation with Berkman Center for Internet and Society at Harvard Law School and the Advanced Network Research Group at Cambridge University. Key industry partners included: McAfee, Cisco, Palantir, Arcsight, and Niksun.

Much has come to pass in the security World in the two years from the initial requirements definition to contract award. Disruptive technologies like the iPad, cloud computing, 4G, IPv6 were introduced into the marketplace. Threat tradecraft (Stuxnet, Koobface) and detection/mitigation techniques evolved rapidly. No longer was dark space analysis the central focus of defensive tradecraft. To a certain degree, the requirements passed their 'best before' date upon contract award.

During the course of the study, an aggressive campaign of foreign e-pionage attacks was launched against critical sectors (a.k.a Aurora, Night Dragon). The study saw warnings and indictors of similar activity in Canada. A large number of organizations were critically affected.

COURSE CORRECTION NECESSITATED BY COMPELLING EVENTS

A number of programmatic changes were directed in light of the compelling events and advances in science and technology:

- The scope of work was broadened;
- The content and format of the report was restructured along more contemporary lines; and
- A significant amount of resources were re-vectored to pursue in-depth forensic investigations on the ongoing attacks and follow the Stuxnet incident in the pursuit of evidence-based research. The investigative teams linked up with a number of parallel investigations in Canada in the USA and abroad.

The scope of the project was revised to include an analysis of the current cyber threat tradecraft and all/any effective solutions to defend against it, including, but not limited to, darkspace. The Darkspace Project, as it became known, was accelerated from 12 to delivery in 2 months. The scope had since expanded and deepened.

The challenge was to assimilate a broad assortment of unstructured requirements accumulated over two years, from concept to delivery, and create a narrative that made logical sense in the context of today's threat. For contractual purposes, a traceability matrix was used to map 'requirements' to explicit deliverables.

For pragmatic reasons, given the highly-compressed timeframe, the effort was divided into stand-alone chapters, so that separate research teams could work in parallel, and interim drafts could be supplied to partners and sponsors for concurrent review. A logical flow chart of the substantive research shows how the products come together. This foreword, the project plan, an executive summary, synthesis, conclusion and recommendations further help to tie it all together.

Disruptive technologies (IPv6, 4G, Cloud), rapidly evolving threat agent tradecraft and the pragmatics of one of the largest cyber investigations in Canadian history changed and influenced the course of the research midstream and ultimately the conclusions that were reached.

CHALLENGES, OBSERVATIONS AND BREAKTHROUGHS

The first challenge the team had was to build the mechanism to capture real data at extra-ordinary data rates and volumes. We were then presented with an "embarrassment of riches" required substantial open source data mining, in a way that never collected Personal Identifiable Information (PII) whilst leaving worthwhile security metrics. This ability to parse data sets in this manner was a major breakthrough for a number of reasons: firstly it demonstrated the feasibility of redaction of massive data sets into manageable that still yield exceptional results in the ability to detect APTs; secondly eliminated the risks associated with data breach of PII; and thirdly, allowed us to farm-out analysis off-line to universities and take advantage of an untapped sources of keen minds. **Crowd sourcing of deep forensic analysis was shown to be highly effective in addressing hard cyber security problems at a national scope.**

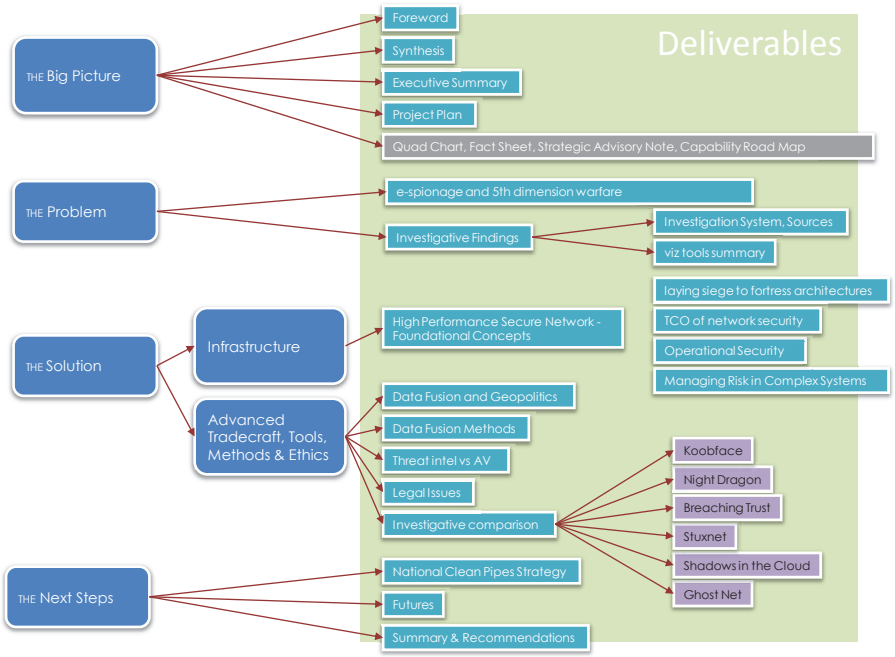
The second challenge was sourcing that advanced analytics and data fusion. It became self-evident early on, that most of the critical data either was buried in the noise-floor or was already imperceptible to existing threat detection-mitigation systems (people, processes and technology). This led to the observation that unless an organization has advanced collection systems, Security Information Event Management (SIEM), and a multi-source data fusion system supported by expert intelligence analysts, then your chances of detecting sophisticated e-spionage and the latest APTs is negligible. Furthermore, a secondary observation is that an organization's ability to share cyber security data and participate in complex investigations is impaired.

CENTRAL THEMATIC EMPHASIS

Provided with these prima facie *observations*, a deliberate emphasis was placed on a discussion of the significance of data fusion in the framework of *Advanced Analytics and Dark Space Analysis for Predictive Indicators of Cyber Threat Activity.*

The community also needed actionable intelligence and pragmatic solutions to address a clear a present threat to the privacy and security of Canadians.

FLOW CHART OF SUBSTANTIVE RESEARCH PAPERS - Darkspace Project



It therefore followed that the logical output of the study should address the requirements in the chief headings of:

- **Problem Definition**: An accurate, actionable assessment of the real cyber threat facing Canadian public and private sectors. This chapter consolidated research threads from *e-spionage and 5th dimension warfare*, a *comparison* of parallel investigations, and primary *investigative findings*.
- **Tradecraft and Methodology**. Advanced defensive tradecraft, analytical capabilities and methodology including multisource data fusion was used to hunt down sophisticated threats. Topics that were covered include a summary of *visualization tools* and *data sources* used in the analysis, a detailed design of the *data fusion system*, a discussion of *methodology* starting with *Data Fusion and Geopolitics, threat intelligence vs anti Virus Research*, specific *data fusion Methods*, and finally an informed opinion of *legal issues* surrounding forensic investigations of this type.
- **Solution**. Industry-validated reference architecture© for that would establish new de facto standards for Enterprise Security Architectures (ESA) that are effective against most cyber threats facing and organization today. This chapter is based upon *Foundational Concepts for High Performance Secure Networking* The sub-chapters address the weaknesses of traditional *fortress architectures*, the importance if *Operational Security* Controls, while showing how to calculate the *Total Cost of Ownership (TCO) of network security*. Furthermore, it explains how to *Manage Risk in Complex Systems in real-time*.

- **Futures**. The futures chapter provides summary of all cyber security research to date critiques their ability to effectively defend against advanced persistent threats. The section identifies emerging technologies and suggests worthwhile research projects for the future.

The business case for national clean pipes strategy is provided as part of the set of recommendations to this research project.

The following auxiliary reports were provided with the deliverables because they were unquestionably influential to the direction and methods of research applied to the DarkSpace Project:

- Ghost Net
- Shadows in the Cloud
- Stuxnet
- Night Dragon
- Koobface
- Breaching Trust

THE DARK SPACE PROJECT - START

The DarkSpace Project - *Advanced Analytics and Dark Space Analysis for Predictive Indicators of Cyber Threat Activity* brings to a conclusion much of the research and efforts to date by providing incontrovertible documented evidence[3] of a clear aggressive and sophisticated threat, widespread attacks and measurable losses. The business case for 'clean pipes' solution[4] is substantiated by a compelling body-of-evidence built over a number of years by teams of experts, that is a matter of historical record[5], subjected to academic peer review.

The findings of the PSTP Botnet study, a year earlier, we hope influenced the National Cyber Security Strategy, which called for the establishment of Government and Industry partnerships to ensure the security of Canada's Critical Infrastructure. Within the Communications Sector, the response to this call was the establishment of the Canadian Strategic Telecommunications Advisory Committee (CSTAC). CSTAC is an Industry and Government group aimed at improving the overall Cyber Security of Canada's Critical Infrastructure. There are a number of groups that report up to CSTAC and provide input to standards. One of these is the Canadian Telecom Cyber Protection Working Group (CTCP). CTCP is a technical level group that will define standards and implement recommendations of CSTAC mandates.

[3] 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.
[4] As presented to the Canadian Security Telecommunications Advisory Committee (CSTAC)
[5] Ibid

The problem definition and solution-set for advanced cyber threats that was documented by the Dark Space project was used as grounding context, business case for the national clean pipes strategy, and influenced a Cyber Security and Privacy Standard for Telecommunications Services Providers.

THE PHOENIX 'CLEAN PIPES' IS REBORN

'Clean pipes' was coined a decade ago to describe carrier-level initiatives to filter 'toxic' content from Internet if requested by end-users. The process consists of detecting malicious traffic in the carrier cloud (upstream), fusing the threat data with global sources, and using advanced analytics to produce and disseminate cyber threat intelligence as a value-added service to businesses, and for real-time mitigation within the cloud as an upstream security service. The prime business drivers for 'clean pipes' are: corporate responsibilities, direct losses, brand risk, and creating new value-added revenue streams to otherwise rapidly commoditizing connectivity services.

The 'clean pipe' solution, which is the ultimate conclusion of the Dark Space project, has been well documented within the *reference architecture for high performance secure networking*©. A low-risk migration plan could be fully implemented in months. The program would necessarily involve: access to a spectrum of high-value infrastructure and global data sources; integrating these sources, deploying central data fusion technology, resourcing the centres with advanced analytics capability and disseminating (PII sanitized) real-time threat intelligence for integrated risk management and both upstream/downstream mitigation of threats by systems designed to act on this data autonomously. This includes the necessary oversight framework to ensure privacy concerns are met.

ABSTRACT

Cyberspace is best understood as a complex global ecosystem subject to technical and social drivers. The research carried out by this study suggests that current approaches to cyber security are ill-suited to detecting or anticipating threats, which increasingly rely on hybrid socio-technical vectors.

Securing national cyberspace requires a paradigm shift toward a common operating picture (COP) of cyberspace. The project undertook research and experimental work along several axes critical to establishing a common operating picture of cyberspace. The principal outputs are grouped under the following three categories: i) research into the practical and ethical dimensions of a behaviour-based model of detecting and anticipating cyber threats; ii) a reference architecture for implementing the objectives of the national cyber security strategy; and, iii) testing and validating methodological approaches to detecting advanced cyber threats on the basis of "live" data obtained from operational sources that had been stripped of PII.

EXECUTIVE SUMMARY

"Any organization that contends that their network is not penetrated, isn't looking hard enough."

Current approaches to cyber security are ill-suited to detecting and anticipating threats, which rely on a hybrid socio-technical vectors of attack.

This report summarizes the findings that employed a multidisciplinary, evidence-based approach to review and test current best practice in the detection and anticipation of advanced cyber-based threats. The research suggests that defence against advanced threat vectors requires paradigm shift away from an emphasis on post-event forensics, and towards a more holistic proactive approach that emphasizes intent and inability to quantify the consequences of cyber insecurity. While this shift is generally within existing COTS solutions, it requires cultivating new skill sets and competencies, as well as addressing and emergent set of legal and ethical considerations. A next-generation reference architecture for high-performance secure networking was validated against advanced persistent threats.

The research is carried out by a team of open-source researchers from academia and industry, and grouped into three parallel but in interconnected components: academic research, technical development, and applied experimentation.

This report is organized into three parts.

Part One provides an introduction and background to the research objectives, and the conduct of the project.

Part Two presents an overview of the activities and deliverables carried out by the project.

Part Three consists of draft recommendations for future research.

Results

This research constructed an accurate threat picture and designed the effective security solution, which demonstrated means to recover billions in direct and indirect damages owing to cyber attacks. The report constitutes the body-of-evidence for a compelling business case for a national cyber security strategy.

The investigation uncovered a significant number of high-confidence targeted threats over 24 hour period, from within a gargantuan data set; that had previously gone undetected by traditional (standard) security safeguards. This finding represents a manageable target set which would permit eventual attribution to an actor and a risk profile for the organization, should the research efforts been extended past the two month window permitted.

Key Findings:

- ***All-source methods are key to a developing a predictive Cyber threat capability*** but require significant investment into advanced fusion platforms. COTS solutions do exist and could be rapidly deployed but require significant investment in order to deal with the volume and scope of data that requires real-time analysis.

- ***All-source capabilities are complex and require a paradigm shift away from engineering approaches to cyber security***. They require the development of competencies that emphasize a multidisciplinary approach capable of working with heterogeneous data sources. These capabilities should not be retrofitted to existing security operations centres, which focus on network performance metrics, and are ill-suited to predicting vectors of disruption, or quantifying the consequences of network intrusions and exploitation.

- ***Access to netflow data is a key element to Cyber detection tradecraft and determining trending patterns evoke significant ethical and legal challenges.*** Large-scale log analysis incurs significant issues around captured PII that cannot be overcome without resorting to closed research methods. These, in turn, put limits on information sharing. Creating an environment that permits real-time access to critical data, while safeguarding privacy considerations will require development of an appropriate legal and privacy framework, with trusted independent oversight.

- ***Organizations are not able to detect, investigate sophisticated cyber attacks nor are they able to share intelligence without multi-source data fusion systems and advanced analytic capabilities***. All of incidents and patterns of malicious activity discovered in the course of this report where previously unseen by traditional security controls. The ability to distribute cyber threat intelligence analysis was severely limited by an organizations ability to receive and interpret the data. Organizations lack the necessary people, process or technology and mandates to manage advanced persistent threats.

- ***Organizations are running traditional networks that are vulnerable to non-traditional advanced persistent threats.*** Outside of critical infrastructures, we see little evidence of modern enterprise security architectures that includes concepts of: threat intelligence feeds, darknets, data leakage protection, DNS security, upstream security, DDoS protection etc., described in the reference architecture for high performance secure networks. ©

Key Recommendations:

Multi-source Collation, Data Fusion and Analysis. The investigative thrust of this research represents a snap-shot of the current threat activity. As alarming as that is, the true situation is likely much worse. As a matter of due diligence, it is necessary to conduct a 12 month in-depth investigation deploying a data fusion system to process all available sources in near-real time at full-scale. The business case (ROI) clearly shows that the cost savings (fraud reduction, incident prevention, bandwidth recovery) easily pays for the deployment and operation of a capability in any organization and is scalable to a national level.[6] This is a key facet of real-time integrated risk management. One of the goals should be to close the attribution loop on current cyber attacks affecting public and private sectors.

Next Generation Secure Architectures. The investigative evidence[7] demonstrates that traditional network security and policies are not effective against advanced persistent threats. Current work around Enterprise Information Security Architectures (EISA) MUST take under review the findings of this advanced research and other recent studies. In particular, the reference architecture for High Performance Secure Networking © herein represents the emerging industry standard for EISA and has been shown to be uniquely effective against sophisticated attacks.[8]

National Clean Pipes Strategy. Support should be provided to carrier-led initiatives to filter 'toxic' content from Internet. The process consists of detecting malicious traffic in the carrier cloud (upstream), fusing the threat data with global sources, and using advanced analytics to produce and disseminate cyber threat intelligence as a value-added service to businesses, and for real-time mitigation within the cloud as upstream security services. The prime business drivers for 'clean pipes' are direct losses, brand risk, and creating new value-added revenue streams to otherwise rapidly commoditizing connectivity services.

Cyber Security Standard For Telecommunications Services Providers The public sector and critical infrastructures should be encouraged to contribute to a standard that aims to ensure that customers have a much more reliable and safe user experience by ensuring the availability of service to the customers and limiting the malware that those customers might face. No amount of work by a service provider can ever fully remove malware as a problem, however, often the presence of malware will be detectable and a service provider can inform a customer of it's presence. Reducing malware and other cyber security issues will free up bandwidth for other uses, and generally make Canadians safer. This will generally lead to a better user experience for customers and reduced network management issues for providers. However, there must be a legitimate demand citizens, businesses and governments.

[6] National Clean Pipe Strategy and Business Case, CSTAC

[7] 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.

[8] The availability and cleanliness of reference architecture was measured to be significantly better than large traditional networks (100,000 user+) using upstream inbound-outbound analysis.

THE PLAN

Introduction

This report summarizes the research carried out under the terms of the Public Security Technical Program (PSTP) Study on Advanced Analytics and Darknet Space Analysis for Predictive Indicators of Cyber Threat Activity and carried out on behalf of the PSTP's e-Security Community of Practice (CoP)[9]. It supports the e-Security CoP through the pursuit of an S&T initiative dedicated to providing research and development recommendations to advance the state of the art in cyber threat intelligence prediction technologies.

The objective of this study was to employ an open source methodology and approach to test the hypotheses whether advanced tradecraft and dark space analysis could be an effective means for detecting advanced cyber threats including zero – day attacks - and provide a predictive capability defence against advanced persistent threats.[10] The study was carried out by a team led by Bell Canada that included: the SecDev Group, Canada Center for Global Security, Bell University Labs, Cisco, McAfee, Niksun, and Arcsight.

The work of the project was deconstructed into three parallel components:

- **Academic research** into the practical and ethical dimensions of detecting and anticipating advanced cyber threats.
- **Technical development** of a reference architecture designed to meet the intended objectives of the national cyber security strategy.
- **Applied experimental work** testing and validating advanced methodological approaches to detecting advanced cyber threats on the basis of real data.

In an effort to promote synergy where practical researchers were generally involved across all three components.

[9]The e-Security Community of Practice includes, but is not limited to the following government agencies: Communications Security Establishment Canada (CSEC, Royal Canadian Mounted Police (RCMP), Department of National Defence (DND), Canada Revenue Agency (CRA), and Industry Canada (IC).

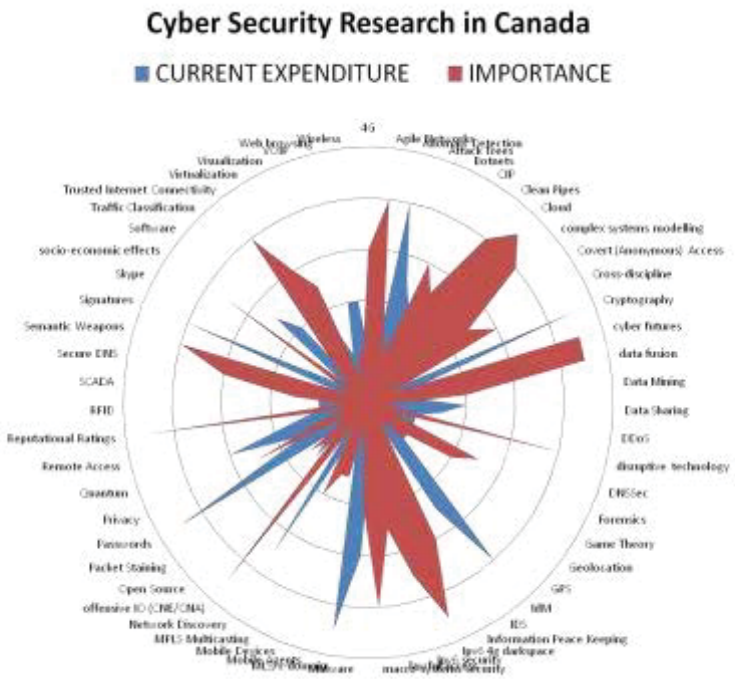
[10] Team Cymru http://www.team-cymru.org/Services/darknets.html

Research Background

Current industry best practice suggests that near-real-time (NRT) cyber threat intelligence can facilitate the implementation of a proactive defence of the critical cyber infrastructure and counter the rapid evolution of cyber threats.

At the same time, experience accrued by Internet operators suggests that the fusion of carrier-level net flow data with global threat intelligence feeds can achieve a workable degree of cyber situational awareness that can be leveraged for proactive defence, especially with a data fusion platform. But applying all-source data fusion and multidisciplinary analysis in real-time on live net flow data requires access to appropriate data, and appropriate skill sets, competencies, and toolsets. For the most part, bringing together these requisites is a major challenge. Carriers are reluctant to share net flow data without legal assurances over the handling of PII. Toolsets and skills required for analysis are expensive, and are difficult to implement in and operational setting without incurring significant legal and ethical challenges. Research methodologies are complex and some tradecraft requires legal testing and challenge in order to determine its status under existing privacy and cybercrime legislation. Moreover, the technical environment is itself fast evolving, and generates significant disruptive tendencies that introduce uncertainty and can quickly date research findings.

The team reviewed over 400 cyber security research projects conducted in Canada over the past five years. The discovery process involved literature searches, interviews, and tracing funding. The team also had unique insight to into the product development plans of major industry leaders as partners under NDA. Additionally, Bell University Labs had traditionally funded over $2.5 Billion in external ICT research. Bell Canada is the lead reseller and consumer of cyber security products and services in Canada. Thus, details of cyber security research were available from sales metrics. Therein, we reviewed tens of thousands of cyber security projects and extracted those that we would categorize as research. The following graphic illustrates the relative expenditure and importance of 38 common cyber security research themes in Canada. Future recommendations are also included in the analysis.



The majority of cyber security research in Canada is conducted by a hand full of Universities across broad interests. Whereas, the lion's share of the public sector cyber security research funding has gone to esoteric multi-level/cross-domain and cryptography themes.

Research tends to be exclusively reactive-defensive, and thus lacks the insight necessarily gained by proactive-offensive knowledge.

Overall, research would greatly benefit from much closer ties to industry programs. Given lack of access to operational systems and real World data, there is understandably very little evidence-based research. Quantitative (experimental) data appears to be created mostly in laboratories. This tends to lead to solutions and conclusions that are erroneous, unscalable or impractical. Size matters, and labs often do not scale to address emergent macro effects or model a complex systems, as is cyberspace. The big data problem is significant.

A high percentage of research is being conducted in areas that yield very low ROI or protection indexes when applied to operational systems. Even more odd, is the number of 'research' projects that are being pursued when a COTS product already exists or the problem has already been solved. Much of the research is appears to be preoccupied dealing with a unique solution to yesterday's problems. We highly recommend research (cyber security futures) that addresses tomorrow's threats, disruptive technologies and evolution cyber security and insecurity.

Current expenditure rating was derived from the number of research projects on that topic, the overall budgets and resources that appear to be allocated.

The importance rating is based upon a protection index derived from the ability of the method/technology being researched to effectively reduce advanced cyber threats. The protection index is created by empirical measurement on a large scale network infrastructure.

Methodology and approach

The research carried out under this drew upon original, as well as in progress research carried out by a multiple of research and industry partners. Because of the compressed timeframe, the research work was coordinated across constituencies using a number of organizational mechanisms, including confidentiality containers, that ensure that issues around the handling of data, did not trigger privacy or other PII concerns. For the most part, this approach worked well, although the limited timeframe did not allow for broader team meetings, which would have resulted in greater inter-oblation and cross-fertilization of findings across the three project component/phases (see below).

The duration of the research also precluded the application of larger scale data modeling methods and tool sets to the operational feeds made available under the terms of this study. This work is ongoing, and is expected to yield significant insights material to the objectives of this study.

The project was organized into three distinct independent phases meant to mutually reinforce the overall objective of the project.

Component One - The project commissioned academic papers that surveyed state-of-the-art methods and approaches to detecting advanced cyber threats, and the legal and ethical implications of existing detection and investigation tradecraft. This component also included a review of current science and technology programs, as well as operational programs aimed at developing a common operating picture capability in support of the objectives of the national cyber security strategy.

Component Two - development of a reference architecture © in the context of a national cyber security strategy in cooperation with industry partners. The study identified the solution for establishing a common operating picture (CoP) of in cyberspace based upon all-source data fusion.

Component Three - the research embarked on a number of controlled experiments designed to validate an open-source methodology for near-real-time detection, and anticipation of socio-technical threats and vectors. The experimental work was partially completed, although it did validated the hypothesis that existing security systems deployed on typical networks were incapable of detecting many current generation cyber threats (malware).

All three components were undertaken simultaneously by the bind project team and where practical, team members were given full visibility over data and findings.

Activities and findings

Commissioned Academic Research

The project commissioned a series of rapid research papers in order to assess the state-of-the-art cyber detection/mitigation. The research papers were not meant to be academic essays, nor full-blown research reports. Rather were commissioned as collections of "best knowledge" synthesized and referenced in a way as to make them a useful guide for future research.

Research paper #1: **Threat Intelligence vs AV**. What is threat intelligence, and how does it differ from antivirus research, and security research? Does it represent a new approach to understanding cyber threats, how does a complement and or supplant existing methods? The paper critically compared and contrasted the methods for detecting and mitigating the malware threat, and documented the evolution from code based threat mitigation through to behaviour-based threat anticipation. Historically, anti-malware efforts have focused on the analysis of code. Antivirus research has concentrated on the rapid heuristic detection of malware code behaviour - designed to rapidly detect, and defend desktops were latterly networks from emergent strains of malware. Security research examines the patterns of interconnections between malware code, namely viral vectors, and command-and-control networks of architecture. In the recent past, both fields have blurred, and acting complemented by a third approach which attempts to examine the actors responsible for running code and focuses on profiling individuals, as well as some of the tradecraft and behaviours that are used by these individuals.

Research paper #2: **Data Fusion**. What are fusion methods, what is their etymology, what are the differences between data mining, and behaviour-based modeling, what are the leading platforms and approaches to all source fusion and how are they applicable to cyber research? This paper examined the elements of a fusion methodology for analyzing cyber threats. Traditionally, data mining and statistical analysis have been preferred by systems administrators as a means of isolating and localizing threat vectors. With the emergence of APT and complex multi-vector threats, fusion methods which blend technical analysis with threat intelligence and behaviour based mapping techniques have emerged as a promising, albeit unproven means for real-time anticipation of threats. This paper examined the traditional methods of cyber threat detection (data mining, log file analysis, network monitoring), as well as some of the tools of fraud detection more broadly. These then were compared to the emerging generation of detection tools, which focused on the behaviour mapping and multi-source, interdisciplinary analysis. The paper provided a matrix that lists, compares and contrasts differing toolsets (ie., Zeropoint and Palantir, I2, Centrifuge, Maltego, GEOtime, Tableau, etc.)

Research paper #3: **Legal and ethical dimensions** of fusion techniques based on honeypot, sinkhole and use of DPI for threat detection. The use of honey pots, sinkholing, packets staining, and DPI is generally accepted as legitimate practice by network operators in order to mitigate against

questionable or legitimate traffic (as defined by the accepted usage policy of the provider). Whether these techniques could be used at a larger scale, by governments, groups of corporations, or nongovernment organizations as a means of practicing collective defence is open to question. The objective of this brief paper was to lay out the legal challenges to applying "network defence and detection practices" beyond the clearly defined bounds of a network, which can be proven to be owned by the subject pursuing these practices. Can these techniques be used by security researchers, academic institutions, corporate entities, or a duly constituted network Defence agency without breaking new ethical and legal ground.

Research Paper #4: **Lessons learned: Stuxnet, Ghostnet, Shadows, Koobface, Breaching Trust** - that inform or suggest advanced techniques, policy processes, legal and ethical dimensions of developing next generation detection and investigation systems. The objective of this paper was to take a crosscutting view of the four key investigations undertaken by the Information Warfare Monitor grouping successful techniques, practices, challenges, and observations into "lessons learned" categories.

Research Paper #5: **E-spionage, cyber terrorism and 5th Dimension Warfare in 2011.** This Paper provides a Common Operating Picture (COP) of cyber security based upon global and national threat intelligence. The chapter included an expert strategic analysis of threat agents, means and methods affecting Canadian interests with special focus on suspected state-sponsored espionage and warfare. Linkages to historic and current investigations were provided as they unfolded before our eyes.

Research Paper #6: **Data Fusion Methodology and the Geopolitics of Cyberspace**. The paper discussed a fusion methodology that integrates technical interrogation, in-country field research, data analysis and visualization techniques. It explained the central characteristics of fusion methodology and how it can be operationalized in case study research. This paper was prepared in part on the basis of investigations undertaken by the SecDev Group and Citizen Lab, including Ghostnet, shadows of the clouds, and Koobface. The paper examined some of the ethical and legal implications raised by the methods, including questions of privacy, data retention, and security of field researchers, and included a critical analysis of the method‘s limitations and shortcomings and point towards future developments.

Technical Development - Reference Architecture ©

This effort designed and demonstrated proof of concept for a reference system architecture for high performance secure networking that could be validated by this evidence-based based research and scaled to carrier level system in the context of a national cyber security strategy.

This research project required construction of an automated system to extract threat data, which functioned within the context of mature operational programs, leverage emerging technologies, and could be integrated with upstream infrastructures, and organizational systems. The methodology employed considered all technical and non-technical critical interdependencies within an operational environment to ensure that its function was workable within the framework of existing priorities, risk tolerances, budgets and laws. The research simultaneously addressed the health of broadband networks and advanced persistent threats in tandem with the security of rapidly evolving networks and the ever expanding IP universe. The study addressed critical dependencies with important control planes such as DNS security and trusted internet connectivity (TIC) in the same manner recognized through the close integration of the Comprehensive National Cyber Security Initiative (CNCI).

The design demonstrated a clear migration path from legacy to a state-of-the-art solution for monitoring the core national network systems and provided clear measurement of Total Cost of network Ownership (TCO) and Return on Investment (ROI).

Non-technical constraints that continue to inhibit the deployment of Canadian cyber defence capabilities to date were discussed.

Industry best practice

Bell, Cisco, and McAfee collaborated on reference architecture for high performance secure networking© with important support from Zeropoint and Palantir, Arcsight, Niksun, Arbor Networks, Juniper, Microsoft, Apple and Nomimum. The reference architecture represents the industry gold standard for proactive network defence. It comes in two flavours:

- The 98% solution, as the name would suggest, is nearly effective at mitigating all known threats and can be assembled off the shelf with excellent ROI for security dollar spent; and
- The 99% solution comes close to providing six nines confidentially, availability, and integrity by including an advanced solution set onto a reference architecture.

All source fusion

A large number of data sources were used to build a contiguous threat picture from global to national and enterprise levels:

- Global Threat Intelligence was derived from reputable sources like Arbor McAfee, Microsoft, Team Cymru, Spamhaus, etc. This provided a view external and enveloping our target infrastructure.
- Global Cyber Intelligence was commissioned from McAfee Threat Intelligence Services and DNS/BGP malicious activity data from Root servers using open sources Three million malware samples were analysed as well as suspicious activity inbound and outbound to the target infrastructure.
- National Information Infrastructure (NII) view used very large carrier-grade sensors arrays consisting of millions of individual sensors. Peakflow sampling of 900 petabytes of raw data revealed approx 200 petabytes of malicious traffic, which was mitigated. The sheer volume of data precluded forensic examination of all the traffic. This data had no PII associated with it.
- Deep-Analysis was conducted against target infrastructure the size of 100,000 machines. A sample of two (2) weeks of security log files yielded 2 billion records (after significant reduction) and took a team of forensic analysts 2 months to investigate. The analysis spun-out a dozen parallel investigations and linked several forensic teams.

Applied Experimentation

The objective of the applied experimentation component of the project was the capture and analysis of a statistically meaningful sample of suspected malware activity originating from: a) Assigned infrastructure ranges, and b) IP addresses associated with the public cloud (publicly visible IP ranges).

As a secondary objective, the research tested and validated a two step methodology for generating large-scale data sets derived from operational data, suitable for analysis within an and protected public research setting. In part, this was the necessary condition of the research, in order to protect confidential data, as well as sensitive information relating to the structure/operation of the networks, while ensuring access to operational level network data. Consequently, the research was divided into two components to ensure that privately identifiable information, and/or confidential information was excluded from data passed to researchers working in a public university context.

There were two parallel forensic teams:

- research carried out by a team with access to primary data (primarily network topography and addressing)

- University-based team, which worked with clean data, but possessed no PII or other means to identify the origin/source of data to be analyzed.

The work of both research teams was monitored and directed by researchers and legal/privacy oversight team with visibility on both sides the project.

Methodology and sources:

The first component of the research analyzed DNS requests to known malware domains originating from within the Public cloud. The IP ranges analyzed included assigned IP space, dark space and public cloud infrastructure). The research relied on data from two upstream SOA sensors and examined data between 3 and 28 February 2011. Sensor "A" - monitored for 56 known malware types, and analyzed data between 23 and 28 February 2011. Sensor "B" - observers ~ 70 MB DNS requests per day from a dynamic DNS network that is heavily used by malware operators. Statistical analysis supports evidence that upwards of 60% of DNS requests to the public cloud originates from malware. Data from the Sensor "B" was observed over 24 hour period, and analyzed into known and suspected malware connections. Suspected malware domains were subsequently cleaned of originating IP/domain information and passed over to the team for further analysis.

The second_component of research analyzed file path structures and requests derived from an analysis of outgoing HTTP proxy logs. The file paths were stripped of originating IP/domain information, so as to prevent the inadvertent transfer of PII to the research team. However, time stamped data was preserved in order to aid time-series studies of recurrent connections. The data was gathered from four NetApp proxies, between 28 January and 19 February, 2011, in two batches. Batch one consisted of a single day sample (28 January) of approximately 812 MB (compressed). Batch two consists of over 80 GB (compressed), corresponding to two weeks worth of log files (1-19 February). The file path calls were analyzed for signatures known malware, or connections to IP/ domains, suspected/known to be used by specific malware. The resulting list of domain/IPs is compared/ analyzed the list of known and suspected malware domains generated by the log analytics. Domains that do not correspond to the log lists are further analyzed, and where warranted honeypot in order to determine the characteristics of suspected malware, or exclude malware activity.

Suspected/known malware was triaged into four categories: i) known, ii) unknown, suspected targeted APT, iii) unknown, suspected commercial, iii) unknown. All four categories are further analyzed using the fusion platform to create a typology of malware infections, and identify vector/events, which could be used, to explain the: a) nature and origin of threat, b) event/cluster analysis, c) identify possible mitigation strategies.

Investigative Results

Preliminary analysis suggests that traditional security did not capture a significant amount of malware activity, which was readily identifiable when threat intelligence heuristics were applied against temporal and signature-based criteria, existing cross ASN malware connections that were readily visible when run through a rule-based cluster visualization.

Further research yielded comprehensive data on structured requests originating from assigned network space in a manner that shows/protects the identity of the networks, and other PII from public space investigators. The absence of originating IP information, however, made it difficult to link specific file path requests mixed it difficult to link identified malware with specific infections occurring within the public cloud without significant follow-up investigation of the malware command-and-control domains.

This part of the project was a partial success. The experiment proved that it's possible to pull data from operational servers in a manner that protects PII, making it available to a larger open source research community.

The data yielded evidence of interesting malware connections, corresponding to known crimeware kits, and bot net architectures. These kits consisted of commonly used variants, contemporary variants, and bespoke modifications.

The data was also sufficient to discover and identify IP and domain information by searching file path call information. These domains or IP addresses clustered, and an analysis of the IP addresses and domains yielded clues as to providence and origin.

However, the data also yielded significant noise. Without corresponding originating IP and DNS information, it was difficult to use this method in order to determine bespoke or highly targeted attacks. The research yielded evidence of two adapted Zeus bot nets, but deeper analysis in order to identify APTs at this level would require more data points than this method allows.

Initial Recommendations

A cyber futures plan identified and discussed areas that require further research. We estimated time horizons, and evaluated respective TRLs from a next-generation perspective; ones that surpass existing threat capabilities and counters emerging technologies before related services are deployed on a wide-use basis.

An analysis of opportunities and gaps, derived from a matrix of existing operational programs, is included.

THE PROBLEM

The impetus for security research is to counter the danger to information and technology posed by deliberate agents. This chapter provides a detailed accounting of the cyber threat and risks in cyberspace on the global stage and national scene.

E-SPIONAGE, CYBER TERRORISM AND 5TH DIMENSION WARFARE IN 2011

The Perfect Storm is developing in cyberspace. The maelstrom has already hit landfall on the leading edge of technology. Here, the phenomena represent a confluence of trends that cyclically reinforce the energy of the surge in the impending cyber-storm. National information infrastructures are now decisively engaged in a conflict other-than-war. The battle over information sovereignty has begun just as globalization has eroded constructs of Westphalian sovereignty and legitimacy. Consumerization, cloud computing and crowd sourcing phenomena have created a cyber commons. The social contract, as it pertains to cyberspace, is fragile. Although governments around the world have invested in themselves, little has been done to safeguard businesses citizens over the years. Now the telecommunications, financial sectors and human rights movements are fighting on the front lines against trans-national crime and state-sponsored campaigns. Over one-trillion inbound attacks per year are dealt with in a pre-emptive fashion by global telecoms carriers and the security industry. That is 125 million attacks per hour inbound at 1 billion km/hr![11]

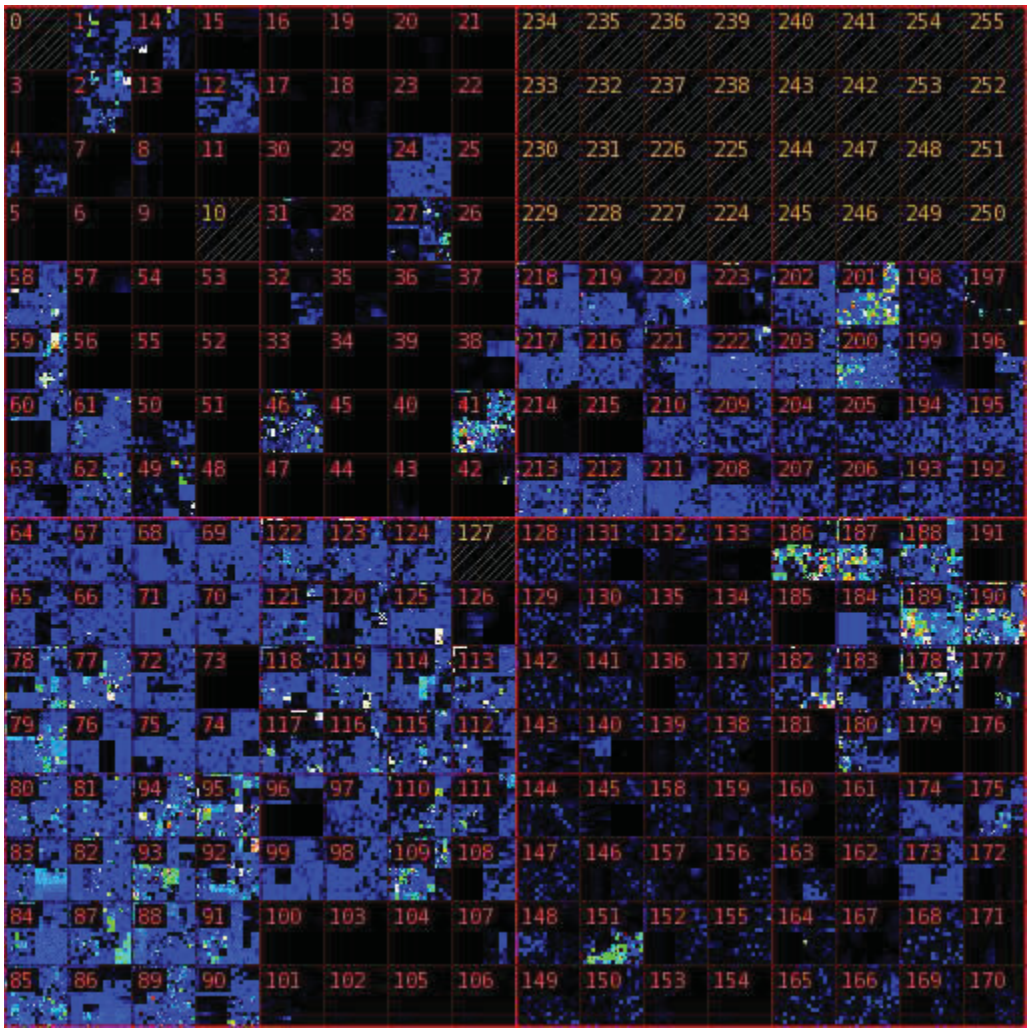
"Cyberspace is so toxic at its outer limits that any PC placed at the source would be instantaneously possessed by ubiquitous evil. Virtually anonymously they lurk interconnected networks; spying, compromising and exploiting. They can attack and withdraw back into the darkness at the speed-of-light. They are the hackers and crackers, telecommunications phreakers, precocious script kiddies,

[11] 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)

corporate espionage programs, cyber-terrorists, spies and sophisticated translational organized criminal syndicates engaged multibillion dollar heists. "- Cyberthreat, Warwick Publishing (August 1, 2000) ISBN-13: 978-1894020831

Public and private sector executives in Canada are being successfully targeting by organized crime and hostile intelligence agencies using spear phishing tactics. Then, just when you think you have identified the threat agent and understand the tradecraft, your organization is blind-sided by the actions of an insider with access to your most sensitive computer files, and a penchant for trouble. No system or organization is safe. [Proactive cyber defence and forecasting the perfect storm October 2008, , Bell Canada.]

The map below by Team Cymru represents a summary of malicious activity seen on the Internet over the past 30 days combined. The IP space is mapped into this image using a Hilbert Curve.



Agents of chaos

People attribute sluggish computer networks or outages to chance, when the cause is often deliberate. In this age, the mouse has proved mightier then the inter-continental missile to deliver multiple nuclear payloads, launched from places like Russia and China, as incarnated by robot networks (botnets). The strikes rain onto Canada relentlessly. Decontaminating the fall-out after one of these cyber bombs has gone off inside your organization is a costly affair. The repercussions of foreign cyber attacks against Canada are estimated in the billions each year[12], or about six-times more costly than our entire defence budget. The only defence is a proactive one. But if no one has noticed, is this just the cost of doing business?

Cyber Crime is big business

"Cyber crime is now the most significant challenge facing law enforcement organizations in Canada" were the headlines of a nationwide survey, commissioned by the Canadian Association of Police Boards (CAPB) in 2008. The mischievous, thrill seeking hackers of the 1980's has given way to a sophisticated breed of cyber criminal who has the resources and technical capability to conduct large scale criminal activity over the Internet. Today, the tool of choice for these criminals is the robot network or botnet where home and office computers are hijacked, often without the knowledge of their owners, and programmed to serve a botnet controller for illegal purposes such as: espionage, fraud, identity theft, bulk email or spam and distributed denial of service attacks.

Robot Networks in the Literature and Recent Research

A botnet is a collection of software agents, or robots, that run autonomously and automatically. The term is most commonly associated with IRC bots and more recently malicious software, but it can also refer to a network of computers using distributed computing software.

http://en.wikipedia.org/wiki/Botnet

[12] Based upon a net aggregation of 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).

Sophisticated large scale Botnet quarantine tradecraft and facilities have existed in telecommunications networks since the 1990s. The Storm Worm began 19 January 2007 by compromising machines, installing a kernel level rootkit and merging them into a larger robot network (Botnet); one that has now grown to 50 million computers globally.

The 2009-2010 Report *Combat Robot Networks and Advanced Persistent Threats*, by Bell Canada and SecDev provides a deep-dive study into:

- advanced Botnet tradecraft and Advanced Persistent Threats (APT);
- quantitative evidence of ongoing attacks, the threat agents and prevailing uses of Botnets to support criminal activity against Canadian interests;
- a discussion of the legal and privacy concerns related to information collection on Botnet activity and the issues related to proactive defence measures against Botnets;
- effective architectural solutions to mitigate the risks posed by Botnets;
- strategic business transformation roadmap for police, intelligence, defence and public safety agencies; and
- advanced tools and techniques that can be used by Law Enforcement Agencies (LEA) to monitor Botnet activity and to gather evidence and actively pursue criminal activity using Botnets.

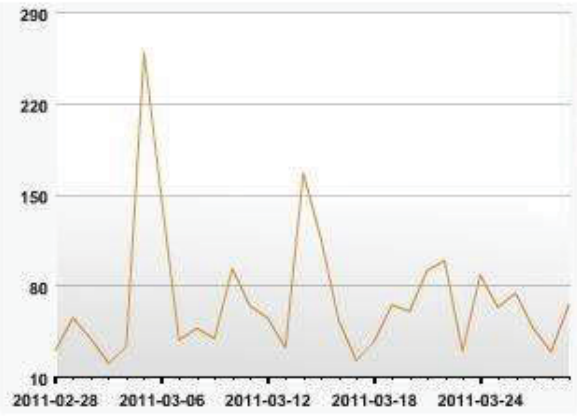
A recent report by entitled *Detection, Measurement, Disinfection & Defence*, by the European Network and Information Security Agency (ENISA), Fraunhofer FKIE, and University of Bonn, Germany, serves an excellent summary of literature search of botnet detection and mitigation techniques in practice and research.

Team Cymru Darknet project, CAIDA's Network Telescope project and the Internet Motion Sensor project at the University of Michigan are examples of applying dark space analysis to threat detection.

Average Daily Botnet Traffic

This chart shows the average amount of traffic we see to each botnet command and control (C&C) server we are monitoring daily. This is the actual bandwidth consumed by the bots as they check in with the controller and receive commands. This data is based on a sampled view of traffic, and shouldn't be treated as hard numbers, but can give you an idea of the rates of usage involved in running a botnet.

Daily DDoS Attacks



Our malicious activity monitoring includes insight into distributed denial of service (DDoS) attacks launched by various botnets around the globe. This chart indicates the number of attacks seen each day across a subset of our monitoring infrastructure, giving some insight into trends and patterns in miscreant activity.

Decentralized botnet command-and-control architectures, loosely coupled links between the bots enable communication within the botnet and provide the basis for its organization. A common term for this class of botnets is peer-to-peer botnets. The knowledge about participating peers is distributed throughout the botnet itself. Consequently, information about the whole botnet cannot be obtained directly, and commands have to be injected into one peer of the botnet. Usually, this is either realized over the communication protocol directly or via the update functionality. In the latter case, bots will exchange their revision number upon communication and, if these vary, the older bot is updated to the version of the new bot. In doing so, a revision is propagated through the botnet over time. The insertion of such updates and commands into the botnet usually happen from an arbitrary point, making localization of the botmaster almost impossible. This provides a high degree

of anonymity. Monitoring its activities or following such a new release through the network is very difficult. [Detection, Measurement, Disinfection & Defence, by the European Network and Information Security Agency (ENISA), Fraunhofer FKIE, and University of Bonn, Germany]

Botnet can use covert channel within other common available Internet technology and services, such as Instant Messaging (IM), Really Simple Syndication (RSS) or social networks. The motivation behind the use of these existing infrastructures is an implicit guarantee of network stability, because the providers maintain their legitimate services. Furthermore, these services require low verification of identity when considering initial registration and can be exploited for indirection of control flow. It can be assumed that almost every Internet-related technology is under investigation by criminals in search of tools for botnet operations. [Detection, Measurement, Disinfection & Defence, by the European Network and Information Security Agency (ENISA), Fraunhofer FKIE, and University of Bonn, Germany]

Events demonstrate the significance of botnets as a threat to national security as, for example, the botnet-driven attacks against Estonia in 2007, against Georgia in 2008, and Iran in 2009. [Detection, Measurement, Disinfection & Defence, by the European Network and Information Security Agency (ENISA), Fraunhofer FKIE, and University of Bonn, Germany]

Botnet Economics. Selling malware can also be divided into multiple stages of a supply chain, including malware distribution services or botnet or crimeware construction kits. In this case, another layer is introduced into their business, providing additional anonymity for the developers. For some botnet creation kits, service level agreements exist, mainly targeting updates and patches. Even botnet services featuring telephone support has been detected. The direct customers of the malware supply chain are botmasters or bot-herders. Use of botnets requires a far lower level of technical skill than the development of malware. Many construction kits are well documented and have a graphical user interface. Botmasters control the bots, work on the expansion of the botnet, and use the botnet to generate profit. Services, such as the maintenance of botnets, command-and-control servers or bots, are all available for purchase through underground communities. Further generation of profits comes from offering botnet services to third parties. Illegitimate control of as many as hundreds of thousands or even millions of remote computer systems, usually with the highest privilege levels, provides botmasters with enormous computing power and bandwidth capacity for use as a business asset. The infrastructure bundled into a single botnet is worth several magnitudes of the initial effort needed to acquire them through malware. Indeed, botnets have various characteristics in common with regular cloud computing, such as heterogeneous resources, decentralised scheduling of commands or network overlays, and resilience and mechanisms for failover. [Detection, Measurement, Disinfection & Defence, by the European Network and Information Security Agency (ENISA), Fraunhofer FKIE, and University of Bonn, Germany]

An ITU report, giving an overview of financial studies about malware, presented numbers ranging from $US13.2 billion for the global economy in 2006 to $US67.2 billion for US businesses alone in

2005. Consumer reports estimated direct costs to US citizens of malware and spam at $US7.1 billion in 2007. The cost of click fraud in 2007 in the US was estimated to be $US1 billion. While the number of malware samples has been increasing at an exponential rate over the last few years, Computer Economics has measured a declining worldwide impact of malware attacks on businesses, with financial costs of $US17.5 billion in 2004, $US14.2 billion in 2005 and $US13.3 billion in 2006. [Detection, Measurement, Disinfection & Defence, by the European Network and Information Security Agency (ENISA), Fraunhofer FKIE, and University of Bonn, Germany]

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]

Symantec published a graph that depicts Attack Kit evolution timeline.

The growth in the number of samples is symptomatic of the widespread application of the concept of polymorphism to binary malware files. Polymorphic malware contains a fixed code sequence that modifies the malware binary code during propagation but remains unchanged itself. Metamorphic malware is changed fully within every propagation attempt. [Detection, Measurement, Disinfection & Defence, by the European Network and Information Security Agency (ENISA), Fraunhofer FKIE, and University of Bonn, Germany.]

Botnets are a global phenomenon and Canada is no exception. Whether the domestic issue is terrorism, organized crime or integrity of government, botnets play an increasingly important role.

Last Year 2010

Bell Canada's **2010 national cyberthreat** report was derived from a network sample of 839 petabytes[13] of anonymous communications traffic examined over the period of a year. Detailed threat analysis was performed on a malicious traffic sample size of 200 Petabytes. In addition to a case study of botnet activity during Vancouver's 2010 Olympic Games. The 2010 report represented the largest statistically valid sample set of cyber threat activity in Canada to date, upon which leaders can rely on evidence-based decision-making to combat botnets and their controllers.

In the course of this study, there was evidence found of extremely large distributed denial of service attacks, sophisticated foreign controlled robot networks, spynets and high volumes of cybercrime in Canada, which led to the estimate that 5-12%[14] off all computers in Canada are compromised and are actively part of a botnet. Similar estimated have been publicly presented by McAfee, Symantec, Trend Micro and Microsoft.

Conductance of Risk

Previous research found that the velocity and magnitude of evolving risks propagated through cyberspace is a function of connectivity and conductance through critical infrastructure interdependencies and their risk conductors. Cyberspace is the nervous system that binds all critical operations. Quantitative research shows that telecoms is a super-critical infrastructure – as important to public safety as electricity.

Attack Vectors and Inadequate Safeguards

Cyberspace is expanding beyond billions of computers and other Internet-aware devices, all of which are highly exposed to hijacking-malware that can assimilate them into a larger criminally controlled robot network. The Internet is on the brink of exploding in size with the roll out of wireless 4G devices and now IPv6.

Unfortunately there are many different attack vectors that can be used to infect a host. A host can be infected by a malicious link embedded in a web page or email or by downloading and executing a maliciously crafted file or through an infected USB stick into a computer like Stuxnet, or by simply accessing the Internet.

"Foreign governments preparing sophisticated exploits like Stuxnet, cyberattackers have targeted critical infrastructure." - **In the Dark - Crucial Industries Confront Cyberattacks**, McAfee's second

[13] Peakflow metadata sample with no PII collected.

[14] 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).

annual critical infrastructure protection report written with the Center for Strategic and International Studies (CSIS), May 2011.

"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."*

Most of the attack vectors are based on zero-day exploits, which have not been identified or remediated by the application or security product vendors and can infect even a well protected host. Furthermore, once infected, the host will download bot agents that resist detection and continue to morph in order to evade updated signatures by anti-virus and firewall vendors, or simply disable AV capabilities on the host. These kinds of infections can only be detected by observing the bot agent behaviour, which is characterized by mass port scanning over all possible network addresses and "beaconing" or attempts to communicate with the botnet command and control (C&C) servers. The C&C servers also employ counter detection capabilities such as rapidly changing domain names and IP addresses to conceal their activities but this behaviour can be monitored as well and can be used to track down and neutralize the servers and hopefully bring their human controllers to justice.

Most organizations use standard security architecture practices to secure their networks. However, as shown conclusively in the 2010 study, there is still a considerable amount of botnet traffic that can be seen going to and from corporate networks. The way and means in which organizations manage the security of infostructures must fundamentally evolve to include the carrier cloud.

Cyber- Intelligence led decision making

"You can't manage what you don't measure."

Timely and accurate information becomes critical in the fight against advanced persistent threats (APT). There are many excellent sources of cyber intelligence and these can be used to identify the infected hosts and the C&C servers. However, the task of gathering intelligence is difficult one, which must contend with often outdated legislative and economic models.

The APT interdiction strategy outlined in the 2010 Bell-SecDev Botnet report addresses the aforementioned issues. Information sharing is, therefore, a critical component of botnet defence as no single agency, has the complete picture of threat activity. Thus, private/public partnerships within Canada and internationally are requisite part of an effective botnet interdiction strategy. In addition, information sharing will assist in identifying potential victims in advance of harm being done.

The 2010 report also demonstrated conclusively that a proactive cyber defence is the most effect strategy to employ against the botnet threat. In order to safely and effectively combat criminal botnets, a fundamental business transformation is required involving people, processes, technology and culture. Based on these key areas, this study outlines a strategic roadmap to achieve discrete tactical successes in the areas of integrity of systems, support for infrastructure and, ultimately, fighting cybercrime.

Current Situation Report

"Organized Crime employing miscreants and spies with the assistance of evil Multinational corporations and bullet proof ISPs operating with the duplicity of Nation State espionage programs. Militaries are already fighting in the 5th dimension … and, of course, terrorists/extremists trying to radicalize everyone on the Planet when then aren't blowing themselves up." – 5th Dimension Warfare briefing, Bell Canada, 2011.

In 2011, Foreign Information Communications and Telecommunications (ICT) Industries and cyber infrastructures are suspected to be used as platforms by Hostile Foreign Intelligence Services (HoIS) for e-spionage purposes. Similarly, for-profit Signals Intelligence networks are becoming more common and harder to distinguish state programs from organized crime networks. Although motives may vary, means and methods share a certain commonality. The lines between state sponsored espionage, cyber-crime, competitive intelligence and hacking are becoming blurred, even to the threat agents. Offensive operations can be outsourced, distributed and coordinated without any of the participating parties being fully aware of the whole picture or end objective, such in the case of Stuxnet. Similar levels of sophistication are seen whether the attack is criminal or espionage in purpose. Dual-use exploits such as the Zeus botnet are typical when we reverse-engineer technology and intent. This assertion is based upon a number of investigations that pinpointed the source of attacks to servers and individuals with links to both criminal organizations and nation states.

"We found accelerating threats and vulnerabilities. For the second year in a row, IT executives in the critical infrastructure sector told us that they perceive a real and growing cyberthreat. Extortion attempts were also more frequent in the CIP sectors. And 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.

Critical infrastructure sectors in Canada and the USA are being actively targeted by both criminal and suspected state entities. Attacks are becoming more bodacious:

"The Nasdaq Stock Market, was breached over the past year, Nasdaq OMX found malware on a part of its network called Director's Desk. Some of the evidence points to Russian computers or proxies." - The Wall Street Journal

An unclassified 2009 report *Economic Warfare: Risks and Responses* commissioned in early 2009 by the Pentagon's Irregular Warfare Support Program - which prepares U.S. government and military agencies for emerging non-traditional threats, states that "a three-phased attack was planned and is in the process against the United States economy. Jihadists or countries such as China may have cost the global economy $50 trillion in a series of co-ordinated strikes against the U.S. economy." The

report claims two unidentified traders deliberately devalued trillions of dollars' worth of stocks at the height of the crisis. "There is sufficient justification to question whether outside forces triggered, capitalized upon or magnified the economic difficulties of 2008," the report says, explaining that those domestic economic factors would have caused a "normal downturn" but not the "near collapse" of the global economic system that took place. This uncertainties and speculation around this report emphasises the need for better capabilities to collate financial and cyber intelligence metrics using an advanced data fusion platform supported by a skilled team of analysts.

Cyber warfare is asymmetric, agile, manoeuvrable, synthetic, and irregular – Bell Canada briefing to DND, 2009

The reported cost of downtime from major attacks exceeds U.S. $6 million per day. More than half of the executives surveyed said they had experienced "Large-scale denial of service attacks by high level adversary like organized crime, terrorists or nation-state. A majority believed that representatives of foreign governments had already been involved in such attacks and infiltrations targeting critical infrastructure in their countries. In 2007, McAfee's annual Virtual Criminology Report concluded that 120 countries had, or were developing, cyber espionage or cybe war capabilities. [In the Crossfire Critical Infrastructure in the Age of Cyber War, McAfee 2011]

Many of cyber incidents leading into 2011 are the result of advanced targeted and persistent threats from multiple sources. Pursuing one investigation typically uncovers a multiple threads and actors. Further analysis yields a web of second/multi-order interrelationships between threat actors and exploits. What is becoming more evident is that there have been systemic campaigns from foreign sources against Canadian critical infrastructures, financial, telecoms, defence and government.

It is our experience that, if something looks bad, and you go into investigate, you are not going to like what you find. While conducting our own investigation, the more we looked, the more we found. One lead spun another thread. Organized crime, espionage, terrorism, insiders; it was all there. Any organization that contests that they are not penetrated is simply not looking hard enough.

Canada is among the most cyber-enabled countries in the World, presenting a disproportionably rich and attractive target. Additionally, Canada's relationships and cross-border critical infrastructure interdependencies provide a conduit for risk and transference of toxic content.

Of the 3 million pieces of malware we analysed, only 1% was targeted. What makes the task of security more daunting is that sophisticated targeted operations are masked by the noise of broad-band cyber attacks, which are becoming sophisticated in of themselves. One of the most serious threats is posed to organizations is by hostile foreign espionage programs enabled by trans-criminal organizations and facilitated by multinationals corporations.

Bell has been actively involved in a number of investigations and deep-dive research project involving critical infrastructures and the pragmatic implementation of a nation-wide cyber security strategy. Similar published cases of e-spionage and 5th Dimension Warfare include: Night Dragon, Aurora,

Ghostnet, Shadows, Titan Rain, Strom Worm, Zeus, and Stuxnet investigations. Bell Canada's Botnet and Darkspace Studies produced with the Defence Research Establishment provide a comprehensive threat picture and advanced security solutions against the most pernicious of these threats.

Global Threat Intelligence

In an ever more networked world, the cyber vulnerabilities of critical infrastructure pose challenges to governments and owners and operators in every sector and across the globe. [In the Crossfire Critical Infrastructure in the Age of Cyber War, McAfee 2011]

The 21st Century has seen the weaponization of cyberspace, and the arms brokers are not the defence industry - it is organized transnational crime. We now see the largest state-sponsored cyber attacks subcontracted to criminal syndicates. In this melee, the critical infrastructure sectors are the ones fighting on the front lines, with consumers caught in the cross-fire.

Critical infrastructure owners and operators report that their networks and control systems are under repeated cyberattack, often from high- level adversaries like foreign nation-states. Assaults run the gamut from massive DDOS attacks designed to shut down systems all the way to stealthy efforts to enter networks undetected. Although attribution is always a challenge in cyberattacks, most owners and operators believe that foreign governments are already engaged in attacks on critical infrastructure in their country. Serious cyberattacks are widespread. [In the Crossfire Critical Infrastructure in the Age of Cyber War, McAfee 2011]

Militaries have not built their own weapons for quite some time. The commercial sector manufactures and sells weapons. In cyberspace, sophisticated weapons can be created by one person and a computer.

Computer Network Operations (CNO) is for sale. Consider that it may take 4 people, 4 months and less than $1 million to build a country-destroying 1 million machine robot network. It is even cheaper to rent one. This is not theory, it is best practices.

State-controlled telecommunications and financial infrastructures form some of the most powerful SIGINT platforms on the planet. Our enemies don't have privacy, regulatory compliance, mandates or laws to impede them. They are learning through experience. These countries are acquiring technology through overt means. They can also press into service their manufacturing sector to shape new technologies and software, which finds its way into our computers. Consider that, much of the information about Canadians and Canadian information is accessible from foreign servers or fortuitous intercept points or off-air or from space. Trusted connectivity and digital rights management are more important than ever. Unfortunately, many organizations treat their Internet services as a commodity and apply tradition security controls based upon a perceptual ambiguity regarding the real risks.

Generally ISPs very much have the mentality that we just haul traffic." said Adam Rice, chief security officer of Tata Communications, the world's largest wholesaler of internet service. "If you pay for the [mitigation] service, we'll kill [a DDOS attack] before it gets to you, but otherwise providers tend to watch it go by. By acting together, he said, the "tier one providers" —who own and operate the backbones of the global Internet—could do much more technically to mitigate such attacks."

The war on terrorism has made full use of kinetic weaponry. However, bullets have little effect in countering smartly delivered ideology. Cyber-terrorism is covert-communications networks, influence operations, radicalization, recruitment and revisionism. Information peacekeeping is the means of countering semantic level attacks. Where are the information peacekeepers?

Traditional War-fighting vs netcentric warfare

In the 1950's, the primary means of securing automated data processing ADP systems was by Tempest shielding the electronics and locking the computer in a room. Military-grade encryption devices were used when communications was necessary between these hardened centres. This model has persisted for years past its "best before date". Eventually, the pressures of technology and threats precipitated a rapid evolution of secure network architecture in just a few years.

The next solution to come along (currently in practice) consisted of a mix of approved technologies, zoning and point-security solutions codified in policy. Notwithstanding, standards, best practices, policy, and doctrine have always lagged technology and the threat by years if not decades. The security architecture in common use today for enterprise computing environments, has not changed significantly in 20 years. Stuff like Firewalls, Anti-virus, Intrusion Prevention Systems, Data Diodes, Virtual Private Networks, Link Encryption, Identify Management, all refurbish old ideas with new technology.

Consider that, thousands of years of Warfare have taught us that disruptive technologies and tactics require complete fundamental change. Armies who persist in holding on to tradition too long are often defeated in dramatic fashion. Medieval knights in full armour succumbed to the cross-bow. The musket was perceived as dishonourable by the Samurai who preferred to bring a sword to a gunfight. In China, the "Righteous Fists of Harmony" believed that Chi Energy and their Kung Fu would stop bullets in the Boxer Rebellion of 1900. This strategy did not end well. Eighteenth and 19th century armies dressed in bright bold colors and elaborate uniforms to intimidate the enemy, promote unit cohesion, and permit identification in battle. They also lined up in an open field and were subsequently mowed down by gun fire by their enemy camouflaged in the tree line.

Post WWII Western armies organized themselves around fighting the Combined Arms Armies of the Warsaw Pact in the European theatre of operation. In the mid-1990's, the defence departments still taught its officers tactics based around a fictitious Canadian Corps-level force pitted against Russia and East Germany. Incredulously, this doctrine was active after the Berlin Wall fell (in 9 November 1989) and while we were engaged in the Gulf War against the Iraqi, not Russia.

Why are these military examples relevant to cyber security? All real-World events have an echo in cyberspace. Conversely, as the Internet grows in importance, the more profoundly it will affect the physical World. Human nature, conflict and security trends carry-over and play out in cyberspace.

In 2009, we are fighting an asymmetric threat of extremist religious fundamentalist groups and their ideology. Computer security has been preoccupied with hackers since the 1960's, but has been largely unresponsive to the rise of state-sponsored programs in the 1990's and the current dominance of this threat landscape by organized crime. Meanwhile, terrorists have competitive advantage conducting influence operations. Yet, most enterprises are using anachronistic models to meet these contemporary threats – building better knives to bring to a gun fight.

Firewalls and intrusion detection systems are not necessarily obsolete, but your security posture it depends more on how you use safeguards, interconnect them, and where you place them in the architecture.

We now know quantitatively, and with a high degree of precision, just how effective (or ineffective) are traditional enterprise security architecture and IT security standards used today in the public and private sector.

Traditional Enterprise Security Architecture, policies and standards are only 20 per cent effective at preventing cyber attacks from penetrating an organization today. The remaining 80 per cent, requires innovative Security Architecture design, most of which can only be accomplished in the Cloud (at a carrier level or higher). We say this after a year of observing the quantity of malicious

APTs passing through organizational networks undetected. - [Whitepaper Managing Risk in Complex System - Real Time Risk Management in ESA, Bell Canada]

"Only twenty per cent (20%) of the solution is inside the box."

The Perfect Storm is developing in cyberspace; powered by macro effects like technological convergence, globalization, emergence and rapidly evolving threats. Think of global warming in virtual space. Cyber security would be much like consulting the Farmer's Almanac to prepare for severe weather event, without a real-time global threat model. Traditional means of security cyberspace have reached a theoretical limit.

Canada has now experiencing Distributed Denial of Service Attacks of 40Gbps. This is 70x orders-of-magnitude larger than the attacks than brought down the Country of Estonia. DDoS in Russia is commonplace recently peaking at 100Gbps.

Sophisticated trans-national organized criminal syndicates are engaged multibillion dollar heists, a cold war of state-sponsored e-spionage rages and terrorists seek to radicalize our youth in social networking sites and within massively multiplayer online gaming environments. Executive spear phishing tactics compromise corporate data and consumers are being robbed of their identities at an alarming rate.

In this age, the weaponry is incarnated by massive robot networks (botnets) that generate 125 million attacks and have compromised an estimated 1.5 million Canadian computers. Any one of these botnets would rip through the fabric of your corporate network in a heartbeat. It is a time when the annual costs to Canada owing to foreign-launched cyber-attacks currently rival our entire defence budget. But it is barely perceivable, because everyone globally is affected.

The evidence[15] of the threat in Canada is real:

- 29 million zero-day exploits/yr[16]
- 54 Gbps malicious traffic
- Half-a-trillion malicious e-mails/yr[17]

[15] 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).

[16] 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]

[17] 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).

In total, 200 Petabytes of malicious traffic was stopped in the cloud in Canada last year by ISPs alone.[18]

To put this in perspective, 50 petabytes represents the entire works of humankind, from the beginning of recorded history, in all languages.

And this is a conservative estimate, and researchers are encouraged to repeat the experiment using the same methodology and data sources.

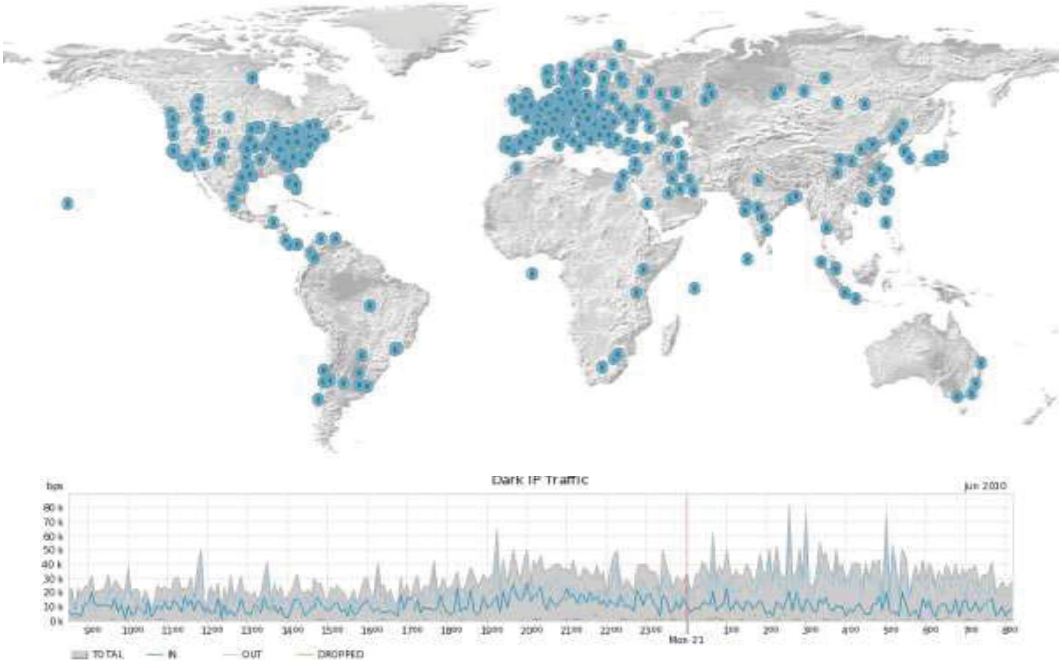
[18] CSTAC

Historical Context to e-spionage and cyberwar

"Information in nature science may be sought through inductive reasoning; the laws of the universe can be verified by mathematical calculation, but the disposition of the enemy is ascertainable through espionage alone." - Sun Tzu 500BC

Espionage has been described as "the second oldest profession, and just as honourable as the first." The practice of intercepting wireless signals existed at the time of the Russo-Japanese War of 1904. The disciplines of electronic warfare (EW) and signals intelligence (SIGINT) evolved over the years. The doctrine of Information Warfare (IW) reached the peak of evolution in 1994, and cyber espionage subsequently emerged in nation states[19]. China and Russia were very quick to adapt the concepts into their arsenal and has evolved throughout the 20th century into the "last, best-kept secret of the state".

Cyberspace has transformed the practice of signals intelligence. Whereas previously, signals intelligence agencies spent billions of dollars building collection platforms that snatched conversations out of the ether - today's cyber spies can rely upon a globally interconnected set of networks, and automated bot nets to systematically harvest information and engage in espionage.



[19] Proactive Cyber Defence and Predicting the Perfect Storm, First Edition Published April 2009

Some states Russia and China regard their telecommunications infrastructure and industrial base as a national asset and use it as a weapons platform to: facilitate foreign Signals Intelligence collection, project foreign policy agendas, perpetrate state-assisted crime, shape the global supply chain, or launch an all-out cyberwar coordinated with a ground battle; as in the case of Georgia and Estonia conflicts.

Chinese executives report a uniquely close level of cooperation with government, as well as high levels of regulation by, and confidence in, government. These figures are striking; they identify China as a leader in government engagement with industry. [In the Crossfire Critical Infrastructure in the Age of Cyber War, McAfee 2011]

But global networks are not the only thing driving the transformation of signals intelligence. Increasingly, espionage is becoming privatized - run by shady networks of contractors, cyber criminals, and privateers. This 'unique' private-public partnership (P3) applies Internet crowd sourcing to espionage and war fighting - enabling the rapid development and deployment of technology and tradecraft. We now find ourselves decisively engaged with foe's that leads with their best offensive line - and one that pays top dollar for top talent.

"The threat sees the network as an asset, not a commodity."

2007 Annual Report to Congress on the Military Power of the People's Republic of China –

"The People's Liberation Army (PLA) is building capabilities for information warfare, computer network operations, [which could] be used in pre-emptive attacks. China's CNO concepts include computer network attack, computer network defence, and computer network exploitation. The PLA sees CNO as critical to achieving "electromagnetic dominance" early in a conflict. The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks."

And China has not been shy in flexing its cyber muscles. In the spring of 2010, China's state-owned China Telecommunications propagated false routing tables from IDC China Telecommunication, which effectively hijacked 37,000 networks, (12% of the Internet) redirecting them to IDC China Telecommunication instead of their rightful owners. These networks included about 8,000 North American networks.[20] A report by the United States-China Economic and Security Review Commission, said the move affected data traveling over both the government and military networks of the United States, including information from the Senate, the Army, the Navy, the Marine Corps, the Air Force, the secretary of defence's office, NASA, the Department of Commerce and the National Oceanic and Atmospheric Administration, as well as from many American companies. It has been postulated that this operation was conducted as either a proof of concept or as a target templating exercise. The subsequent targeted (spearphishing) attacks in 2011 from servers in China required the detailed intelligence gleaned from tradecraft such as DNS redirection. At least, DNS

[20] A Chinese ISP momentarily hijacks the Internet (again), Robert McMillan April 8, 2010

attacks have a good ROI for a threat actor. In March 2011, it was discovered that AT&T facebook users had been redirected through China for some time.

The Problem Set

During the cold war, spy cases were intriguing but not relevant to most folks. It was a war fought in secret between intelligent agencies by cloak and dagger. The average citizen and business-owner could distance themselves from the spectre of espionage.

Cyberspace today most resembles what Hobbes called a state of nature— a "war of every man against every man." Hobbes thought that only government and law could end that war. But in cyberspace, the role of government is more complicated. Globally, a majority of critical infrastructure is in the hands of private companies, which often operate in more than one country. For these companies, governments are partners; they are regulators and policemen; they are owners, contractors and customers; but they are also seen as aggressors, infiltrators and adversaries. The owners and operators of the critical infrastructure which makes up this new battleground will continue to get caught in the cross-fire—and may indeed need what amounts to their own ballistic missile defence. Even when governments assume the role of defender, seeking to prevent attacks and improve security, many IT and security executives are sceptical about their ability to deter or protect against cyberattacks. Forty two percent said that government regulation either had "no significant effect" or actually "diverted resources from improving security." [In the Crossfire Critical Infrastructure in the Age of Cyber War, McAfee 2011]

The role of governments, legitimacy, and Westphalian sovereignty are openly questioned in the context of cyberspace, given the pressures of globalization, extended supply chains, and extra-territorial interdependences.

"The Government's role is still unclear. How are governments responding to the vulnerability of their core civilian infrastructures? In general, they continue to play an ambiguous role in cybersecurity. Globally, industries fear attacks by governments, and more than half of respondents say that they have already suffered from government attacks. Governments also play another, more notorious role in cybersecurity. One of the more startling results of our research is the discovery of the constant probing and assault. Our survey data lend support to anecdotal reporting that militaries in several countries have done reconnaissance and planning for cyberattacks, mapping the underlying network infrastructure and locating vulnerabilities for future attack. Their intelligence and military arms infiltrate and prepare to attack the networks of other countries. During the interviews conducted for this report, the cyberthreat that was cited most often was government-sponsored sabotage and espionage."- **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.

The lines between the state and private enterprises, crime, espionage and 5th dimension warfare are blurred, and why we talk about spys, criminals, independent contractors and warriors interchangeably. We can no longer think of spying as a distinct phenomenon. Nor can we conduct counter-espionage operations in a traditional way. Spying can switch from a criminal vector at the light-speed. E-spionage is an industrial-grade problem that affects everyone insidiously. Most threat actors wear a number of hats. An Eastern European hacker does not make a distinction between white-hat and black-hat.

"In the murky netherworld of cyberspace our notions of hackers, cyber-terrorists, and spies… are deceived by appearances and befuddled by intent. The reality is that the cosmopolitan threat agents of 2010 have compounded agendas and common exploitation tools at their disposal. Although this does not necessarily mean that traditional threat agents have merged organizations nor have established lines communications; in cyberspace that start to look similar, act the same and tread over each others conventional turf. Cyber space acts as a confluence for the threat, and the threat like a collective." – Combating Robot Networks and their Controllers, Bell Canada, Study 06 May 2010.

E-telligence

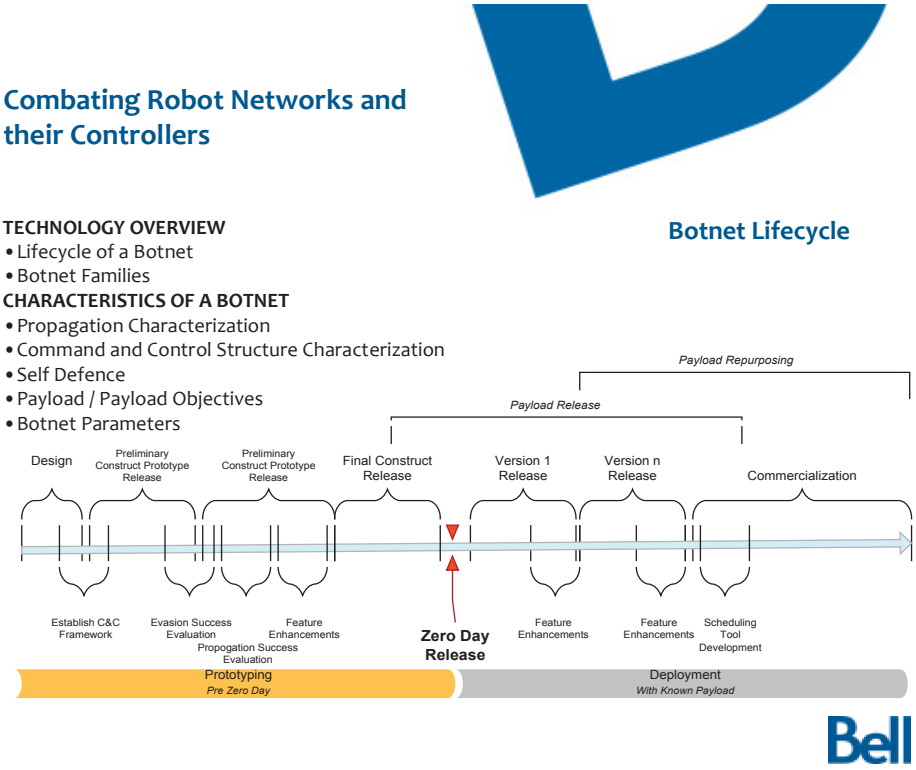
"…a foreign government is believed to have tasked its intelligence service to gather specific information. The intelligence service in turn contracted computer hackers to help meet the objective, in the course of which the hackers penetrated databases of two Canadian companies. These activities resulted in the compromise of numerous computer systems, passwords, personnel and research files of the two companies." - [Economic and Information Security Public Report, Canadian Security Intelligence Service, May 1998]

Conventional misconceptions contend that only nation states possess the sophistication, means, motive and mandate to conduct e-spionage; and that e-spies are only after military secrets.

This is simply no longer the case.

More than half of all the executives surveyed thought their nation's laws were inadequate to deter cyberattacks. There were also doubts about the capabilities of governments to prevent and deter attacks. A startling 45 percent believed their governments were either "not very" or "not at all" capable of preventing and deterring cyberattacks. [In the Crossfire Critical Infrastructure in the Age of Cyber War, McAfee 2011]

Focused targeting and a persistence of attack, rather than technology are the distinguishing features of e-spionage today. Quantitatively, organized crime is by far the most prevalent and resourced threat on cyberspace. The tradecraft and technological sophistication is, for the most part, identical to that of hostile intelligence services. Just look at the sophistication and formal engineering that goes into creating, propagating and controlling robot networks.



It is therefore no surprise, hostile nation states systematically outsource e-spionage and computer network attack (CNA) to national telecommunications providers and indigenous organized criminal groups. [21] Privateering of CNO with virtual Letters-of-Marque provides the state non-attribution and safe harbour for the criminals. E-spionage can hide in the noise generated by broadband use of criminal botnets.

"There is considerable evidence available to substantiate that there is a quid pro quo between Russian authorities and select hackers. The fact that Russian authorities were reluctant, unable to prosecute individuals involved in the politically motivated DDOS attacks against Estonia in Georgia, further substantiate this point. It is easier to outsource this to those that have the expertise, by essentially granting them a letter of Marque that allows them to pursue criminal activities, so long as they're also available to work for the state. This is an increasing problem, exacerbated by the fact that there is no international treaty governing cyberspace, or warfare in cyberspace." – The SecDev Group

[21] Global Network Operations and the Emerging Threat, White Paper, Bell Canada

However, spying and cyberwar does not pay the bills. So, organized crime is left to run the business by economic pillaging using robot networks; all with the duplicity of the state.

"We use computers to send viruses to the West and then we poach your money." - Russian ultra nationalist, Vladimir Zhirinovsky

The BIN (Bank Identification Number) Feed comprises a near-real-time list of bank accounts and credit cards that have been identified by Team Cymru as potentially compromised. This data comes from Team Cymru's unique insight into the Underground Economy.

Foreign e-telligence doesn't just focus on military targets. Increasingly, it is political and economic assets that are targeted. In part, this is a consequence of characteristics of the cyber environment. Systems are now interconnected and data leaks from classified systems to public networks. Moreover, interconnection means that attacks that leverage social vectors - basically the trust people put into relationships with others - can be successful in overcoming even the most sophisticated firewalls and technical defences.

Best-practise secure high-performance network architectures will stop 98% of the malicious activity including a chuck of sophisticated e-spionage threat. An advanced investigative and proactive defensive capability is required to tackle the remaining 2% of the threat. [High Performance Secure Network - Foundational Concepts Reference Architecture and Advanced Investigative Capability, Whitepaper, Bell Canada]

Tradecraft has adapted to take advantage of these soft targets. One characteristic of e-spionage is that it's often carried out by commercial grade botnets which are sophisticated, difficult to detect, and where the deployment cost is close to zero. Intelligence actors can focus on targeting and analysis, and can essentially outsource the collection activity to third parties.

E-spionage will also come at you sideways by compromising your supply chain through the persistent shaping of infrastructure components and the traffic.

On a slightly more sophisticated level, the foreign ownership control and influence of critical infrastructure and the pervasive use of untrusted providers for goods and services such as Internet and telephony, exposes many organizations to e-spionage. Treating critical infrastructure like a commodity is precarious strategy.

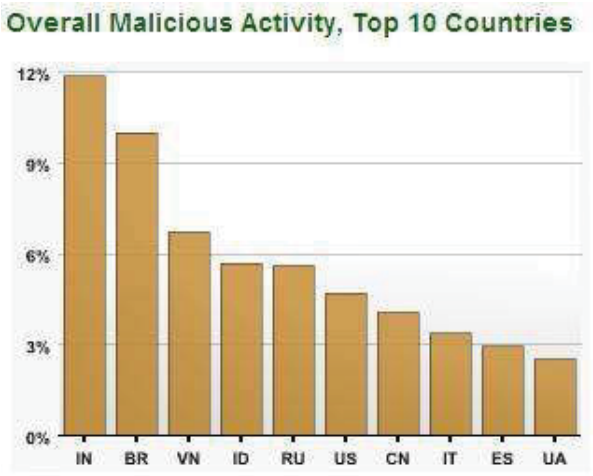
Supply chain security is integral to a cyber security strategy at a national or enterprise level.

A recent investigation by the Information Warfare Monitor uncovered security and privacy breaches affecting TOM-Skype—the Chinese version of the popular voice and text chat software Skype, marketed by the domestic Chinese company TOM Online. TOM-Skype routinely collects, logs and captures millions of records that include personal information and contact details for any text chat and/or voice calls placed to TOM-Skype users, including those from the Skype platform. The report called into question the extent that TOM Online and Skype cooperate with the Chinese government in monitoring the communications of activists and dissidents. [22]

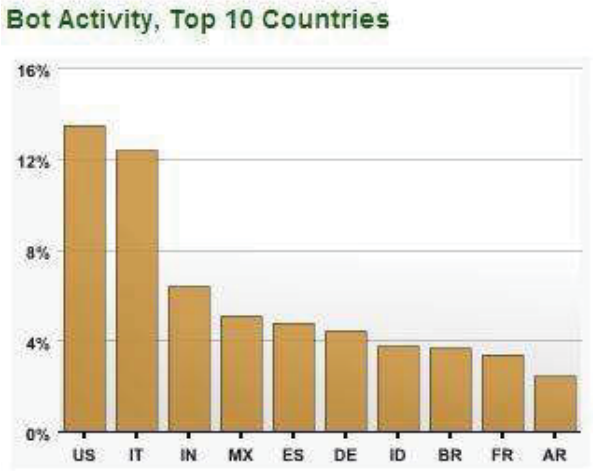
[22] Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform by Nart Villeneuve, Chief Research Officer, Secdev.

The Bad Actors

"Russia, China, India and Cuba have acknowledged preparations for cyberwar and are actively developing IO capabilities…" - CSIS Public Backgrounder No. 11: Information Operations 2004



This chart lists the top 10 countries seen contributing to malicious activity online in the last 24 hours, as a percentage relative to total malicious activity in the same period. IP geolocation isn't perfect, so this data isn't exact, but we believe it should be roughly representative of the current global picture.



This chart lists the top 10 countries seen contributing to botnet activity online in the last 24 hours, as a percentage relative to total malicious activity in the same period. IP geolocation isn't perfect, so this data isn't exact, but we believe it should be representative of the current global picture.

Russia

Russia is one of the clear leaders in evolving and adapting its intelligence practices to the cyber domain. While the remaining largely undeclared, cyberspace operations consisting of sophisticated bot net attacks, denial of service events, and selective use of private communications harvested from cellular phones and Internet vacation, have been used to silence opposition, and shape the politics domestically, and within the Commonwealth of Independent states. These aggressive new

techniques stand in direct contrast to traditional human source methods, which it remained cautious and conservative.[23]

"Russian Military Doctrine has always included the notion of Information Weapons; a fusion of advanced command and control, communications, intelligence systems, psychological and electronic warfare." - Dr. Garigue, 1994

Criminal groups are alleged to be working in cahoots with Russian security forces. Among these, the most often cited is the Russian Business Network (RBN), which has been described as embodying the greatest concentration of evil in cyberspace and is considered by some experts as the most significant deliberate threat to Canadian information infrastructures. RBN offers Internet access, computer network exploitation and attack services to organized crime and state security services alike. Spamhaus calls RBN "the world's worst spammer, child-pornography, malware, phishing and cybercrime hosting networks, providing bulletproof hosting."

Bullet-proof hosting services, Fast-Flux Service Networks and the use of the server-side polymorphism of malware binaries, are techniques for massively disrupting automated malware detection. Encryption is used for the protection of command-and-control traffic or the possibility of digitally sign commands with to prevent takeovers through impersonation. Indicators detectable on the local machine of the threat level of posed by malware include the use of obfuscation techniques to increase analysis time or to stay undetected, and the sophistication used to maintain a presence on the infected system. Malware provides an update, or even a dedicated Pay-Per-Install service, this also provides the possibility of re-infecting the computer system or introducing some other malware in order to prolong its presence. [Detection, Measurement, Disinfection & Defence, by the European Network and Information Security Agency (ENISA), Fraunhofer FKIE, and University of Bonn, Germany]

The RBN's apparent immunity from prosecution in Russia, lends credence to the theory of that they operate under some umbrella of protection by Russian officials, possibly in return for providing capabilities against targets of mutual interest and a platform for e-spionage.

China

The PLA considers *active-offence* to be the most important requirement for information warfare to destroy or disrupt an adversary's capability. Contrast this with some western country' predilection for a strategy of incidence-response and disaster recover. The recent targeted cyber attacks have demonstrated the futility of such a policy.

[23] Proactive Cyber Defence and Predicting the Perfect Storm, First Edition Published April 2009

Gordon Housworth [5/31/2007] writes – *"Informationalization, has entered Chinese military thinking in earnest, affecting both foreign commercial and military assets. US and EU commercial assets have already suffered serious predation from Chinese military assets and Chinese commercial assets operating under military direction. Shifting from 'passive' to active cyberwarfare, the PRC intends to "be able to win an "informationized war" by 2050."*

Operations and Investigations

Lengthy investigations like Titian Rain, Moonlight Maze, and Aurora have uncovered a tangled web of intrigue and skulduggery involving their former cold war antagonists. The Deputy Defence Secretary in a congressional hearing stated "in no uncertain terms that we are in the middle of a cyberwar."

The Botnet Analysis and Tactical Tool for Law Enforcement (BATTLE) by Team Cymru displays IRC and HTTP botnet, crimeware, and phishing data on an interactive world map in near real time. It is intended to provide enough information to enable law enforcement to identify botnets and attacks that are of interest to them.

These 'branded' operations and investigations are part of a grander tapestry having no clear beginning or end, but rather a continuum. There is a clear evolution of attack; a trend to increased sophistication, commercialization and boldness. We also operational and investigative leadership be taken up private sector and academic researchers.

Titan Rain: Titan Rain was the U.S. government's designation given to a series of coordinated attacks on American computer systems since 2003. The attacks were labelled as Chinese in origin, although their precise nature (i.e., state-sponsored espionage, corporate espionage, or random hacker attacks) and their real identities (i.e., masked by proxy, zombie computer, spyware/virus infected) remain unknown. In early December 2005 the director of the SANS Institute, a security institute in the U.S., said that the attacks were "most likely the result of Chinese military hackers attempting to gather information on U.S. systems. Titan Rain hackers gained access to many U.S. computer networks, including those at Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and NASA.

Source: http://en.wikipedia.org/wiki/Titan_Rain

The report Shadows in the cloud: Investigating cyber espionage 2.0 by SecDev Group, Citizen Lab and the Shadowsever Foundation describes a complex ecosystem of cyber espionage that systematically compromised government, business, academic and other computer networks. Data was stolen from politically sensitive targets. The report analyzed the malware ecosystem employed by the attackers, which leveraged multiple redundant cloud computing, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in Chengdu, People's Republic of China (PRC).

Similarly, the Tracking Ghostnet: Investigating a Cyber espionage network investigation discovered over 1,295 infected computers in 103 countries, 30% of which were high-value targets, including ministries of foreign affairs, embassies, international organizations, news media and NGOs. The capabilities of Ghostnet are far-reaching. The report provided evidence showing that numerous computer systems were compromised in ways that circumstantially point to China as the culprit. The report underscores the growing capabilities of computer network exploitation, the ease by which cyberspace can be used as a vector for new do-it-yourself forms of signals intelligence. It serves as a clear warning to policy makers that information security requires serious attention.

"Attribution is difficult because there is no agreed upon international legal framework for being able to pursue investigations down to their logical conclusion, which is highly local." - Dr. Rafal A. Rohozinski, Secdev

Buck Shot Yankee - "The worm entered the military's classified systems when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control" - Deputy Defence Secretary, William Lynn

In 2008, the CENTCOM suffered what has been reported as the worst breach of US classified military networks to date (available in open sources). The attack vector, a relatively low-risk computer virus called Agent.btz (a variation of the SillyFDC worm), entered CENTCOM networks by way of a flash drive attached to a US military laptop in the Middle East. Once installed, the malicious code propagated across classified and unclassified networks gaining access to sensitive information and ex-filtrating data to an unidentified entity. Public sources attribute the breach to a foreign intelligence agency, with some pointing to Russia. DOD responded to the breach with Operation Buckshot Yankee, an effort which targeted poor IT security practices and placed a ban on the use of all USBs. USB ports were disabled and filled with liquid cement. All portable storage device and networks had to be inspected and cleaned. This was a massive undertaking which negatively impacted theater level operations. It took 14 months to effectively purge the networks of Agent.btz. The breach was significant for two reasons:

An unsophisticated and dated virus code yielded significant success for the attacker. The attack vector was unremarkable and posed a relatively low-level threat. Iterations of the malicious code had been in circulation since 2005. Yet it successfully exploited vulnerabilities in DOD's network with alarming ease and speed. The successful attack exposed DOD's outdated and insufficient cyber defence capabilities.

Catalyzed DOD efforts at securing cyberspace. Operation Buckshot Yankee "marked a turning point in US cyberdefence strategy." # It provided the impetus for setting up US Cybercom as a sub-unified command and catapulted cyberspace to a top-tier security issue in the department. In the longer term,

DOD may have benefited from the breach by forcing it to address significant vulnerabilities in cyber defence.

William J. Lynn III, "Defending a New Domain," Foreign Affairs, Sept/Oct. 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

Stuxnet: - A cyber worm dubbed 'Stuxnet' targeted the Iranian nuclear facility at Natanz suggested that, for cyber war, the future is now. Perhaps most striking is the confluence between cyber crime and state action. States are capitalising on technology whose development is driven by cyber crime, and perhaps outsourcing cyber attacks to non-attributable third parties, including criminal organisations Stuxnet is a sophisticated computer program designed to penetrate and establish control over remote systems in a quasi-autonomous fashion. It represents a new generation of 'fire-and-forget' malware that can be aimed in cyberspace against selected strategic targets.

The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target only Siemens Supervisory Control and Data Acquisition (SCADA) systems that are configured to control and monitor specific industrial processes. Stuxnet infects PLCs by subverting the Step-7 software application that is used to reprogram these devices.

Different variants of Stuxnet targeted five Iranian organisations, with the probable target widely suspected to be uranium enrichment infrastructure in Iran; Symantec noted in August 2010 that 60% of the infected computers worldwide were in Iran. Siemens stated on November 29 that the worm has not caused any damage to its customers, but the Iran nuclear program, which uses embargoed Siemens equipment procured clandestinely, has been damaged by Stuxnet. Kaspersky Labs concluded that the sophisticated attack could only have been conducted "with nation-state support."

Source: http://en.wikipedia.org/wiki/Stuxnet

Aurora

Google detected a highly sophisticated and targeted attack on there corporate infrastructure originating from China that resulted in the theft of intellectual property. There was evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. [24]

[24] David Drummond, SVP, Google, Corporate Development and Chief Legal Officer 1/12/2010

"Sources confirm that China's Politburo directed the intrusion into Google's computer systems in that country. The Google hacking was part of a coordinated campaign of computer sabotage carried out by government operatives, private security experts and Internet outlaws recruited by the Chinese government. They have broken into American government computers and those of Western allies." – US Diplomatic Cable, Wikileaks, as reported by the New York Times.

Source: http://www.mcafee.com/us/threat-center/operation-aurora.aspx

Night Dragon: In 2011, coordinated covert and targeted cyber attacks are being conducted against Canadian and US critical infrastructures and governments from China. These attacks have involved social engineering, spear-phishing attacks, exploitation of operating systems vulnerabilities to target and harvesting sensitive information. The Night Dragon attacks work by methodical and progressive intrusions into the targeted infrastructure. These attacks have involved social engineering, spear-phishing attacks, exploitation of Microsoft Windows operating systems vulnerabilities, Microsoft Active Directory compromises, and the use of remote administration tools (RATs) in targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations. We (McAfee) have identified the tools, techniques, and network activities used in these continuing attacks — that we (McAfee) have dubbed Night Dragon — as originating primarily in China. The following basic activities were performed by the Night Dragon operation:

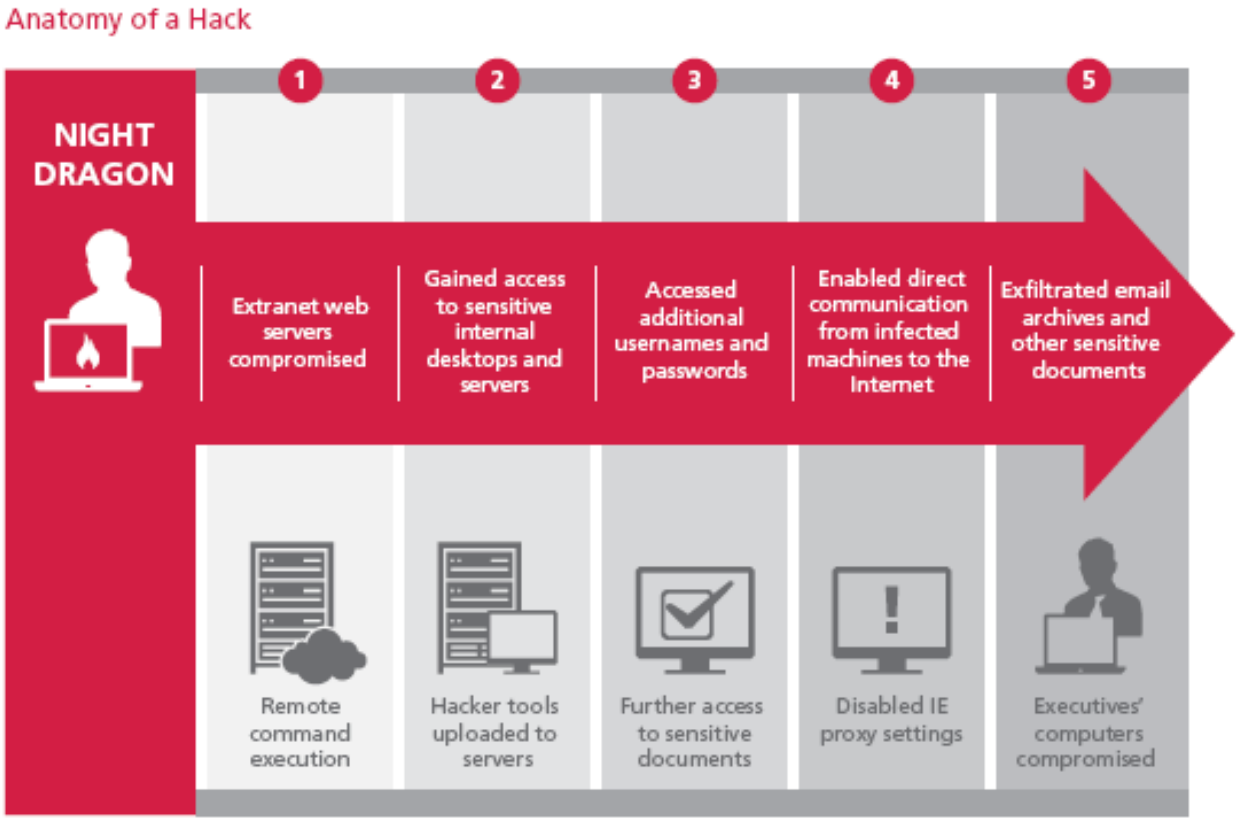
a. Company extranet web servers compromised through SQL-injection techniques, allowing remote command execution

b. Commonly available hacker tools are uploaded on compromised web servers, allowing attackers to pivot into the company's intranet and giving them access to sensitive desktops and servers

c. Using password cracking and pass-the-hash tools, attackers gain additional usernames and passwords, allowing them to obtain further authenticated access to sensitive desktops and servers

d. Initially using the company's compromised web servers as command and control (C&C) servers, the attackers discovered that they needed only to disable Microsoft Internet Explorer (IE) proxy settings to allow direct communication from infected machines to the Internet

e. Using the RAT malware, they proceeded to connect to other machines (targeting executives) and exfiltrating email archives and other sensitive documents.



Source: Global Energy Cyberattacks: "Night Dragon" By McAfee® Foundstone® Professional Services and McAfee Labs™ February 10, 2011

Zeus

In 2009, the Washington Post reported that attackers were able to break into a defence contractor and steal documents pertaining to the Joint Strike Fighter being developed by Lockheed Martin Corp using targeted attacks, known as "spear phishing," Google was compromised in January 2010 along with other hi-tech companies and defence contractors.[25]

[25] Kneber (Zeus) in Depth by Nart Villeneuve, Chief Research Officer, SecDev.

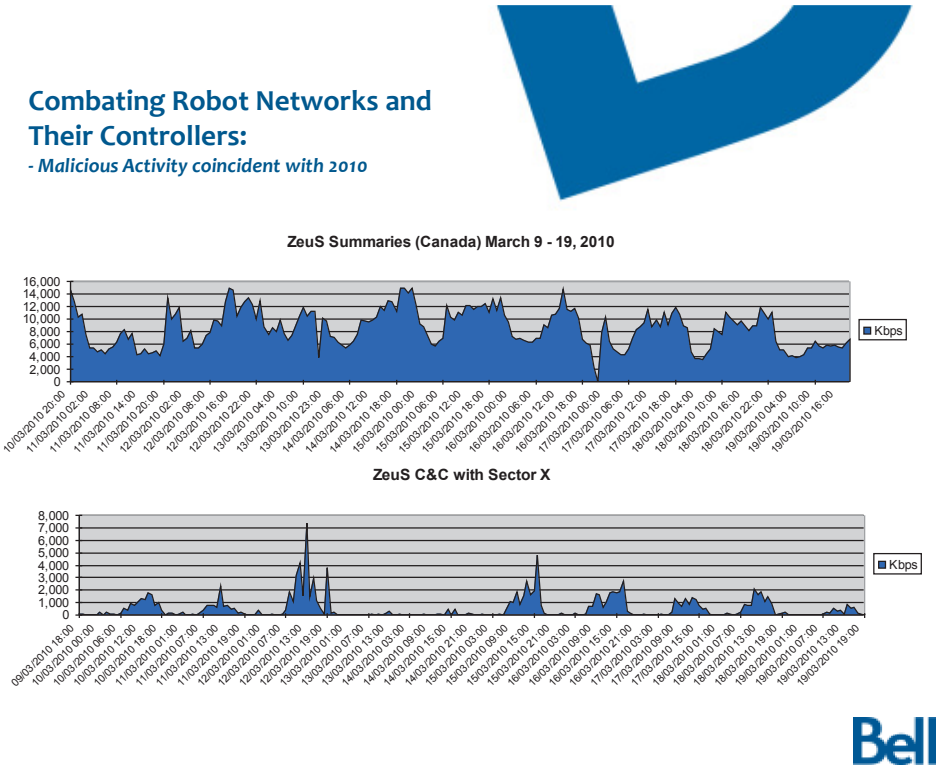
Netwitness revealed the existence of a Zeus-based botnet that had compromised over 74,000 computers around the World where the attackers demonstrated technical sophistication "on par with many intelligence services."

SecDev's investigation confirmed that Zeus was being used to infect targets within the government and military sectors with second instances of malware designed to ex-filtrate data from the compromised computers. The malware downloaded an additional piece of malware on to the compromised machines, which focused on ex-filtrating sensitive documents. The investigation found at least 81 compromised computers that had uploaded a total of 1,533 documents to the drop zone. They found sensitive contracts between defence contractors and the U.S. Military, documents relating to, among other issues, computer network operations, electronic warfare and defence against biological and chemical terrorism. The investigation found the security plan for an airport in the United States as well as documents from a foreign embassy as well as a large UN-related international organization.

On February 6, 2010, Brian Krebs reported that attackers using the Zeus trojan targeted a variety of .gov and .mil email addresses in a spear phishing attack that appeared to be from the National Security Agency, and enticed users to download a report called the "2020 Project." Following the publication of the article by Brian Krebs, attackers took portions of his article and used them as lure in further spear phishing attacks. The malware connected with a command and control server located in China.

The Zeus botnet was highly active, coincident with the 2010 Olympic Games.[26]

[26] Combating Robot Networks and their Controllers, Bell Canada and Defence Research, April 2010



Storm Worm: The Storm Worm (dubbed so by the Finnish company F-Secure) is a backdoor Trojan horse that affects computers using Microsoft operating systems, discovered on January 17, 2007. The Storm Worm began infecting thousands of (mostly private) computers in Europe and the United States on Friday, January 19, 2007, using an e-mail message with a subject line about a recent weather disaster, "230 dead as storm batters Europe". During the weekend there were six subsequent waves of the attack. As of January 22, 2007, the Storm Worm accounted for 8% of all malware infections globally.

Source: http://en.wikipedia.org/wiki/Storm_Worm

Robot Spynets

Cyberspace is expanding beyond billions of computers and other Internet-aware devices, all of which are highly exposed to hijacking-malware that can assimilate them into a larger criminally controlled robot network. Most organizations use standard/traditional security architecture practices to secure their networks. These are inadequate safeguards against advanced persistent threats. As shown conclusively in recent studies[27], there is still a considerable amount of botnet traffic[28] that can be

[27] Combating Robot Networks and their Controllers, Bell Canada and Defence Research, April 2010

seen going to and from these networks. In the course of this study, the evidence was provided of extremely large distributed denial of service attacks, sophisticated foreign controlled robot networks, spynets and high volumes of cybercrime affecting both the public and private sector.

Victimization

E-spionage must be addressed by a proactive pre-emptive strategy. A passive reactive strategy focused on passive-reactive-defence invites cyber attacks. The increased activity in cyberspace by actors such as China and Russia point to an emerging ecosystem in cyberspace; one which requires attention at the foreign policy as well as technical levels. A failure to do so will result an increased exposure and will lead to even more, audacious acts.

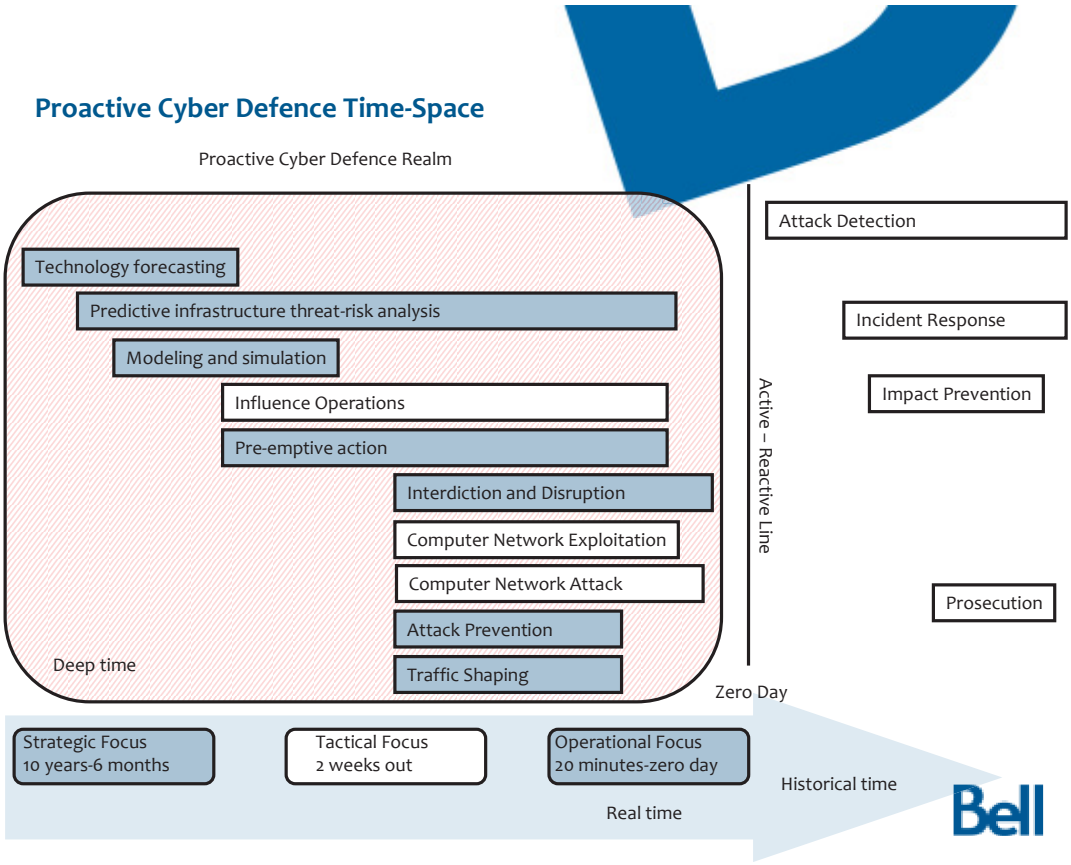
If you act like a victim, you will be played as one.

[28] Cyber intelligence estimates were derived from a anonymized (no PII) network sample of 839 petabytes of communications traffic examined over the period of a year. Detailed threat analysis was performed on a malicious traffic sample size of 200 Petabytes. This represents the largest statistically valid sample set of cyber threat activity in Canada to date, upon which police can rely on evidence-based decision-making to combat the cyberthreat.

How to approach the threat

"Right now, the sheriff isn't there," said retired Gen. Michael Hayden, who recently ended a long career as a senior U.S. intelligence official as the director of the CIA, saying cyberspace was like the Wild West of legend. "Everybody has to defend themselves, so everyone's carrying a gun." But in the cyber domain that was like expecting each citizen to organize their own national defence. "You wouldn't go to a post office and ask them how they're tending to their own ballistic missile defence... but that is the equivalent of the current set-up in cybersecurity," Hayden said.

Ironically, most organizations have invested heavily in treating the symptoms and not the cause. Words like 'react', 'respond', 'recover', and 'restore' are expensive and ineffective alone. Recall that "an ounce of prevention is worth a pound of cure".



Predicting and interdicting an attack before it occurs, provides far more and better options at lower cost, than detecting and reacting to an impact. Prior to every major cyber security incident in Canada there have been early warning signs and opportunities to act. However they have ended up costing Canadians billions owing to the subsequent measurable impacts.

"Preventing a threat event before it happens" is much more difficult. Scenes from the movie, Minority Report come to mind, where the 'precogs' foresee incidents and events with enough lead-time for authorities to intervene. The disturbing ramifications are that people are punished for crimes that they did not yet commit. Similarly, the ubiquitous surveillance depicted in the film 1984 is unnerving in this day and age.

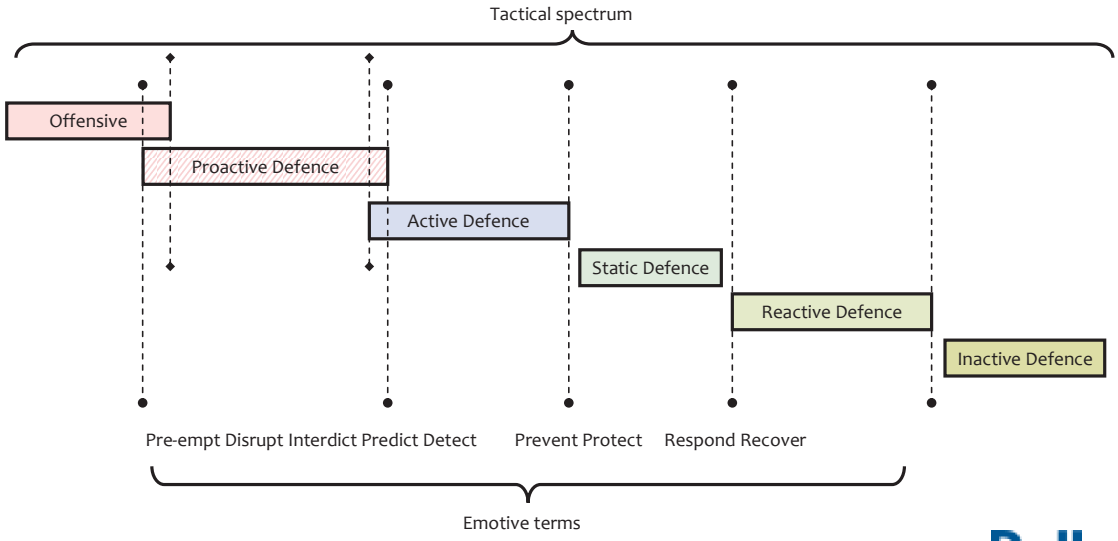
No one is suggesting that we employ such intrusive surveillance, nor are we advocating, you will be happy to know, pre-cognitive enforcement and punishment. What is promoted, is intelligence-led proactive defence that interdicts, disrupts, pre-empts and thus prevents emerging threat intent. Not only is this possible, but it is necessary today. No PII is required to make this happen.

So how do we begin to act, rather than react, to emerging threats?

First we must acquire accurate intelligence upon which scarce resources can be deployed most efficiently against developing threat-vectors. Such situational awareness is developed from sciences, technological forecasting, social trending, environmental scanning, threat analysis and modeling. We need to take a serious look at the evolving World in which we live, and understand that the threat agent is subjected to the same trends as are we.

Deliberate threat agents adopt the new technologies early. Consider the early and rapid spread of cell-phones and pager use amongst the youth. This was a strong indicator of the resulting illicit activities by that demographic. The common trend is that criminals will own a technology legitimately, then use it to facilitate crime, and finally exploit the technology itself. By understanding the effect of introducing disruptive-technologies into society, and envisioning their criminalization, one can effectively predict the early development of a threat. Such accurate strategic forecasting buys police time and precision.

Mind map of the proactive defence



Bell

But how does one establish means, motives and marks in a target-rich and threat-heavy situation? Risk assessments that integrate the source and means of the threat ("threat-from") and the recipient target of this threat ("threat to") play a crucial role in 'precognition'. They can establish "threat-vectors" from source to recipient with greater degrees of certainly. When John Dillinger was asked why he robbed banks, he answered "that is where the money is." Often authorities are too busy chasing the bad guys, when guarding the cyber-gold could save a lot of time and money. This seemingly trivial analogy nevertheless clearly underlines the merit of a "threat to" risk analysis.

The "threats-to" approach begins by identifying potential targets of the threat; the intrinsic vulnerabilities of the asset and its potential exposure to these threats. It is complementary to a "threats-from" analysis and has the advantage of being a more selective examination of threats based upon a given target system. The disadvantage of a "threats-to" approach is that it is reactionary and provides little warning of threat activities, intentions or trends. Nonetheless, if John Dillinger was robbing today, he would exploit cyberspace, because that is where the money is. Today, all money crime has a direct or indirect connection to cyberspace. Illicit micro-banking transactions are more likely to occur in a virtual gaming environment than on a street corner. Authorities need to be just as street-smart in cyberspace as they are on the traditional beat.

Threat events and agents can be examined without immediately linking them to an incident or victim. It is common practice for security and intelligence services to gather information on potential groups that have demonstrated potential to precipitate an attack. This analysis is useful from a security preparedness point-of-view, and to focus investigative efforts to head-off an incident. The analysis involves examining motives, means and methods of a threat agent surrounding a potential threat event. A "threats-from" analysis is performed from within the threat milieu as a proactive step to mitigate the risk by addressing the threat directly. The disadvantage of a "threats-from" approach is its focus on traditional threats-agents-events at the expense of emerging threats and new trends in targets.

A vector is a measurement of direction and magnitude. Direction requires both a start and end point. There is often a gap in the intelligence coverage linking "threats-to" and "threats-from" evidence - but a good investigator needs to connect the dots to deduce a threat vector.

Understanding the World of threat-agents is also important when forming a predictive analysis. A "risk-to" or "vulnerability weighted" perspective to threat analysis suggests static protective safeguards to mitigate perceived exposures. “Threats from” has a more significant bearing on the "predictive" risk analysis in contrast to the "historical or empirical testing". It is a better indicator of what detection and response mechanisms should be added.

Risk assessments that do not examine threat agents and their victims cannot be predictive or proactive. They present but a snapshot in time. Without accurate threat agent information, an assessment cannot determine the magnitude of exposures particularly in this dynamic threat environment.

There is interdependency between a threat and its victim. Two entities are known to be interdependent when they exchange or share: goods, services, communications or geographic proximity. The interesting prospect is that all these metrics are measurable, and, if we can model it, then we can predict it. You have heard the aphorism “follow the money.” Well, consider that, these days, the phenomenon of convergence converts paper cash into electronic funds transfers and places it over the Internet along-side communications. Monetary, communications and geospatial metrics lend themselves well to surveillance technologies. This allows authorities to regain the advantage over evolving cyber threats.

It is impractical to uniformly implement security safeguards and exercise all scenarios across large and complex systems at the highest levels. This is particularly pertinent when countering trans-national criminal organizations or state-sponsored information warfare. This would raise the business risk associated with the programme to unacceptable levels.

But these sciences are still reactive, albeit faster, to the threat’s intentions, and do little to shape a threat’s behaviour. What is it that authorities can do to interdict, disrupt and pre-empt widespread identify theft, banking fraud, espionage and attacks against critical infrastructures when they are perpetrated by networks of robot-armies controlled by organized crime syndicates operating abroad with the duplicity of foreign states?

Home-grown terrorism, domestic extremism and radicalization of our youth manifest themselves over time on the Internet in manipulative relationships with undesirables. The only message that is being heard is that of the militants. Authorities are often called upon when things have gone dangerously wrong, and the only option left is arrest. Early detection of burgeoning threat activities is required without interfering with privacy rights. The authorities must first understand the Internet-based landscape. Secondly, a strong communications plan and viral marketing can be used to counteract the toxic messaging to the victims. Thirdly, influence operations should be considered to shape the behaviour away from crime.

We must be willing to conduct proactive, pre-emptive operations (P2O) in Cyberspace to shape behaviours and avert the development of malicious intent. Enforcement, when required as a final solution, will need to be global and coordinated across critical sectors and boundaries.

Internet Service Providers should be more strongly incented to make use of their position as an access channel to the Internet for their customers and to use their special position for detection efforts. Regulators should intensify their efforts to modernize existing legal frameworks and their interpretation on a national level in order to create a practical basis for dealing with different aspects of cybercrime. The balance between, on the one hand, laws for the protection of privacy and data protection of users and, on the other, the protection of Internet security and the stability of critical infrastructures. [Detection, Measurement, Disinfection & Defence, by the European Network and Information Security Agency (ENISA), Fraunhofer FKIE, and University of Bonn, Germany]

Shuns and Stuns

Until quite recently, this "bag 'em and tag 'em" approach to dealing with malicious activity online had become so ingrained in the security community that most of the thought leaders on security were content merely to catalog the Internet's worst offenders and abide the most hostile networks. Exponential increases in the volume and sophistication of new threats unleashed during the past few years—coupled with a pervasive attitude that fighting criminal activity online is the principal job of law enforcement—have helped to reinforce this bunker mentality. Then, in the fall of 2007, something remarkable happened that seemed to shake the security industry out of its torpor: concentrations of cybercrime activity at a web hosting conglomerate in St. Petersburg known as the Russian Business Network (RBN) caused the ISPs serving the infamous provider to pull the plug. The RBN, which had been a vortex of malicious activity for years, was forced to close up shop and, subsequently, scattered its operations. [Takedowns: The Shuns and Stuns That Take the Fight to the Enemy, By Brian Krebs]

A "shun" occurs when the Internet community effectively ostracizes the problematic network. Shunning involves providing ISPs serving the target network with precise information about the nature and concentration of the illicit activity. On November 11, 2008, I sent a package of incriminating data to two upstream providers that served McColo. Fast forward to May 2009, when the Federal Trade Commission (FTC) orchestrated the disconnection of hosting provider 3FN (a.k.a. Pricewert). As a justification for its actions, the FTC cited many of the same complaints leveled against Atrivo and McColo. For example, a large number of the control servers for the massive Cutwail/Pushdo spam botnet had a persistent presence at 3FN. [Takedowns: The Shuns and Stuns That Take the Fight to the Enemy, By Brian Krebs]

A "stun," on the other hand, centers on strategically targeting structural and organizational weaknesses in large botnets, with the goal of incapacitating them and eventually causing their collapse. When the aim is to stun and then dismantle an entire botnet, researchers typically map out as much of the botnet's core infrastructure as possible and then coordinate with hosting providers, ISPs, and registrars to have those components disconnected simultaneously. Stuns are ideally

executed after careful mapping of the target botnet's infrastructure and resurrection networks. But unplanned opportunities to stun a botnet or botnets may present themselves when a web host is shunned by the Internet community. On January 9, the "Lethic" botnet—at the time considered responsible for relaying roughly 10 percent of all spam—was snuffed out as its control servers were taken offline one by one. The takedown was orchestrated by security experts at Neustar, who had coordinated the effort with the ISPs that were hosting Lethic's servers. That success followed closely on the heels of a textbook stun in early November 2009, when researchers at FireEye in Milpitas, California, engineered the death of the botnet alternately known as Mega-D and Ozdok, which was once estimated to have been the engine behind at least 30 percent of the world's spam. [Takedowns: The Shuns and Stuns That Take the Fight to the Enemy, By Brian Krebs]

The Proactive Game

If one enters the proactive defence game, one should understand that it has a rich narrative upon which one's enterprise can capitalize. From 500BC, proactive defence developed as a strategy, coming into the cyber hype-cycle peak of enlightenment in 1994 and reaching a highly mature cyber capability by 2005. Yet, there still exists great disparity in Canada between sectors that possess an indigenous capability of mature proactive cyber defence programmes and those that do not.

Establishing a common operating picture is central to the matter of discussing and deciding upon a proactive cyber defence strategy across Canadian critical infrastructures. Neither technology nor costs have been the principal impediments to successful proactive cyber defence programmes, thus far.

We may not have all the answers, but the way ahead is clear, as the US Cyber Security Strategy has articulated. Effective Private Public Partnerships (P3) are vital in matters of national security, defence, Information Infrastructure Protection (CIIP) and specifically Computer Network Operations (CNO) given that the majority of critical infrastructures are privately owned and operated.

The answer to the e-spionage threat requires a coordinated response.

At a technical level, there needs to be a focus on rapidly engineered 'best' security practices for modern High Performance Secure Networks.[29] The advice goes beyond 'common' policy and standards; which are decades behind advanced persistent threats. 'Air-gapped' corporate networks are no longer safe – everything is connected.[30]

[29] High Performance Secure Network - Foundational Concepts, Bell Canada

[30] Laying Siege to Fortress Architectures, Bell Canada,

The attack vectors used for e-spionage can be closed off by mitigating against broad advanced persistent threats like criminal botnets and their controllers. Corporate architectures should be built on a strong foundation. Trusted Internet Connectivity (TIC), Core Intelligence[31] and 'clean pipes' provided by upstream security[32] are the cornerstones of the US Comprehensive National Cyber Security Initiative (CNCI), the impetuous of which was in countering the e-spionage threat. Traditional paper risk assessments are compliance audits obsolete upon publication. Real-time risk management and adaptive-dynamic enterprise security architectures are the answer.[33]

Engineering a solution to e-spionage must be performed in the context of an integrated risk management framework that considers (and calculates) business imperatives, the Total Cost of Ownership (TCO)[34] for and Return on Investment (ROI) security per dollar spent.

At an organizational level, education and awareness is key. Most spy nets are built by social engineering entry into a network of interest by using a well crafted e-mail harbouring a malicious link or attachment – hence 'executive spear phishing.' There is no technical defence against a well executed social attack, evil memes or 'viruses of the mind' So, downstream, network owners and citizens must be vigilant in opening suspicious e-mails containing links or questionable attachments.

The problem, as other experts pointed out, is that such mitigation activities could be complicated by regulatory and contractual concerns, unless the law provided safe harbour provisions for companies intercepting and diverting malicious traffic. Moreover, providers who operated in more than one national market might face competing or even contradictory legal obligations in different jurisdictions. [In the Crossfire Critical Infrastructure in the Age of Cyber War, McAfee 2011]

[31] Carrier Grade Intelligence, Tyson Macaulay, Bell Canada Jan 7 2008

[32] Upstream security, Tyson Macaulay, Bell Canada , July 6 2009

[33] Real Time Risk Management and enhanced Enterprise Security Architecture, Bell Canada

[34] Total Cost of Ownership for Network Security, Bell Canada

DNS Infrastructure Threats

Domain Name Service (DNS) is the primary control point of any network from enterprise to national critical information infrastructure. DNS is one of the most cost effective means to centrally monitor network activity, detect Advanced Persistent Threats, control and mitigate security risks. It is also the prime offensive target for network reconnaissance, exploitation and attack.

More than half of IT executives reported DNS poisoning—where Web traffic is redirected— with nearly half of those reporting multiple monthly occurrences. Roughly the same number had experienced SQL injection attacks—which hackers can use to gain access to back-end data through a public Web site—again with nearly half suffering multiple monthly attacks. Such attacks also tended to have a more significant operational impact on victims' systems. [In the Crossfire Critical Infrastructure in the Age of Cyber War, McAfee 2011]

October 21st 2002: There was a co-ordinated attack against all 13 root servers simultaneously which lasted for just over 1 hour.

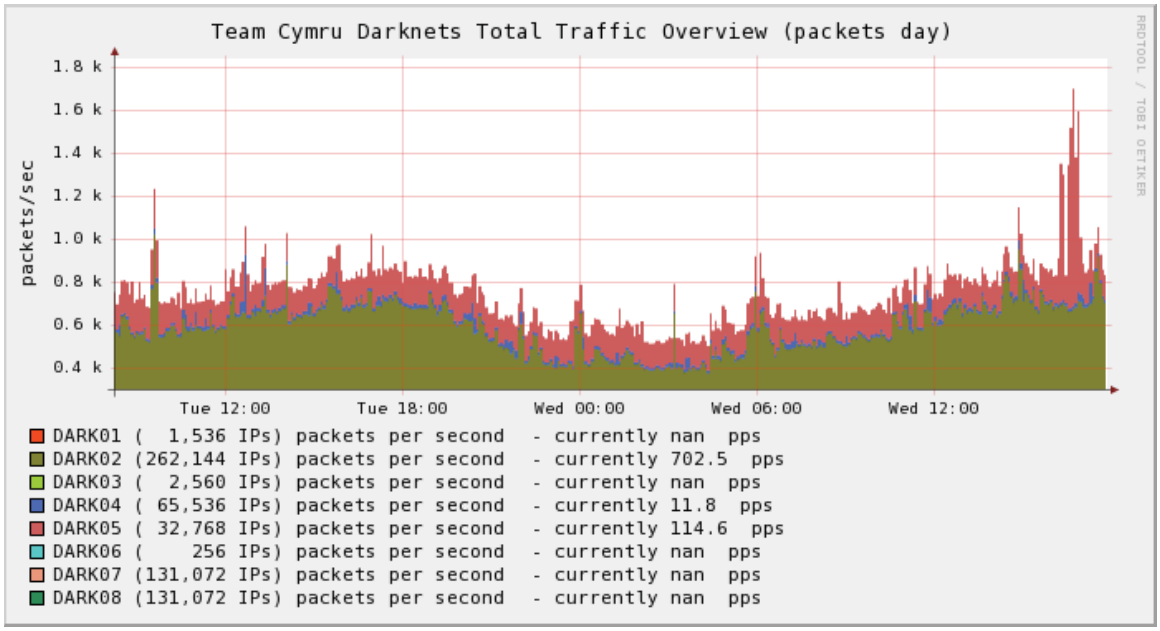
In December 2006, the National Institute of Standards and Technology's (NIST) Special Publication 800-53r1 "Recommended Security Controls for Federal Information Systems" prescribed initial DNSSEC deployment steps necessary for high and moderate impact information systems.

February 6" 2007: An attack originated out of the Asia-Pacific region and targeted 4 of the 13 root servers as well as the .info and .org top level domains. The attack caused disruptions at two of the root servers (g-root and l-root). This was a DDoS attack implemented using a Botnet of between 4000 - 5000 systems; 65% of these were based in South Korea with the rest from numerous other countries. The Botherder was physically located in Dallas, Texas, although the Botnet itself was associated with a Russian reseller. The DDoS attacks lasted through to May 2007.

On August 22, 2008, a Memorandum for Chief Information Officers was issued by the Executive Office of the President that addressed Securing the Federal Government's Domain Name System Infrastructure. The US DNSSEC plan consists of: Enumeration of government Domains, identifying sources of DNS Services and Infrastructure, addressing Barriers to DNSSEC, the creation of a Plan of Action and Milestones for full adoption and piloting a secure DNS Infrastructure. DNS was made a cornerstone of the Comprehensive National Cyber Security Initiative, issued by the President in 2009.

In the spring of 2010: China's state-owned China Telecommunications propagated false routing tables from IDC China Telecommunication, which effectively hijacked 37,000 networks, (12% of the Internet) redirecting them to IDC China Telecommunication instead of their rightful owners. These networks included about 8,000 North American networks including private and public infrastructure in Canada. The likely purpose of the DNS redirect attack was for target templating. Subsequent, sophisticated and targeted attacks were effectively launched against Canadian sectors, which continue to this day.

The Domain Name System (DNS) has an important role, as it allows changes to the C&C infrastructure to be performed dynamically. When DNS is used, the command-and-control server is identified by a (command-and- control) domain name that is resolved by DNS to an IP address. Multiple, successful botnet mitigation techniques aimed at DNS have been applied in practice. An example of this is the deregistration of malicious domain names. However, the worldwide distributed structure of DNS complicates the mitigation process. The principle of Fast-Flux Service Networks (FFSN) is designed to increase resilience and anonymity, and it has achieved significance for several botnets. The idea of fast- flux is comparable to Content Delivery Networks (CDN). When a malicious domain name has to be resolved, a query is usually first sent to the nearest DNS server and then handed through the DNS system to a DNS server controlled by a botmaster. The response to the query will usually include a large number of IP addresses associated with bots. These bots function as proxy servers, forwarding all the client communication to a server, which hides behind the proxy layer. Behind this proxy layer, malicious services like web page phishing, suspicious advertisements, or malware archives for the download of additional modules, can be hidden the DNS response records have a very short period of validity, which results in rapidly changing responses for the same domain name.



A common approach to mitigating botnets is to block malicious domain names. Depending on the DNS service provider in charge, this procedure can require considerable effort. In any case, single domains can be blocked or taken down comparatively easily. This has led to another concept that has been invented for use in botnets, Domain Generation Algorithms (DGA). The idea behind DGAs is to generate C&C domain names (domain names linked by DNS records to C&C servers) depending on

one or more external information sources serving predictable seed values called markers, that can be accessed by bots and botmasters alike. Markers that have been used in this context can be timestamps as well as data from popular websites such as Twitter Trends. While timestamps provide the ability to generate domain names far in advance, the use of dynamic web content eliminates this element of predictability. Hundreds, or even thousands, of domain names can be generated at short intervals. [Detection, Measurement, Disinfection & Defence, by the European Network and Information Security Agency (ENISA), Fraunhofer FKIE, and University of Bonn, Germany]

EVIDENCE AND EXPERIMENTATION

The scientific method demands evidence-based research through experimentation. This chapter validates methodology through forensics and the macro threat picture investigative findings, using deeper analysis on a smaller dataset.

INVESTIGATIVE METHODOLOGY AND SYSTEMS

What is threat intelligence and how does it differ from antivirus research, and security research? Does it represent a new approach to understanding cyber threats, how does it complement and or supplant existing methods?

Background - Antivirus Research

Antivirus programs started out as desktop applications that would scan a user's files, as well as the system's memory and filesystem, and look for infections. File infectors would carry the infection mechanism and payload in an executable file by modifying it, and would rely on a person running the infected program for it to run. Boot sector viruses would copy their payload to the master boot record of a hard drive. Trojan Horse programs, now abbreviated to trojans, are malicious programs that pretend to be something else in order to get the user to execute them. All of these attacks are from files present on a computer, and remain on the computer as files, in the boot record, or in memory.

The way that the antivirus industry has traditionally offered users protection against malicious programs is through signatures. Signature scanning engines run on the user's desktop, searching all files against known viruses by way of fixed strings and other patterns. Antivirus companies have a history of having a very strict code of ethics. There is not a "white hat" / "black hat" / "grey hat" labeling system as there is in security research. Historically, there have been a lot of accusations against antivirus companies that they write the viruses they protect against in order to make money. As a result, antivirus researchers have been very careful to demonstrate that this is not the case. Although these accusations were made a long time ago, and the public now understands the need for antivirus software, many within the antivirus industry still maintain the same restrictions from any research which may be seen as questionable. The antivirus research community is very well-connected, and researchers who use their knowledge to write viruses are quickly blacklisted. [cite] Even when information on how to possibly write malware is released to the public, or a researcher is found involved in other malicious or black hat behaviour, he or she will still likely get exiled from the community. For example, Peter Kleissner was an antivirus researcher who worked for Ikarus Software. He gave a presentation at Black hat on writing a MBR rootkit; as a result, he was forced out of his job and removed from information-sharing resources within the community. [3]

Background - Security Research

Security research is similar to antivirus research in that it covers ways of preventing users from being infected by malicious programs. However, security research covers a much broader range of topics. When looking only at the similar areas of research (preventing users from infection), security research focuses primarily on network-borne threats. Malware is malicious software, which includes viruses. But it also includes many other types of malicious software, including network-borne worms, exploits against vulnerabilities, and phishing applications that mimic real sites in order to harvest credentials.

Malware often uses a network vector for infection. Bugs in computer programs that can be used to compromise security are called vulnerabilities; a working breach in security that comes from a vulnerability is called an exploit. While some programs that compromise security are trojans and require user intervention, malware often uses automated exploits against vulnerable network-facing programs to infect a user's computer. A network-facing program can be either a server or a client program (for example, a web browser). Because of the way client-side programs have become much more complicated, the attack surface for a user's computer has greatly increased, even if only used for "simple" tasks such as web browsing. Browsers have become incredibly complex; a browser may contain code from many different vendors to handle a wide range of tasks. While security research may use signatures (e.g. for IDS/IPS systems), it's a well-known and accepted fact that signatures are not reliable against many threats. The same techniques that are used to make viruses more difficult to detect are also used for malware.

The "rules of engagement" at many security companies differs from traditional antivirus companies. Since network-borne threats need a computer on the other side to communicate with, a researcher investigating live malware networks will be interacting with computers that do not belong to him or her. These computers may be running software specifically for malicious purposes, but may also be user machines that have been compromised and infected. There are many debates within the security community about how to handle incidents that present ethical challenges. One of the most well-known (and longest-running) disagreements is on disclosure: how a security researcher who finds a vulnerability is expected to disclose it, and who to disclose it to. There are three main camps here: vendor disclosure is reporting the vulnerability to the software author and allowing them to handle the rest; full disclosure is publishing the vulnerability details so the entire world can see; responsible disclosure is a combination of vendor disclosure and full disclosure two where the researcher attempts to coordinate disclosure through the company but may release the details if the company is non-responsive. Some "black hats" also prefer non-disclosure; if you don't report a vulnerability, it is less likely it will be fixed, and more systems can be compromised. While the security community has mostly settled on responsible disclosure, the debate is still ongoing. This is especially true when affected companies are non-responsive or hostile towards reported vulnerabilities. Also, a number of black hats have targeted security researchers for responsible disclosure, saying that this

reduces their arsenal of attacks. [Zero For Owned (ZF0) 5 - hosted many places, don't know the original source]

Background - Antivirus Research Versus Security Research

There is currently a good amount of overlap between antivirus research and security research, which is expected due to the overlap in subject matter. "Virus" is often used interchangeably with other types of malware, such as trojans and worms. Traditional AV companies are moving towards heuristics and other technologies to respond to the evolving threats. This move isn't as quick as may be expected, however; most AV engines still mostly rely on signatures.The move is being reflected in the way traditional antivirus companies are repositioning themselves as security research companies with a focus on antivirus. Sometimes these changes are immediately obvious: Symantec's Antivirus Research Center is now called Symantec Security Response. A new product term in the area is "endpoint protection": a combination of an antivirus engine and network scanning services including a firewall and network-based intrusion detection/prevention system.

Some companies that do traditional antivirus research are having ethical issues with the way security research is done. One good example is the case of Roel Schouwenberg, a senior researcher for Kaspersky Lab. He wrote an article about a student project from the University of Michigan called PolyPack, which would take known malware and re-encode it in a way that no antivirus scanners would catch it. [4] The students considered this to be a valid research project demonstrating why signatures are no longer a useful tool in antivirus research; Schouwenberg (as a researcher for a company that primarily uses this technology, whose products missed the malware) said the project was unethical, illegal, and called for the students' expulsion at the very least. While the response against PolyPack was extremely negative from the antivirus industry, it was often positive from security researchers. Gunter Ollman, VP Research of Dambala, a well-known and respected security company, is one of many who wrote a strongly worded response to Schouwenberg. [5] Ollman is of the opinion that the threats will be out there regardless, and having strong tools to test the strength and efficiency of detection and prevention methods is useful. Just because a vendor doesn't like the result against his own company's tools, possibly indicating that his methods are becoming outdated or even just not applicable to all new threats, is not a reason to shut down the research which demonstrates it. In the case of Peter Kleissner, the discussion of whether to remove him from an anti-malware information-sharing community turned into a major debate, with a lot of debate and some lines drawn between antivirus researchers and security researchers. This happened just before Schouwenberg's essay about researchers lacking basic ethics, and likely prompted it. In the end, the decision about Kleissner was much easier due to the other work he had decided to take on after being exiled, tracking whether Virus Total and similar sites had detected new malware. [private emails from the Incidents and Insights list mentioned in Krebs' artice]

What is Threat Intelligence?

A threat is "something that is a source of danger." [1] This includes intentional activity such as systems being compromised or infected with malware, unintentional activity such as a well-meaning user taking the wrong action, and natural risks such as power outages and flooding. Threat intelligence is a combination of collecting information about threats and of the threat agents, which Intel defines as a "person who originates attacks, either with malice or by accident, taking advantage of vulnerabilities to create loss." [2] Unlike general information security, threat intelligence doesn't include subjects such as disaster recovery and business continuity; it focuses on intentional attacks and the actors behind them. Antivirus research is the initial response to malicious software, which started out as scanning the user's files for signs of infection. However, the threats (viruses) already needed to be present before they could be found and removed. Security research involves finding and neutralizing a larger selection of threats, including stopping attacks against user computers in the network, before they reach the computer.

Threat intelligence is research on an even larger selection of threats, including the threat agents as threats themselves. By identifying and understanding the threat agents as threats themselves, instead of only the technology as threats, we can understand and neutralize other threats before they are created. Much like how security research can prevent a desktop infection by stopping the attack in the network, threat intelligence can prevent network threats (as well as desktop threats) before they hit the network. As an example of how threat intelligence can prevent network threats, consider the case of McColo, an ISP that was determined to be hosting a large quantity of malware. Brian Krebs, at the time of the Washington Post, had done some investigation into McColo and determined that it was the staging point for multiple botnets and other malware, and was likely being used primarily for that purpose. In November 2008, prompted by Krebs' investigation, McColo was depeered by its two upstream providers, cutting it off from the Internet. Within one day, spam blocking services (MessageLabs, IronPort) determined that spam levels across the entire Internet had dropped by two-thirds. [6] By investigating the source of the threats, determining the threat agents involved, and going after the bigger threat (the actors themselves), the result was considerably larger than going after any individual malware controller. Threat intelligence isn't a new approach, but its widespread use and effectiveness in information security is the natural next step in combating information security threats. It is not a strict superset of security research, much like how security research is not a strict superset of antivirus research. The focus of each is in a different direction, but there is a lot of overlap. Traditional antivirus research will still be necessary to understand that selection of threats, and the same is true for security research. However, threat intelligence can provide those fields with a lot of useful information to improve the speed and efficiency of research.

[1] WordNet 2.0 definition, from http://www.dict.org
[2] Prioritizing Information Security Risks with Threat Agent Risk Assessment, http://download.intel.com/it/pdf/Prioritizing_Info_Security_Risks_with_TARA.pdf
[3] Former anti-virus researcher turns tables on industry, http://voices.washingtonpost.com/securityfix/2009/10/former_anti-virus_researcher_t.html
[4] Some Researchers Lack Basic Ethics: http://threatpost.com/en_us/blogs/some-researchers-lack-basic-ethics-080509

[5] Ethics Behind Anti-virus Evasion: http://blog.damballa.com/?p=304
[6] Host of Internet Spam Groups Is Cut Off: http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html

DATA FUSION METHODOLOGIES FOR CYBER SECURITY[35]

The increasing complexity of the global communications environment presents new challenges for cyberspace research. These challenges are accentuated by the unique characteristics of the cyber domain, which encompasses at least four spheres: the physical sphere, the code sphere, the regulatory sphere, and the idea sphere.

The physical sphere includes the material infrastructure of computers, routers, cell phone towers, undersea cables, and satellites that establish the mechanical, electrical, magnetic, and optical lines of communication. The code sphere comprises the logical instructions and software that operate the communications that flow through the physical layer. Communications flows are embedded within the regulatory sphere, which includes the norms, rules, laws, and principles that govern cyberspace. The last level is the sphere of ideas, often referred to as the "noosphere", which is defined as the circulation of videos, images, sounds, and text through cyberspace (Arquilla and Ronfeldt 1999). Each sphere generates different data types that relate to physical infrastructure, software code, socio-political connections and inferences, and Web content.

Current cyber threats are multi-vector and traverse across the multiple spheres of cyberspace. Tracking and analyzing threats in this environment requires collecting, analyzing, and visualizing large-scale heterogeneous data sets generated by each sphere. Traditional cyber security methods largely focus on data from the physical and code spheres. This focus is useful for analyzing the technical dimensions of cyber threats, but to gain an understanding of the social and political dimensions of the threat and achieve a more holistic picture of the domain all four spheres must be taken into consideration. However, collecting and analyzing disparate data types from each sphere presents serious operational and methodological challenges for researchers. One approach for addressing these challenges can be found in data fusion methodologies.

Data fusion is a concept that can be generally understood as a process in which multiple disparate data sources are combined to achieve a level of analysis and understanding that would not be possible with a single data point. Data fusion techniques and emerging platforms for data analytics and visualization that can handle structured and unstructured information offer new possibilities for the study of the technical, social and political dimensions of cyberspace threats. In this brief we provide an introduction to techniques and tool sets for probing the multiple layers of cyberspace and describe how data fusion can be leveraged to gain greater understandings of the domain. We proceed by providing a description of traditional network security techniques and tools, the concept of data fusion, and a breakdown of the analysis process for probing each sphere of cyberspace.

[35] This brief draws heavily from Deibert, R., Rohozinski R., and Crete-Nishihata, M. (2011). Data Fusion Methodology and the Geopolitics of Cyberspace. *52 Annual International Studies Association Convention,* March 2011, Montreal, QC.

Traditional Cyber Security Methods and Tools

Traditional cyber security methods and tools sets are focused on monitoring and analyzing the flow of information through computer networks. The majority of commonly used techniques and toolsets can be divided into two broad categories: 1) detection and defence; 2) analysis (see Table 1).

The detection and defence category primarily consists of standard network administration tools used to monitor information flows through a network and detect anomalies and prevent possible threats. Tool sets in this category include firewalls, network protocol analyzers, network scanners, and intrusion detection systems (IDS).

The analysis category includes methods and tools focused on data collection and analytics. The tools included in the detection and defence category can be used as data sources for analysis. Other specially designed data collection systems such as honey pots and DNS sinkholes can be deployed to aid threat detection and analysis.

These traditional approaches to cyber threat intelligence are valuable but have limitations. They are often based on signatures of known attacks, making them less effective at detecting emerging threats (Ertoz et al. 2003). For example, existing IDS anomaly detection techniques struggle to keep up with the changing definition of what an anomaly is as intruders continuously adjust their attack strategies (Chandola, Banerjee and Kumar 2009), and even as they have grown more sophisticated, their high rate of false positives remains problematic (Patcha and Park 2007).

Despite these limitations, anomaly-based detection techniques can be more effective when used as a component of a broader approach that encompasses additional data sources and types of analysis.

Detection and Defence	
Firewalls	Systems designed to permit or deny access to networks based on a set of defined rules.
Intrusion Detection System	Systems designed to monitor network traffic for potential threats and trigger alarms when a threat is detected (e.g. Snort).
Network protocol analyzer	Software designed to capture or "sniff" data packets as they flow through a network (e.g. Wireshark, etc)
Network scanners	Software designed for network exploration and security auditing (e.g. Nmap, ncat, etc).
Analysis	
DNS Sinkholes	Systems designed to take requests from a botnet or infected systems and record the incoming information.
Honey pots	Technical "lures" designed to attract attackers to a network system to aid threat detection and analysis
Sandbox / Virtual Machine	Controlled environments for running programs and monitoring their behavior. Sandboxes are often designed to monitor and analyze the behavior of malware (e.g. CW Sandbox, Norman Sandbox, etc)
Incident databases	Repositories of known attacks and malware samples (e.g. malwaredomainlist.com, virustotal.com)

Table 1: Commonly Used Cyber Security Tools and Techniques

Data Fusion Methods

In broad terms the concept of data fusion can be understood as a process in which multiple disparate data are combined to achieve a greater understanding of a situation than would be possible from a single data point. While this general description describes data fusion in basic terms, fusion methodologies span a number of disciplines each of which adopts different definitions and terminology. For example, the US Department of Defence defines data fusion as a "multilevel, multifaceted process dealing with the automatic detection, association, correlation, estimation, and combination of data and information from multiple sources" (US Department of Defence 1991). Other definitions attempt to be broader such as Dasarathy (2001) who uses the term "information fusion" and explains that

in the context of its usage in the society, it encompasses the theory, techniques and tools created and applied to exploit the synergy in the information acquired from multiple sources (sensor, databases, information gathered by humans, etc.) in such a way that the resulting decision or action is in some sense better (qualitatively or quantitatively, in terms of accuracy, robustness, etc.) than would be possible if any of these sources were used individually without such synergy exploitation

The origins of data fusion methods are primarily military research and applications, but the field has expanded to include a wide range of non-military applications including weather prediction, robotics, traffic analysis, and medical diagnostics (Farina et al 2001; Simone et al 2002; Dasarathy 2010).

Data Fusion in Cyber security

Data fusion has also been explored for cyber security applications, and is a particularly active research area in the development of IDS (Corona et al 2009). A central challenge for IDS is the volume of data generated by networks, the increasing number of threats, and the high potential for false alarms. Data fusion research for IDS applications has been pursued to address these challenges. As Giacinto, Roli, and Sansone (2009) explain

It is widely acknowledged that no single input sources, or feature set, or detection algorithm can offer both high detection performance and low false alarm rate. On the other hand, the use of multiple sources of information, multiple feature sets and multiple detection algorithms has proven to be an effective solution to limit the evasion of the detection, to reduce the volume of false alarms, and to produce tools for forensic investigation. The problem is how to choose the elements to be fused and how to perform the fusion.

Other data fusion applications for cyber security that have been explored include probabilistic threat assessment (Beaver, Kerekes, Treadwell 2009) and denial of service attack (DDoS) detection (Siaterlis and Maglaris 2004).

Similar to traditional network security methods, these data fusion applications are focused on the physical and code spheres of cyberspace. We adopt the general concept of data fusion in a broader sense and apply it to the empirical study of cyberspace geopolitics. Similar to engineering sciences that combine multiple sensor data to conduct a more holistic analysis than would be possible with a single sensor, we combine data from the multiple spheres of cyberspace, and manifestations of social agency and practices connected to them, to obtain a deeper understanding of the domain than would be possible from studying one sphere in isolation. This approach blends techniques and tool sets from the field of cyber security with social science methodologies and theoretical frameworks.

Data Fusion for Geopolitics of Cyberspace Research

Over the past decade the Citizen lab (University of Toronto) in collaboration with the Secdev Group (formerly Cambridge Security Programme, Cambridge University) and the Berkman Centre for Internet and Society (Harvard University) has developed a unique approach to probing questions of power relations in cyberspace that blends technical interrogation, fieldwork, and advanced data analytics and visualization techniques.

We have used this multi-disciplinary methodology to rigorously enumerate the prevalence and character of global Internet censorship through the OpenNet Initiative (http://opennet.net), and to investigate major cyber espionage and criminal networks through the Information Warfare Monitor (http://infowar-monitor.net).

Technical Interrogation

Our methods and tools sets for technical interrogation include the tradecraft and techniques of traditional cyber security research and network administration that focus on the physical and code spheres of cyberspace. The physical and code spheres are foundational layers of cyberspace and investigations in the domain require an understanding of how these layers interact and can be manipulated by actors.

Cyberspace is a dynamic environment that is in constant flux and monitoring threats and the general status of the Internet requires a wide sensor network. An example of such a sensor network is found in the methodology for collecting and analyzing technical data on Internet filtering we have developed in the OpenNet Initiative project.

This methodology consists of deploying specially designed desktop software to users in countries within a testing sample. The software runs automated lists of

URLs, IPs and keywords that are separated into two classifications: the local list and the global list. The global is a standardized list of Web sites that cover a range of categories including political,

social, and security related content. The global list is comprised primarily of internationally relevant Web sites with English content. The local list is created for a country under investigation and includes Web sites related to the specific issues and context of the country.

The testing software is designed to make HTTP requests for each URL in the list from two locations, the connection from within the country the user is based in and a control location based at the University of Toronto. Retrieving two sets of results for each URL enables analysts to compare in country results to unfiltered results from our control server and develop profiles that describe the specific blocking behavior of different regimes. We have utilized this method since 2006 and have collected data on 70 countries, 289 ISPs, and over 129,884 URLs (Faris and Villeneuve 2008; see also http://opennet.net).

Field Work

Technical interrogation can provide detailed information on cyberspace, but pairing technical analysis with contextual data can lead to richer understandings of the underlying social and political processes of activities within in the space that would not be discernible from technical data alone.

For example, in the OpenNet Initiative we combine the technical data extracted from the method described above with contextual research and fieldwork conducted in country. This fusion of the two approaches allows us to situate our technical findings in the local political, cultural, and legal environments of the countries under investigation.

Field research and technical interrogation are best done in an iterative and complementary fashion. Field researchers can help identify the sources and nature of local issues, which in turn can help trigger and target technical tests. Likewise, technical interrogation can help drive and focus field research around particular sites. A good example from our own research comes from the *Tracking Ghostnet* report, which uncovered a global cyber espionage network that had infected 1295 computers in 103 countries, including about 30 percent considered high value political and security targets such as embassies, international organizations, and ministries of foreign affairs. The *Ghostnet* investigation began with a suspicion of penetration and surveillance of Tibetan exiled organizations, including the office of his holiness the Dalai Lama. The field researcher working on the case spent many months among the Tibetan communities in Dharmsala, India. He triaged among the personnel and equipment, and ran network diagnostic software on computers he suspected would most likely be compromised. Once collected, the data was sent back to the Citizen Lab for forensic analysis, which in turn led to further field research and data collection among other likely affected targets in New York, Brussels, and elsewhere (Information Warfare Monitor 2009).

Data Collection, Analysis, and Visualization Cycle

The process of data collection, analysis and visualization is an iterative cycle that must be adjusted according to the specific research questions and data being probed.

Each sphere of cyberspace presents different data types that require different methods and tool sets to conduct analysis.

Information from each of the spheres of cyberspace can be extracted and analyzed for research purposes. Each sphere interacts and overlaps with each other. In particular the boundary between the physical and code layers is somewhat blurred, as is the distinction between the content and social layers. Moreover, a single data point can be interpreted as belonging to multiple layers depending on the analysis technique and interpretive frame of the analyst. For example, knowing the country to which an autonomous system number (ASN) or classless Internet domain routing (CIDR) prefix has been allocated can be used to geographically locate infrastructure and possibly make political or other social inferences.

Providing a comprehensive overview of techniques and tools across the multiple spheres of cyberspace is beyond the scope of the present brief. What follows is a sampling of methods and toolsets to consider for each data layer. The full data collection, analysis and visualization process is illustrated in Figure 1.

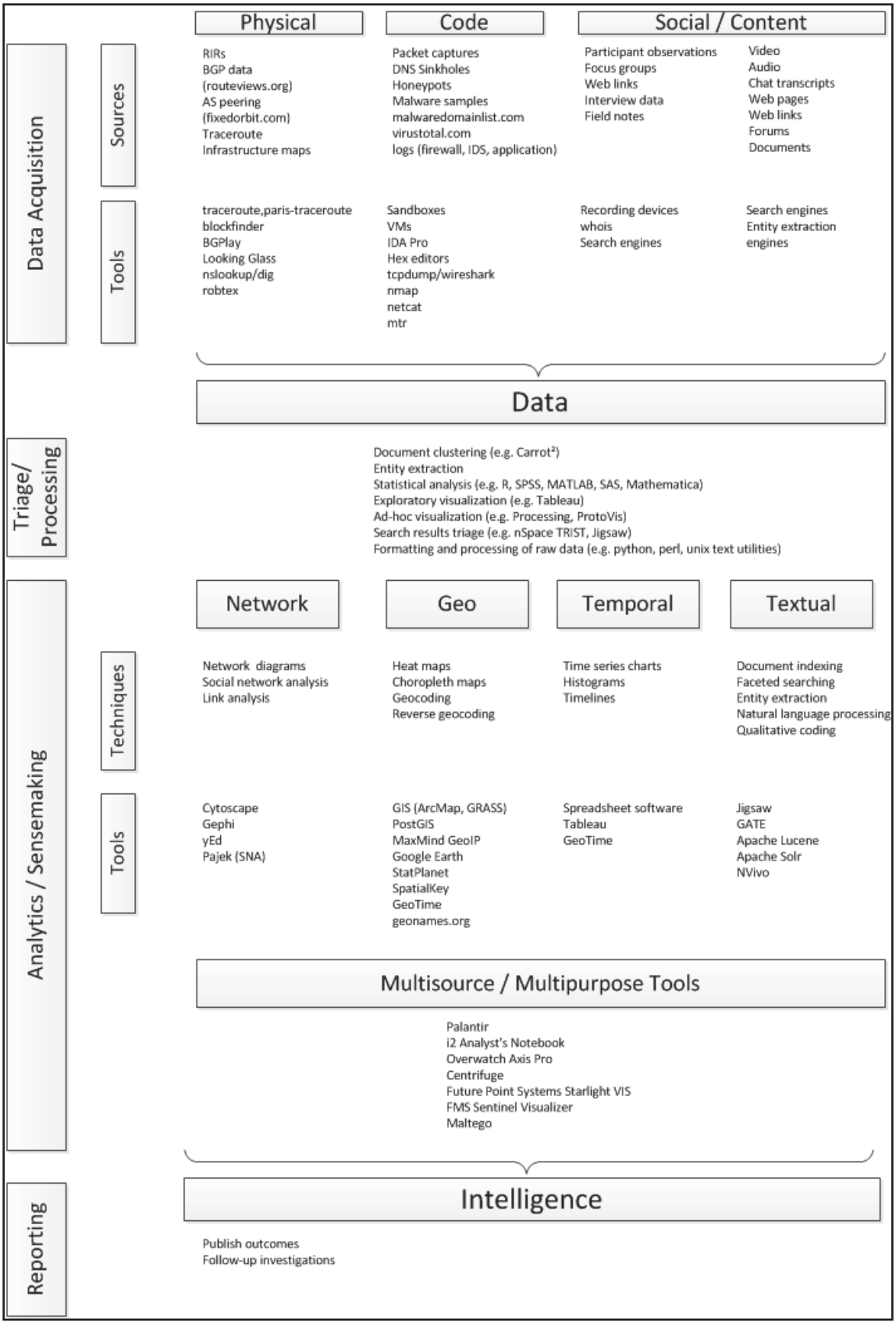

Data Acquisition
Sources
Physical
RIRs
BGP data
(routeviews.org)
AS peering
(fixedorbit.com)
Traceroute
Infrastructure maps
Code
Packet captures
DNS Sinkholes
Honeypots
Malware samples
malwaredomainlist.com
virustotal.com
logs (firewall, IDS, application)
Social / Content
Participant observations
Focus groups
Web links
Interview data
Field notes
Video
Audio
Chat transcripts
Web pages
Web links
Forums
Documents
Tools
traceroute,paris-traceroute
blockfinder
BGPlay
Looking Glass
nslookup/dig
robtex
Sandboxes
VMs
IDA Pro
Hex editors
tcpdump/wireshark
nmap
netcat
mtr
Recording devices
whois
Search engines
Search engines
Entity extraction
engines
Data
Triage/ Processing
Document clustering (e.g. Carrot²)
Entity extraction
Statistical analysis (e.g. R, SPSS, MATLAB, SAS, Mathematica)
Exploratory visualization (e.g. Tableau)
Ad-hoc visualization (e.g. Processing, ProtoVis)
Search results triage (e.g. nSpace TRIST, Jigsaw)
Formatting and processing of raw data (e.g. python, perl, unix text utilities)
Analytics / Sensemaking
Techniques
Network
Network diagrams
Social network analysis
Link analysis
Geo
Heat maps
Choropleth maps
Geocoding
Reverse geocoding
Temporal
Time series charts
Histograms
Timelines
Textual
Document indexing
Faceted searching
Entity extraction
Natural language processing
Qualitative coding
Tools
Cytoscape
Gephi
yEd
Pajek (SNA)
GIS (ArcMap, GRASS)
PostGIS
MaxMind GeoIP
Google Earth
StatPlanet
SpatialKey
GeoTime
geonames.org
Spreadsheet software
Tableau
GeoTime
Jigsaw
GATE
Apache Lucene
Apache Solr
NVivo
Multisource / Multipurpose Tools
Palantir
i2 Analyst's Notebook
Overwatch Axis Pro
Centrifuge
Future Point Systems Starlight VIS
FMS Sentinel Visualizer
Maltego
Intelligence
Reporting
Publish outcomes
Follow-up investigations

Figure 1: Data collection, analysis, and visualization cycle

Data Collection

This section surveys some of the different data types that can be extracted from the various layers of cyberspace and outlines methods and techniques for deriving information from them.

Physical

The physical layer is defined by the computers, cables and networking hardware that establish the various lines of network communication. This material infrastructure generates data points that can be mapped and monitored and helps researchers understand machine level interactions in the network. Some of the data from this layer can be represented geographically (e.g. maps of regional fibre-optic backbones, undersea cables, satellite infrastructure, etc).

Data sources that can be used for mappings of the physical infrastructure include routing mechanisms such as border gateway protocol announcements, and autonomous system and Classless Inter-Domain Routing (CIDR) allocations available from Regional Internet Registries (RIRs).

There are several useful Internet resources that provide network-level information:

- routeviews.org observes BGP announcements from sensors they have deployed throughout the Internet and provides a utility called BGPlay for visualizing the data.

- bgpmon.net is a monitoring tool that can alert the user in case of an "interesting" path change such as prefix hijacking.

- team-cymru.net provides an IP address-to-ASN mapping service.

- fixedorbit.com provides information on the peers and neighbours of a given ASN.

- www.robtex.com provides reverse DNS lookup for an entire class C network based on a given IP address, which can sometimes be used to get a sense of the sites that are hosted in a similar space.

Geocoding of IP addresses using a database such as MaxMind - GeoIP, while imperfect, can also provide some insight into this layer. The traceroute utility may be used to measure the route path

and latency of packets over an IP network, which can lead to information about network topology and where in the path satellite or long-haul submarine cable transit occurs (Wagner 2008).

Code

Data sources from the level of code can be extracted from the network monitoring and threat analysis tools described in section 2 (e.g. firewalls, IDS log files, packet captures, honeypots, sinkholes, online malware repositories, etc).

Content / Social

Gathering data on social behaviour in cyberspace can be conducted by directly probing individual actors through traditional qualitative methodologies such as interviews, surveys, participant observation, focus groups, etc. Information on social networks, activities, and interactions can also be extracted from Web content such as Web pages, hyper links, tags, and other media (Rogers 2010). The same Web content can also be collected and analyzed as independent media artefacts in isolation from the users that generate them.

A key challenge to collecting Web content data is ephemeral nature of the Internet. Researchers cannot depend on content always being available or archived reliably. For Web content that is no longer available a tool that can be of use is the Internet Archive Way Back Machine (http://www.archive.org/web/web.php), which has archived 150 billion Web pages from 1996 onwards and provides an index with timestamps.

Triage

Once a suitable amount of information becomes available, it must be triaged and processed before it can be effectively analyzed. Data triage can be approached in a number of ways and choosing an appropriate technique often depends on the nature of the data.

At the initial triage stage it is desirable to get a general sense of the data and begin exploring it to formulate hypotheses that may be worth testing. Noisy or irrelevant data may be detected and eliminated with the help of statistical analysis. When dealing with large amounts of free-form textual data, techniques such as document clustering and entity extraction can help an analyst drill down into items of interest. Visualization can also be a very powerful tool for recognizing patterns and anomalies. Frameworks such as Processing (http://processing.org) or ProtoVis (http://prefuse.org) can help programmers develop custom visualizations of data for analysts. Similarly, spreadsheet or business intelligence software can be used by analysts to create scatter plots or other charts that make outliers and correlations more apparent.

Raw data often requires processing to make it compatible with analysis and visualization tools. Large data sets make the processing stage particularly important, as dealing with raw data at high quantities can be unmanageable. Automating data transformations and general clean-up with ad-hoc scripts can be an effective means of performing tedious processing.

Once items of interests have been isolated and processed into a manageable state they are ready to be introduced to the analysis and sensemaking stage.

Analysis / Sensemaking

Data can be classified in many ways. Understanding the type of data to be analyzed can help determine the most appropriate tools for analysis. When dealing with data extracted from cyberspace at least four general analytical approaches can be considered: network, geographic / spatial, temporal, and textual. Special-purpose analysis tools and techniques exist for each of these approaches. In addition there is an emerging category of all source multi-purpose analysis platforms that enable all four levels of analysis in a common environment.

Network Data Analysis

Network data is represented as nodes (vertices) that are connected via links (edges) in a structure called a graph, or network. In social network analysis, where nodes represent individuals or organizations and links represent some kind of interdependency between them, software such as Pajek (http://pajek.imfm.si) provides node centrality measurements which can help identify actors that play key roles in or between certain groups.

Communication events between computer systems can be visually modeled as links, and by running automated layout algorithms suspicious patterns of activity may be more readily observed (Conti 2007; Marty 2008). Cytoscape (http://www.cytoscape.org) and Gephi (http://gephi.org) are two popular open source tools for visualization and analysis of graphs.

Spatial Data Analysis

Data that can be linked to a physical location (point or region) in the world is known as geographic, or spatial information. Geographic information systems (GIS) such as the industry standard ArcGIS (http://www.esri.com/software/arcgis/arcview/index.html) or the cross-platform GRASS (http://grass.osgeo.org) combine cartography, statistical analysis and database technology to provide an analytical platform for spatial data. Aggregating data and displaying such data as a heat map or choropleth (thematic) map in its geographic context can make it easier to understand trends as they relate to physical locations and/or political divisions. Technology such as the Google Maps API allows data to be plotted and "mashed up," (i.e. compared with data from varied sources).

Geocoding refers to the process of determining the coordinates of a location (e.g. latitude/longitude) from an address, city name, or other geographic description. Geographic data comes into play while doing cyber research when looking at where certain domains have been registered, or where an assailant is (or appears to be) coming from. MaxMind GeoIP (http://www.maxmind.com/app/ip-location) is a product for geocoding IP addresses, though analysts should realize it has limitations with respect to accuracy and precision.

Web content can also be mapped spatially and relationally for social analysis. For example, Richard Rogers and his group at the Digital Methods Initiative have developed a tool called Issue Crawler, which is designed to draw inferences around connections between online communities based on the collection and analysis of links made between Web sites and blogs of organizations (see http://govcom.org).

Temporal Data Analysis

A great deal of data encountered in the course of cyber security research has a temporal dimension. Examples include log file timestamps, domain registration dates, and botnet command and control servers that may use fast-flux DNS techniques to avoid being shut down.

Visualization is often an effective means for identifying temporal trends. Using spreadsheet or business intelligence software to create time series charts and histograms help show changes in values over time. Plotting events on a timeline may make certain correlations stand out, for example the date of denial of service attacks corresponding to important anniversaries or otherwise significant dates. Also worth mentioning here is spatio-temporal data (i.e. information with both a geographic and temporal component). Combining a timeline with a map, along with a tool that supports linked selection or dynamic filtering, greatly assists with data exploration. GeoTime (http://www.geotime.com) is an example of a special-purpose application that uses a 3D display to simultaneously show the geographic and temporal distribution of events. It may also be used with non-geospatial data, for example nodes in a network, to show communication events over time.

Textual Data Analysis

The huge amount of open-source, unstructured text available on the Internet is a valuable data source, though its sheer volume can make it difficult to effectively utilize for research purposes. Automated processing of unstructured data is a perennial challenge for computer science sub-disciplines such as artificial intelligence and natural language processing. However, there are tools available that can help facilitate the analysis of such data types. For example, entity extraction engines automatically identify and categorize people, places and organizations, times, quantities etc. in unstructured text documents. Document indexing makes finding key words in a large corpus much faster than a linear search would be. Qualitative coding software can be used to categorize documents and determine themes.

Multi-source / Multi-purpose Platforms

In contrast to the special purpose tools described above, there is an emerging class of analytical platforms designed to handle large amounts of disparate data and provide a unified workspace for analysts to collaborate. An example of this kind of system is Zeropoint and Palantir (Wright, Payne, Steckman and Stevson 2009). Its primary user interface is a graph (node-link) view where the user can search for connected entities or documents based on properties of interest. New nodes and links may be created dynamically, and a user-defined ontology may be used to specify entity properties and relationships. Companion views such as a property histogram, timeline and social network analysis helper provide support for common analytical tasks. Unstructured documents can be imported, and are indexed for fast searching. Portions of text can be selected and tagged as corresponding to a particular entity. A geospatial application is also integrated. As new structured data is imported, new properties and links can be made with existing entities.

Platforms that provide a common environment for the analysis and visualization of structured and unstructured data can also help multiple analysts collaboratively contribute to an on-going investigation. Enabling this form of collaboration can help mutli-disciplinary teams draw from each other's differing expertise and analytical strengths.

Reporting

Once analysis has been completed, hypotheses validated, and conclusions drawn, the resulting information needs to be made available to interested parties. A report should provide an overview of the problem or situation being addressed, as well as mention the relevant information sources. Sources are important because data analysis can only be as good as the data used as input. Any assumptions made or limitations of knowledge or evidence should be mentioned. A high-level overview of the major steps in the analysis is necessary for others to have confidence in the conclusions.

To this end, analytical software that allows the user to track their process via a reporting component of some sort is helpful not only for organizing thoughts and hypotheses, but also for walking through an analysis (Gotz and Zhou, 2009). Such an integrated system can also help impart tradecraft. An example of this is found in GeoTime, where a user can write free-form text in an auxiliary view and insert "snapshot" hyperlinks that will replay a specific, possibly annotated view of the data (Eccles, Kapler, Harper and Wright, 2007).

In terms of data visualization, one may distinguish between approaches that help with exploration and discovery compared to those that clearly and effectively convey a particular message to an audience. An interactive system can help someone draw their own conclusions, whereas static (or occasionally animated) charts and diagrams illustrating compelling relationships in the data are more appropriate for disseminating information.

References

Arquilla, John and David F. Ronfeldt. *The Emergence of Noopolitik: Toward an American Information Strategy*. (Washington, D.C.: RAND, 1999)

Beaver, Justin M, Kerekes, Ryan A, Treadwell, Jim N, 2009. An Information Fusion Framework for Threat Assessment, Paper in conf proceedings, The 12th International Conference on Information Fusion, Seattle, Washington, July 2009.

Chandola, Varun., Arindam Banerjee, Vipin Kumar. 2009. Anomaly detection: A survey. *ACM Computing Surveys,* 3.

Corona, Igino, Giorgio Giacinto, Claudio Mazzariello, Fabio Roli, Carlo Sansone. 2009. Information Fusion for Computer Security: State of the Art and Open Issues *Information Fusion 10:* 274-284

Conti, Greg. *Security Data Visualization: Graphical Techniques for Network Analysis*, (San Francisco, CA: No Starch Press, 2007).

Dasarathy, Belur. 2001. What, where, why, when, and how? *Information Fusion*, 2:75–76.

Dasarathy, Belur. 2004. "A panoramic sampling of avant-garde applications of information fusion," *Information Fusion,* 5:233–238

Dasarathy, Belur. 2010. "A representative bibliography of surveys in the information fusion domain," *Information Fusion*, 11:299-300

Eccles, Ryan, Thomas Kapler, Robert Harper, and William Wright 2007. Stories in GeoTime, IEEE Symposium on Visual Analytics Science and Technology. Sacramento, California. October 28-November 1 2007

Ertoz, Levent., Aleksander Lazarevic, Eric Eilertson, Pang-Ning Tan, Vipin Kumar, and Jaideep Srivastava. Protecting against cyber threats in networked information systems, SPIE Annual Symposium on AeroSense, Battlespace Digitization and Network Centric Systems III, Orlando, FL, April, 2003.

Faris, Rob, and Nart Villeneuve. 2008. "Measuring Global Internet Filtering," In *Access Denied: The Practice and Policy of Global Internet Filtering*. Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain. eds. Cambridge MA: MIT Press. 5-27.

Giancinto, Giorgio, Fabio Roli, and Carlo Sansone. 2009. Information Fusion in Computer Security. *Information Fusion,* 10:272-273.

Gotz, David, and Michelle X. Zhou. 2009. "Characterizing users' visual analytic activity for insight provenance." *Information Visualization,* 8:42-55.

Information Warfare Monitor, 2009. Tracking GhostNet: Investigating a Cyber Espionage Network Citizen Lab / The SecDev Group, <http://www.tracking-ghost.net>.

Marty, Raffael. *Applied Security Visualization*, (Boston MA: Addison Wesley Professional, 2008)

Patcha, Animesh., and Jung-Min Park. August 2007. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51:3448-3470.

Rogers, Richard. 2010. Internet Research: The Question of Method -- A Keynote Address from the Youtube and the 2008 Election Cycle in the United States Conference. *Journal of Information Technology & Politics*, 7:241-260.

Siaterlis, Christos, and Basil Maglaris, Towards Multisensor Data Fusion for Dos Detection. 224 ACM Symposium on Applied Computing. March 14-17 2004, Nicosia, Cyprus.

Simone, G., Farina, A., Morabito, F.C., Serpico, S.B., Bruzzone, L, 2002. "Image fusion techniques for remote sensing applications," Information Fusion 3 (2002) 3–15

United States Department of Defence, 1991. Data fusion lexicon Data Fusion Subpanel of the Joint Directors of Laboratories, Technical Panel for C3, 1991

Wagner, Tyler J. "Identifying undersea fibre and satellite links with traceroute." http://www.tolaris.com/2008/10/09/identifying-undersea-fibre-and-satellite-links-with-traceroute. Accessed March 16, 2011.

Wright, Brandon, Payne, Jason, Steckman, Matthew, and Scott Stevson, 2009. "Palantir: A Visualization Platform for Real-World Analysis," IEEE Symposium on Visual Analytics Science and Technology. October 12 - 13, Atlantic City, New Jersey, USA

INVESTIGATION SYSTEM, SOURCES AND ARCHITECTURE

Advanced Cyber Analytics [ZeroPoint]

Advanced Cyber Analytics is a network intelligence capability that provides large organizations with the ability to establish full situational awareness of their network systems and exposures. The system acts as an intelligence platform that aggregates and fuses DNS metrics, IP addresses, malware, geographical and temporal information and other data from multiple feeds; derived from a client's network, the upstream telecommunications carrier and from global threat intelligence sources.

Instead of having to combine a number of different technologies, the system provides the ability to not only gain a holistic perspective of computer network traffic, but respond to and investigate incidents from a single platform.

The solution works at carrier/enterprise scale with big-data to create targeted intelligence that facilitates rapid identification, management and remediation of network threats proactively, including Advanced Persistent Threats (APT). The solution actively manages an organization's cyber domain by combining detection, alert and response capabilities within one system.

Cyber data sets can be extremely large, heterogeneous, and complex. This often leads to performance, scalability and flexibility bottlenecks when using traditional tools and systems. In contrast, the solution architecture was specifically designed for data sets and situational awareness in the cyber domain. This approach optimizes performance, flexibility, and scalability, making it ideal for organizations with large and complex networks who face the most advanced and complex threats.

The *Zeropoint and Palantir* data fusion platform performed a central role in the research. All data sources were fed into the system for triage, deep analyse, collaboration, synthesis and visualization. The system enabled us to store, search and share knowledge and the mission with greater speed and fewer resources. Powerful and rich analysis advancements were leveraged simultaneously against structured, semi-structured, and unstructured data from multiple disparate data repositories and sources all at once.

ZeroPoint is a network intelligence platform that provides large organizations with the ability to establish full situational awareness of their network systems and vulnerabilities, by aggregating DNS, IP and other data from multiple feeds derived from a network and from the global Internet.

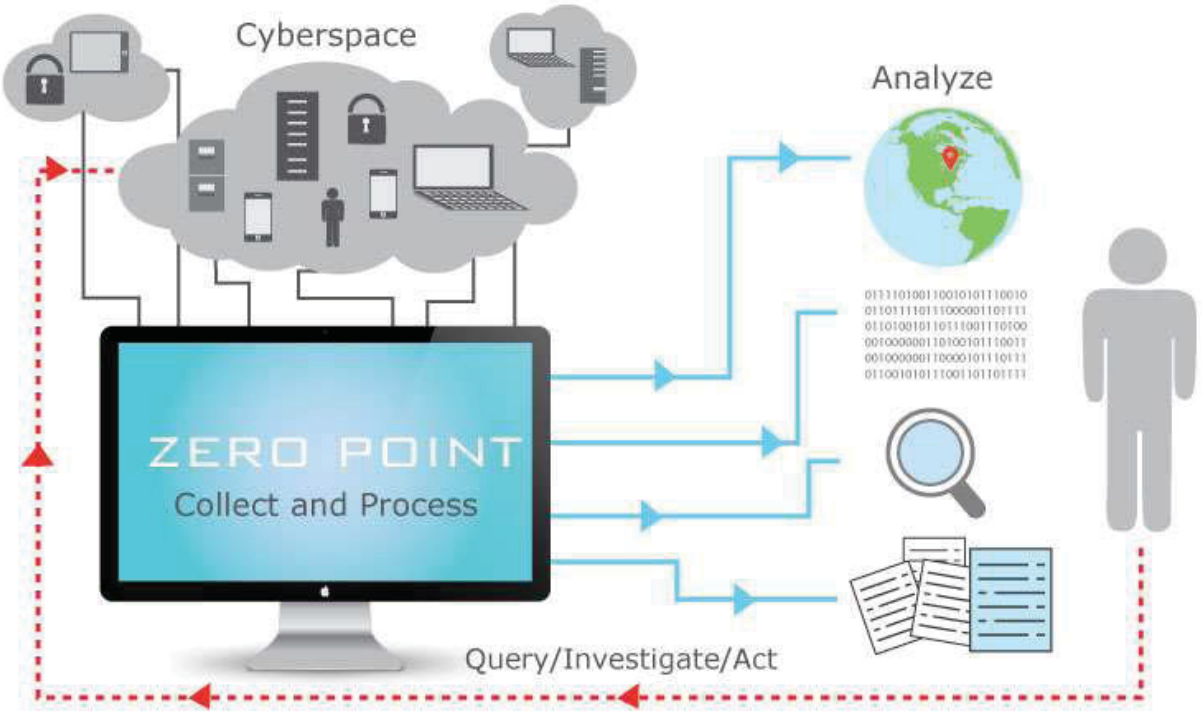


Figure 1: A diagram demonstrating the intelligence collection, processing and analysis cycle employed by ZeroPoint for cyber intelligence

ZeroPoint works at scale with big data to create targeted intelligence that facilitates the rapid identification, management and remediation of network threats, including APTs. ZeroPoint actively manages an organization's cyber domain by combining detection, alert and response capabilities within one system.

Unlike conventional cyber security products, ZeroPoint does not monitor what happens within your network, but focuses on what your network would look like to an outside entity and how it is communicating with the Internet. ZeroPoint is unique in that it operationalizes big cyber data analytics, allowing for the creation of targeted intelligence in real-time.

ZeroPoint combined information on DNS queries, IP addresses, malware, geographical and temporal information into a single platform, thus eliminating the problem of centralizing relevant computer network data. This give us the ability not only to gain a holistic perspective of their computer network traffic, but also to respond to and investigate incidents from a single platform.

Cyber data sets can be extremely large, heterogeneous and complex. This often leads to performance, scalability and flexibility bottlenecks when using traditional tools and systems. ZeroPoint was specifically designed for data sets and situational awareness in the cyber domain. Unlike other network security systems, ZeroPoint's approach optimizes performance, flexibility and

scalability, making it ideal for organizations with large and complex networks that face advanced and complex threats.

Threat detection and neutralization: ZeroPoint analyzed and scored network traffic, allowing for automatic or manual classifications for permitting, alerting or blocking connections.

Gather intelligence: ZeroPoint's constantly growing knowledge base provided the team with the ability to access information instantly on millions of publicly advertised IPs, domains and malware samples.

Establish network activity baselines: ZeroPoint allowed the team to gain perspective on network traffic levels to determine when events are occurring outside of normal bounds.

Identify and mitigate Advanced Persistent Threats: Using ZeroPoint's scoring system, in combination with its fusion of network-traffic data with temporal and spatial information, we were able identify APTs, block them, and can then do further analysis by importing the information into investigative platforms such as Palantir or I2.

Geo-visualization and temporal analysis: By fusing network data with geographical and temporal components, ZeroPoint revealed the real-world context of incidents, showing where traffic is physically going and when it's going there. This allows for the analysis of traffic patterns that can indicate malicious activity, such as behaviour that suggests the presence of a botnet.

Threat mitigation: With ZeroPoint, organizations we created custom DNS rule sets for specific domains, CNAMES, netblocks and IPs. This allows network owners the ability to block or sinkhole DNS requests occurring on the network – an effective method of mitigating threats. This capability is also useful in the analysis of security threats.

Access the data feed: All the data that make up ZeroPoint's knowledge base were easily accessible through an open API. This allows for an organization to query ZeroPoint to gather any known information regarding entities, and incorporate it into other tools being used in-house.

Service-Oriented Architecture

ZeroPoint has been designed with a Service-Oriented Architecture in mind, allowing for the data in the knowledge base to be easily transferred to different applications or viewed in ZeroPoint's own user interface. Technical staff can look at the data at a granular level, but information was also made available in a user-friendly format for non-technical personnel and managers.

The ZeroPoint interface can be broken down into the following functional components:

Network Health Snapshot: ZeroPoint provides situational awareness of a network's status in real time, allowing the user to quickly identify security concerns.

Network Manager Interface: Based on the available data and the Network Health Picture, ZeroPoint allows managers to stage a rapid response to security situations on the network.

Network Intel Interface: It is not only important to see and respond to network incidents as they occur, but also to be able to analyze the data available, either to mitigate the chance of a security threat occurring, or to see what the environment was like prior to an event. ZeroPoint allows for the data to be viewed in a way that can be used to conduct dynamic investigations (deep dive/drill down), in order to gain a technical understanding of events in a given situation.

Because ZeroPoint was designed with an open API, data from its knowledge base are easily integrated into different applications. ZeroPoint treats everything in the knowledge base as data, which can be outputted to virtually any format, including geospatial, temporal and statistical displays, as well as scoring, dashboards and other traditional reporting metrics. ZeroPoint data can also be exported into other toolsets and platforms for further analysis or reporting.

Integration with Palantir and I2

Recent studies and experience have shown that, when investigating cyber threats, looking at data from the network level alone is not enough. Simply put, these threats also involve physical devices, people and locations. As demonstrated in the *Ghostnet* (2009) and *Shadows in the Cloud* (2010) investigations published by the Information Warfare Monitor, investigators needed to conduct cross-domain analytics in order to determine who was behind a particular attack, what other attacks they were involved in, and what we can glean from other information sources.

While ZeroPoint provides unparalleled understanding of computer network activity, we determined that it was essential to integrate ZeroPoint with a general-purpose analytics platform that would allow users to drill down into specific security incident(s) and to integrate cyber data with non-cyber data sets for complex analysis.

For this reason, ZeroPoint is integrated with one of the world's leading analytics platforms, Palantir. Provided by Palantir Technologies, based in Palo Alto, California, the Palantir system is based on four foundational pillars that address the major intelligence infrastructure requirements of both government and the private sector: data integration; search and discovery; knowledge management; and secure collaboration.

This integration allows analysts to fuse ZeroPoint's network-security knowledge base with data collected by Palantir from non-network domains, such as personnel files, financial transactions, geographical locations, dates and times of significant events and unstructured documents from

classified and open sources. Analysts are then able to gain insights they would not have had if the two datasets had remained in separate silos.

Together, the two systems allow analysts to fuse network-level data with "real world" data (be they open sources, closed sources, human resource records, transaction data, event data, unstructured reports, etc.) to create a truly holistic view of cyber threats.

The integration is seamless and easy to use for the operator: Any data available in the ZeroPoint knowledge base can be brought into Palantir. For example, an analyst can bring an alert generated in ZeroPoint directly into Palantir as a fully resolved security event, using a helper application. Because the alert is imported as a resolved entity, an analyst can then search through previous investigations and/or build a new one based on that entity.

The combination of ZeroPoint and Palantir provides the user the ability to:

- maintain a situational awareness of what is occurring on a computer network;
- identify, respond to and mitigate security incidents by identifying malicious traffic;
- conduct cross-domain investigations to fuse computer network and real-world data, in order to gain a better understanding of modern security threats, and to respond to them effectively;
- pursue different analytical paths based on the same data; and,
- import, analyze and investigate threats in a completely audited format, so that any analytical insights and conclusions are sourced, tracked and presentable to a higher official (manager, policymaker, judicial official).

Integration with traditional security products

In technical terms, one way of understanding what ZeroPoint does – and how it is different from other cyber security products – is captured nicely in the three challenges once outlined by former U.S. Secretary of Defense Donald Rumsfeld:

"Known knowns," or things we know: In the context of Internet security, this means looking for threats or patterns that are already known. Most intrusion detection systems used by network administrators parse through existing network traffic to find things that match particular, defined signatures.

"Known unknowns:" Roughly speaking, this challenge is addressed by Security Information and Event Management Systems, or SIEMs. These are technologies that collect all of the available data existing within networks from individual system logs and devices. They then attempt to create a neat haystack, from which it is possible to extract the needle.

Finally, there are the "unknown unknowns:" These are the most difficult to detect because analysts do not always know what they are looking for. This is the level at which ZeroPoint operates.

SIEMs: ZeroPoint shares many of the characteristics of a traditional SIEM system, such as the correlation and aggregation of data, and alerting mechanisms. However, unlike conventional SIEMs, ZeroPoint can expand on these capabilities: not only can ZeroPoint issue alerts, but it also packages the alerts with the option to investigate and respond as well – all within the same interface. ZeroPoint does not focus exclusively on providing insight into potentially bad traffic, but instead provides an overview of all traffic, allowing clients not only to detect signs of malicious activity, but also to build an in-depth understanding of how their network functions under normal conditions as well.

DNS Detection Technologies: ZeroPoint differs from traditional DNS detection technologies in a number of ways: first, it builds a knowledge base founded on the metadata dissected from DNS requests and IP addresses associated with those domains, as well as the netblocks and ASNs that manage them, combined with geographical and temporal statistics. This approach provides the ability not only to block or allow DNS requests, but also to gain a complete perspective on the request and what other entities it is related to. Second, ZeroPoint is dynamic, and can very easily incorporate additional sources of information to provide more insight into computer network traffic, including linking custom block lists and malware analysis results to the entities they are related to.

ZeroPoint - Technical

The Internet is extremely diverse and complex, with millions of hosts, sites and networks spread across the world. However, it has fundamental underlying protocols that can be leveraged to provide a comprehensive view of Internet communication. These protocols can provide invaluable insights into the nature and origins of cyber threats that go beyond simple security alerts, allowing analysts to track, describe and even predict cyber threats through the study of information about how these threats are circulating within cyberspace. This kind of information – also referred to as "metadata," or data about data – is the main pillar of ZeroPoint's approach.

The majority of traffic on the Internet uses two primary protocols: IP, which are used to identify individual computers or networks; and DNS, which provides easy-to-understand, technically manageable infrastructure for mapping domains to IP addresses. ZeroPoint collects information from both protocols, and then fuses that data with additional sources such as malware signatures (block lists) and geographical locations. This creates a growing knowledge base, including a map of unique entities on the Internet, that dynamically updates and expands itself over time.

ZeroPoint draws on this knowledge base as it monitors the response to all DNS requests (internet traffic) from a client's organization, dissecting that information into the following categories based on the domain, and the fully qualified domain name: DNS record type, IP addresses, associated geographical location, netblock, and ASN. As it does so, it instantly cross-references this information with the data from its knowledge base – a process that not only allows it to quickly assess whether a

client's network is in contact with a potential threat, but that also provides a complete understanding of the organization's communication with entities on the internet in general.

The ZeroPoint backend – its knowledge base – is scalable and flexible, and is not limited by a fixed schema or ontology for the data contained within it, so it can incorporate virtually any kind of data. At any time it is possible to update, insert or change information based upon a specific event. This design is optimal for cyber data, where multiple and diverse data sources make a fixed schema a detriment to performance, scalability and cost.

ZeroPoint also incorporates open-source and commercial cyber data, such as malware signature feeds, domain blacklists and other security information, into its dynamic knowledge base. The only requirement for inputting additional information is making sure the data follow a similar schema to ensure that the underlying entity (ASN, netblock, IP address, domain, etc.) is defined.

The system is designed with the following logical flow:

Collect Data: Acquire data that relate to different types of important information (e.g. passive capture, pcaps, CSV, APIs).

Extract: Get the relevant data attributes based upon the source (such as parsing external blacklists, or traversing and extracting elements from packets). Depending upon what information fills in these attributes, the data are broken up and additional contextual information is inserted in the applicable areas, such as ASN and geographical information for a specific IP.

Pull and Route: Information related to the extracted attributes is gathered or sent to secondary data stores. Specific elements are evaluated against separate data sources, such as GeoIP and a network database. This process uses outside sources to provide additional context for network data captured by ZeroPoint. Data are also organized into collections related to the core elements.

Log: The core attributes are stored in an indexed, optimized fashion.

Data Access: Core attributes provide quick retrieval of substantial amounts of information.

ZeroPoint Deployment Options

Cloud-based: ZeroPoint's cloud-based implementation includes a managed DNS solution that permits organizations to actively manage their security beyond traditional firewall/perimeter defence.

On-site/hardware-based: ZeroPoint's hardware-based version is designed to work within client-operated networks. It is available in a 1U form factor for easy implementation.

Datafeed: The knowledge base and intelligence infrastructure used by the ZeroPoint product line are available as a standalone datafeed, to be integrated with an organization's other intelligence tools.

Custom analytics: ZeroPoint can be deployed by a consulting team comprised of The SecDev Group or a partner organization to conduct forensic and/or live analysis on data provided by a client.

LEGAL CONSIDERATIONS

An effective strategy for dealing with cyber attacks necessitates a proactive defence consisting of interdicting and disrupting threat activities. The goal of this strategy is to discover, infiltrate and disrupt or render inert criminal activity before there is harm. To this end, fusion techniques are highly useful. This section lays out some of the legal challenges applying to "network defence and detection practices" beyond the clearly defined bounds of a proprietary network.

One way to understand such legal challenges is to look at the techniques employed and to ask the following 4 questions: (1) "what information is collected"; (2) "how is the information collected"; (3) "how is the information used"; and (4) "to whom is the information disclosed". Although non-exhaustive, these questions help to determine whether legal issues are engaged. For example, asking what data are collected helps determine whether privacy legislation is relevant. If personal information[36] is collected, the collection may be subject to privacy laws.

Network Ownership and the Role of Service Agreements and Policies

Network ownership provides a certain degree of management latitude. That said, service providers may be obligated by service level agreements with their customers to provide a certain quality of service. Through IT management and service provider policies such as a "terms of use" or a "privacy policy", parameters around service are established. For example, a service level agreement may set out uptime requirements for the service provider. To meet these metrics the service provider may employ techniques such as deep packet inspection (DPI). If this practice is set out in the agreement, it may bolster a service provider's use of DPI were it to be challenged.

In addition, the service provider may use a complementary suite of policies to establish expectations. For example, a privacy policy which details (among other points), the manner in which personal information may be collected, the purpose(s) of the collection and how such information may be used, appears to be an accepted practice at law. This may allow for the collection of personal information without express consent of the individual. Under such circumstances, however, notice is key, and, therefore, relevant policy would need to be made accessible to the individual. Thus, while documented policies are an integral component of mitigating legal issues, they are not in and of themselves sufficient to ensure practices are compliant legally.

Limitations of this Analysis

Organizational use of fusion techniques may vary based on sector membership, business requirements and objectives. While some general statements may be made about potential legal challenges, the devil is in the details. For example, without a line of sight into individual organizational practices, it is difficult to know with whom information may be shared. For this

[36] Personal information is any information which can be linked directly or indirectly to the individual – from social insurance number to an IP address. See e.g. section 2 of the *Personal Information Protection and Electronic Documents Act* (2000, c. 5) which broadly states: "'personal information' means information about an identifiable individual...".

reason, this brief is limited to high-level identification of legal challenges only. A more precise legal analysis may be better achieved on a case-by-case basis.

Legal Background

Privacy Legislation

There are a number of pieces of privacy legislation across Canada, which may apply depending on the sector to which an organization belongs. All of the privacy acts are similar in terms of promoting fair information practices like: accountability, transparency, consent, data minimization, limiting use, disclosure and retention, accuracy, safeguards and individual access (challenging compliance). However, there may be some jurisdictional differences (e.g. requirements related to breach notification).[37]

Private Sector

The *Personal Information Protection and Electronic Documents Act*[38] applies to all private sector organizations in respect of an individual's personal information in connection with: commercial activities in all provinces (with the exception of Quebec, Alberta and British Columbia where they have their own legislation which has been deemed substantially similar); and in connection with employee information where the organization is a federal work, undertaking or business (e.g. a telco, shipping, airline, etc.)[39]

Individual consent is required for any collection, use or disclosure. However, there are certain exemptions from the consent requirement such as where personal information may be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed.[40] There is also an exemption for use without consent for the purposes of an emergency that threatens the life, health or security of an individual.[41] Finally, there is an exemption from the consent requirement where personal information is to be used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information.[42] In this latter case, it needs to be used in a manner that will ensure its confidentiality, and the Privacy Commissioner is informed of the use before the information is used. [43]

Public Sector

[37] See, e.g., section 34.1 (1) of Alberta's *Personal Information Protection Act* (PIPA) which has added a new requirement for organizations to notify the Information and Privacy Commissioner of incidents "involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual." PIPA also gives the Commissioner the power to require organizations to notify individuals to whom there is a real risk of significant harm as a result of such an incident.
[38] (2000, c. 5) [PIPEDA].
[39] PIPEDA s. 4.
[40] See PIPEDA s.7(1)(b) or 7(2)(a).
[41] PIPEDA s.7(2)(b).
[42] PIPEDA 7(2)(c).
[43] *Ibid*.

Public sector has both federal and provincial privacy legislation. At the federal level, the *Privacy Act* [44] applies to personal information collected by the government and its institutions including federal law enforcement agencies.[45] Here too there are exemptions worth noting. For example, the government may disclose for research purposes where it cannot otherwise reasonably de-identify the information.[46] In such a disclosure it would need written undertaking that no subsequent disclosure of the information will be made.[47]

At provincial level all provinces will have their own acts governing privacy. For example, in Ontario there are three pieces of legislation addressing privacy: (1) the *Freedom of Information and Protection of Privacy Act*[48] applying to the Government of Ontario and its institutions (including Ontario universities and the Ontario Provincial Police); (2) the *Municipal Freedom of Information and Protection of Privacy Act* [49] applying to municipal governments (including local law enforcement); and (3) the *Personal Health Information and Protection Act, 2004*[50] for health information custodians.[51]

Both the FIPPA and MFIPPA are very similar in terms of content and structure. Both acts contain exemptions for research and law enforcement. On the research side, a disclosure is permitted if:

- the disclosure is consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained,
- the research purpose for which the disclosure is to be made cannot be reasonably accomplished unless the information is provided in individually identifiable form, and
- the person who is to receive the record has agreed to comply with the conditions relating to security and confidentiality prescribed by the regulations.[52]
- As for law enforcement, both FIPPA and MFIPPA have exemptions for investigations where "...disclosure is necessary to prosecute the violation or to continue the investigation."[53]

Criminal Law

Criminal law in Canada may also have implications for use of fusion techniques. The *Criminal Code*[54] is federal law, which applies nationally, thus all organizations may be impacted by this legislation. It is important to note at the outset that techniques should not be used or seen as being used to facilitate or to perpetrate any of the criminal conduct that they may be capturing. Such a conclusion may indicate that the organization is a party to the offence.[55]

---

[44] (R.S., 1985, c. P-21).
[45] For a complete list of "government institutions" see the schedule of the *Privacy Act*.
[46] *Privacy Act* Section 8(2)(j)(i).
[47] *Privacy Act* Section 8(2)(j)(ii).
[48] R.S.O. 1990, Chapter F.31 [FIPPA].
[49] R.S.O. 1990, Chapter M.56 [MFIPPA].
[50] S.O. 2004, Chapter 3 Schedule A.
[51] See PHIPA s.3(1) for definition of health information custodian. PHIPA may be engaged only where fusion technologies capture personal health information.
[52] See FIPPA s.21(1)(e)(i)-(iii) and MFIPPA 14(1)(e)(i)-(iii).
[53] See FIPPA s.21(3)(b) and MFIPPA 14(3)(b).
[54] (R.S., 1985, c. C-46)
[55] See *Criminal Code* s. 21(1).

Cybercrimes in the *Criminal Code* rely heavily on the definitions of "computer program"[56] and "computer system"[57]. Computer program "means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function" while computer system means:

… a device that, or a group of interconnected or related devices one or more of which,
(a) contains computer programs or other data, and
(b) pursuant to computer programs,
(i) performs logic and control, and
(ii) may perform any other function;

The result is that many cybercrimes would be captured by the fraud provisions wherein such definitions are found.[58] The fraud provisions include: "Unauthorized use of credit card data"[59] , activities such as making, buying or selling any "Instruments for copying credit card data or forging or falsifying credit cards"[60] , "Unauthorized use of computer"[61] and "Possession of device to obtain computer service",[62] "...intercept any function of a computer system".[63]

The *Criminal Code* also contains provisions making offenses of "identity theft"[64] and "trafficking in identity information"[65]. The definition of "identity information"[66] is broad including biometrics, such as a fingerprint, voice print, retina image and other sensitive information such as passport number, social insurance number, health insurance number, driver's licence number or password. This could apply to data captured by fusion techniques.

Furthermore, the *Criminal Code* makes it illegal to intercept private communications without the consent of the originator.[67] Private communication means:

... any oral communication, or any telecommunication, that is made by **an originator who is in Canada** or is intended by the originator to **be received by a person who is in Canada** and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it...[68]

---

[56] *Criminal Code* s. 342.1(2).
[57] *Ibid*.
[58] *Criminal Code* s.342.
[59] *Criminal Code* s.342(3).
[60] *Criminal Code* s.342.01 (1)
[61] *Criminal Code* s.342.01
[62] *Criminal Code* s.342.2 (1).
[63] *Criminal Code* s.342.1(1)(b).
[64] *Criminal Code* s.402.2(1).
[65] *Criminal Code* s.402.2(2).
[66] *Criminal Code* s.402.1
[67] *Criminal Code* s.184(1).
[68] *Criminal Code* s.183 [**emphasis added**].

Given this wording, it is unclear whether this would capture intercepted communication where neither the originator nor recipient is located in Canada. However, there are exceptions to interception as follows: interception with consent of the originator or the person intended to receive the communication,[69] prevention of harm,[70] managing the quality of service of the computer system,[71] and protecting the computer system.[72]

Finally, the *Criminal Code* contains a provision for mischief in relation to data which makes it illegal to destroy, alter or renders data meaningless.[73] This provision also contains language prohibiting conduct that "obstructs, interrupts or interferes" with data.[74] Fusion techniques employed should avoid practices, which could have such effects on data.

Information sharing and Duty to Report

A collective defence strategy would benefit from information sharing. However, there is no general obligation to report crime except for situations potentially involving child abuse/exploitation.[75] Only where there is a perceived benefit to the organization (e.g. a service provider's desire to maintain clean pipes to increase bandwidth), could one envision that incentive to report malicious behaviour would be encouraged. Where, however, information sharing requires capital outlay for new technologies or for administrative processes, organizations cannot be expected to provide them without some compensation.

Anti Spam/Anti-Spyware Law

Canada's new anti spam/anti-spyware law[76] may also have implications for use of fusion techniques. Like PIPDEA, the application of the Act also rests on "commercial activity".[77] The Act prohibits the installation of "computer programs"[78] without the consent of the computer's user or owner. When consent to install the program is requested, it must describe clearly and simply the function and purpose of every computer program that is to be installed.[79]

In addition, if a computer program performs certain potentially undesirable functions, it must bring its "foreseeable impacts" to the attention of the user.[80] The prescribed list of undesirable functions includes:

---

[69] *Criminal Code* s.184.2(1)
[70] *Criminal Code* s.184.1(1)
[71] *Criminal Code* s.184 (2)(e)(i).
[72] *Criminal Code* s.184 (2)(e)(ii).
[73] *Criminal Code* s.430(1.1)
[74] See *Criminal Code* ss.430(1.1)(c) and (d).
[75] See *Child and Family Services Act,* R.S.O. 1990, CHAPTER C.11 at s. 72.
[76] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act [the Act].
[77] See Clause 1(1) of the Act for definition of commercial activity.
[78] The definition is the same as that found in s. 342.1(2) of the *Criminal Code*.
[79] Clause 10(4) of the Act.
[80] *Ibid*.

- collecting personal information stored on the computer system;
- interfering with the user's control of the computer system;
- changing or interfering with settings or preferences on the computer system without the user's knowledge;
- interfering with access to or use of that data on the computer system;
- causing the computer system to communicate with another computer system without the authorization of the user; or
- installing a computer program that may be activated by a third party without the knowledge of the user.[81]

These provisions apply to PCs and computer servers and any electronic devices that allows for the installation of third-party programs — such as smartphones and tablets. Computer programs are exempted if it is reasonable to conclude from the recipient's conduct that the recipient consented to the installation of the programs (*e.g.*, HTML code, Web cookies, javascript code, operating systems, patches and add-ons). Program upgrades and updates are also exempt if the recipient consented to the initial installation and is entitled to receive upgrades or updates.[82]

Potential Legal Challenges with Fusion Techniques

Sinkholing

"A DNS sinkhole server is a system that is designed to take requests from a botnet or infected systems and record the incoming information. The sinkhole server is not under the control of the malware authors and can be used to gain an understanding of a botnet's operation."[83]

What Information is Collected?

Sinkholes collect information on external IP addresses, exact timestamps of when an IP connected, the protocol used, and the port that it is connected on.

Potential legal issue(s): To the extent an IP address can identify an individual, it is personal information. If this information is not de-identified or aggregated, privacy legislation may apply. Breach notification to the victim may be appropriate depending on the organization and its jurisdiction.

How is the Information Collected?

When a malicious actor creates a botnet, he/she creates malware to spread through the botnet. In order for computers to search for the botnet to receive instructions to spread the malware, the attacker registers a domain name(s) to be used as command and control servers. When the computer becomes infected with malware it will look up the domain to receive instructions to propagate. A sinkhole operator will intercept outbound DNS requests. This means that when an infected computer attempts to connects to the domain, the sinkhole disrupts this process and prevents information from being transferred.

[81] Clause 10(5)(a)-(f) of the Act.

[82] Clause 8 of the Act.

[83] *Shadows in the Cloud* at 27.

Potential legal issue(s): As sinkholing results in intercepted communication, it may be an offence under the criminal code. An analysis of the specific facts would be required. Relevant factors may include: consent to intercept, a warrant, or whether the interceptor is a service provider whose actions would constitute exempted behaviour. In addition, if personal information is collected, it must be consented to by the individual, otherwise it would need to meet exemption requirements for collection without knowledge or consent.

How is the Information Used?

Information from a sinkhole may be used to control and prevent an organization's computers from connecting to malicious domains or to identify which computer on a network is compromised. It may also be used to provide detection and prevention of malicious and unwanted activity occurring between organization computer systems and the Internet. In sum, sinkholing information " prevents unwanted communications and is capable of mitigating known and unknown threats hosted on known malicious or unwanted domains." [84]

Potential legal issue(s): If information collected contains personal information it may be used only for the purposes to which the individual consented, otherwise it would need to meet exemption requirements for use without knowledge or consent.

To Whom is the Information Disclosed?
Disclosure of information must be determine on case by case basis. *Potential legal issue(s)*: If information collected contains personal information it may be disclosed only for the purposes to which the individual consented otherwise it would need to meet exemption requirements for disclosure without knowledge or consent.

Honeypots

Honeypots are "traps" used to detect, defect or counteract attempts at unauthorized use of information systems. Honeypots appear to be a part of a network and contain information or resources of value to attackers. In actuality, the honeypot is isolated and monitored, which allows researchers to study threats and to improve security against these threats. In sum, honeypots are designed to be exploited in order to collect attack-exploits and malware.

What Information is Collected?

Honeypots may capture anything from the attacker's identity, login, password and their commands to encrypted SSH sessions, emails, file uploads and details about their targets. *Potential legal issue(s)*: It appears that honeypots capture personal information. If this information is not de-identified or aggregated, privacy legislation may apply. Breach notification to the victim may be appropriate depending on the organization and its jurisdiction.

How is the Information Collected?

There are two categories of honeypots:

[84] Guy Bruneau, DNS Sinkhole, http://www.sans.org/reading_room/whitepapers/dns/dns-sinkhole_33523)

i. *Low interaction honeypots* simulate parts of an operating system, such as certain network protocols. They primarily work by emulating services and operating systems thus appearing to be a single machine, vulnerable to exploit. In some ways, a low interaction honeypot acts like a "listener". It is not collecting malware but details about the exploit in order to better understand what the attacker is attempting to do. Low interaction honeypots are viewed as "less risky" than high interaction honeypot in that the attacker's activity is relegated to the honeypot – there is no access to an actual operating system and , therefore, no ability to attack other systems.

ii. *High interaction honeypots* are systems with real, non-emulated operating system intended to be accessed and exploited by attackers. By giving attackers a "real system" to interact with, the richness of the data available is enhanced. For example, the honeypot would respond like it has been successfully exploited thereby duping the attacker into putting a piece of malware onto the honeypot. This enables researchers to collect actual malware. However, high interaction honeypots are also viewed as "more risky" given that the real environment could enable attacks of non-honeypot systems.

Potential legal issue(s): Low interaction honeypots appear to present a low risk from a legal perspective in terms of how information is collected. That said, care should be taken in use of high interaction honeypots not to facilitate or to perpetrate an attack or harm on another victim. In addition, if the organization is in the private sector and places a computer program (i.e. malware) on another's machine it may be in violation of Canada's new anti spam/anti-spyware law. Lastly, it should be noted that if personal information is collected, it must be consented to by the individual, otherwise it would need to meet exemption requirements for collection without knowledge or consent

How is the Information Used?

With collected information, researchers can determine what computers are out there actively trying to attack other computers and deliver malware. The information may also be used to identify comprised computers around the world and to see what malware is being distributed. Thus, researchers can see new exploits before the public (zero day exploits) and better understand vulnerabilities.[85]
Potential legal issue(s): If information collected contains personal information it may be used only for the purposes to which the individual consented, otherwise it would need to meet exemption requirements for use without knowledge or consent.

1. **To Whom is the Information Disclosed?**
Disclosure of information must be determine on case by case basis.

85

See Lance Spitzer, *Honeypots: Definition and Value of Honeypots*, online: <http://www.tracking-hackers.com/papers/honeypots.html> wherein he says that honeypot information:

> "can then be used for a variety of purposes, including trend analysis, identifying new tools or methods, identifying attackers and their communities, early warning and prediction, or motivations. One of the most well known examples of using honeypots for research is the work done by the Honeynet Project, an all volunteer, non-profit security research organization. All of the data they collect is with Honeynet distributed around the world. As threats are constantly changing, this information is proving more and more critical."

Potential legal issue(s): If information collected contains personal information it may be disclosed only for the purposes to which the individual consented otherwise it would need to meet exemption requirements for disclosure without knowledge or consent.

Packet Sniffing

Packet sniffing is a process, which involves listening or "sniffing" data packets as they travel across a computer network. This process can be conducted for a variety of intents, ranging from analyzing computer networks for the purpose of administration to illicitly attempting to gather confidential data for nefarious ends.

What Information is Collected?

Two categories of information are collected via packet sniffing: (i) header data (information used to deliver the packet to its destination), and (ii) payload data (the contents actual contents of the packet). Header information includes such information as source and destination IP address. Payload information can include plain-text and sensitive information such as user-names and passwords.

Potential legal issue(s): To the extent an header and/or payload information can be used to identify an individual, it is personal information. If this information is not de-identified or aggregated, privacy legislation may apply.

How is the Information Collected?

Packet sniffing is an inherently "passive" activity; the person engaged in sniffing is simply "listening" to traffic flowing across the network and may use the information found in whatever method that suits their purpose. Packet sniffing may occur on both wired and wireless networks and can be conducted by anyone with access to the network without necessarily requiring any special level of access. All one needs is software that may be obtained either as a free, downloadable application or as a commercially available product. The application captures and stores packets as they cross the network. Since these packets are not in an easily readable format, the captured data is then interpreted and analyzed by software called a packet analyzer.

Potential legal issue(s): If personal information is collected, it must be consented to by the individual, otherwise it would need to meet exemption requirements for collection without knowledge or consent. In addition, if the organization is in the private sector it may be prohibited from using a computer program which causes a computer system to communicate with another computer system without the authorization of the user.

How is the Information Used?

The use of such information depends on the intent of the "sniffer". A network administrator may use header information to diagnose network problems. Illicit users may sniff the packets of those connected to a coffee-shop wireless network with the intent of gathering user-names, passwords, or other sensitive information.

Potential legal issue(s): If information collected contains personal information it may be used only for the purposes to which the individual consented, otherwise it would need to meet exemption requirements for use without knowledge or consent.

To Whom is the Information Disclosed?

There is no standard pattern of individual or group to whom this information would be disclosed, as it depends on the purpose of the "sniffer". Legitimate network administrators may sniff packets for their own purposes and not disclose information to anyone. Researchers may using packet sniffing to investigate things such as malware and thus may disclose these results.

Disclosure of information must be determine on case by case basis.
Potential legal issue(s): If information collected contains personal information it may be disclosed only for the purposes to which the individual consented otherwise it would need to meet exemption requirements for disclosure without knowledge or consent.

Deep Packet Inspection (DPI)

"Deep Packet Inspection" (DPI) is a computer networking term that refers to devices and technologies that inspect and take action based on the contents of the packet (commonly called the "payload") rather than just the packet header.[86] Thus, DPI is a "deeper", more analytical look at the packets traversing a network, in order to make determinations about the traffic.

What Information is Collected?

IP packet header and payload information would be collected. IP header information would include such information as source and destination IP addresses. Generally speaking, if the data being transmitted is not encrypted, DPI methods can obtain sensitive information from data payload such as usernames, passwords and the contents of websites visited.
Potential legal issue(s): It appears that DPI captures personal information. If this information is not de-identified or aggregated, privacy legislation may apply.

How is the Information collected?

DPI is a process which must be engaged in by the network operator such as an ISP or corporate IT department. It is implemented by installing specialized devices which inspect packets and adjust traffic based on criteria. For example, DPI may be used in re-routing high-priority traffic, throttling unwanted content or blocking illicit content. This is generally a highly automated process, as one of the primary purposes of DPI is to increase network efficiency.
Potential legal issue(s): As DPI criteria may result in communications being intercepted and blocked, it may be an offence under the criminal code. An analysis of the specific facts would be required. Relevant factors may include: consent to intercept, a warrant, or whether the interceptor is a service provider whose actions would constitute exempted behaviour. In addition, where personal information is collected, it must be consented to by the individual, otherwise it would need to meet exemption requirements for collection without knowledge or consent. Lastly, if the organization is in the private sector it may be prohibited from using a computer program which causes a computer system to communicate with another computer system without the authorization of the user.

How is the Information Used?

[86] https://www.dpacket.org/introduction-deep-packet-inspection-processing

Data collected as part of DPI is used for a variety of purposes. Network administrators may use information gained from DPI for security purposes, examining packets for malware or spam. ISPs may use DPI to prioritize the transit of some types of traffic (e.g., VoIP) over others (e.g. P2P file sharing) in a process called "traffic shaping" or "throttling". Notably, the technology is also used to monitor and block Internet users from unwanted content. DPI could also be used to target advertising to users based on the type of content they are viewing.

Potential legal issue(s): If information collected contains personal information it may be used only for the purposes to which the individual consented, otherwise it would need to meet exemption requirements for use without knowledge or consent.

To Whom is the Information Disclosed?

There is no standard pattern of disclosure for data collected via DPI, and it is still an evolving field. Network administrators and ISPs using DPI to improve network efficiency may simply discard all collected data after automated systems have processed them. In this case, no individual ever looks at the data and it is not stored or disclosed.

However, it is not necessarily the case that data collected through DPI is not stored or disclosed. The technical requirements for an ISP, for example, to collect and store DPI data from many customers would be highly demanding. However, it has been argued that as this process is not transparent, it is conceivable that ISPs could collect and perhaps sell large volumes of data collected through DPI.[87]

There are other potential means through which data collected via DPI could be disclosed. There have been cases of ISPs working with third-parties to direct targeted advertising, while industries concerned with protecting copyrights have worked with ISPs to prohibit file-sharing of copyrighted material.[88]

Potential legal issue(s): Personal information may be disclosed only for the purposes to which the individual consented, otherwise it would need to meet exemption requirements for use without knowledge or consent.

Other Legal Areas for Further Investigation

Intellectual Property

Copying, reverse-engineering malware or breaking technological protection measures (TPMs) may have copyright implications.

Torts
Facilitating the spread of malware exfiltration of code may be seen as negligence.

Contract Law

[87] http://dpi.priv.gc.ca/index.php/essays/the-privacy-implications-of-deep-packet-inspection/
[88] http://dpi.priv.gc.ca/index.php/essays/the-greatest-threat-to-privacy/

Organizations which may be bound to other parties on any number of issues – from service levels and to handling of data or confidential information – may be in breach if they fail to meet such obligations.

Disclosures of Personal Information

There is a dearth of information available on this topic, however, information sharing is a critical piece of an effective cyber strategy.

INVESTIGATIVE FINDINGS

This chapter discusses the investigative process, methodologies and findings to a deep technical level. Here we provide rationale to the experimentation steps, analytical decisions made along the way with frank commentary to limitations, challenges and degree of success.

Executive summary of investigative findings:

Quantifying the risk posed by "dark actors" on corporate networks is challenging. Historically, corporate networks generally were built for resilience and not security. With the exception of some financial and administrative systems, they are mostly open to the public Internet and designed to interoperate and provide communication between the corporate environment and external parties.

In most large corporations, networks were built up over the years on the basis of need. Legacy networks coexist with newer iterations. Systems are optimized and managed for performance, but retiring or rationalizing infrastructure is often difficult in an operational environment. The volumes of traffic are large, and often it is difficult to capture, parse, and analyze in real-time.

Until recently, security of data on corporate networks was not a corporate priority. In the past, network security was by-and-large focused on the illicit use of network resources, or an electronic version of "toll fraud" and something, which could be handled by security tools focus on network performance metrics. Even today, most corporate security systems are designed for static defence providing firewalls and filters designed to inhibit known unauthorized external traffic and to minimize unproductive computer uses by staff. The emergence of cyber espionage, and the use of sophisticated malware as a means of manipulating networks, stealing private, or corporate information, is a relatively new phenomenon against which existing security tools and approaches are not well calibrated.

Corporations are also reluctant to report network security breaches that pertain to the loss of corporate data. Quantifying the value of such losses, as well as the potential negative effect on shareholder value is responsible for the degree of conservatism. Should a corporation report a breach (crime) they are a risk of a fine by the privacy establishment. Thus breach notification punishes the victim and deters in depth proactive forensics. At a practical level, corporations also lack the tools and approaches necessary to capture and quantify dark threat actors, or to quantify losses in a meaningful way. Insurance coverage against losses of confidential information on data networks is scarce and therefore network security remains a function of the Chief Security Officer, and not the Chief Financial Officer.

This experiment was designed to capture and quantify "dark actor activity" on corporate infrastructures. The research was restricted to open source methods, and sought to apply "all source" fusion methodology to the rapid detection of dark actor activities. The data was obtained from two sources: a) Web proxy log files. These files were stripped of any identifiable PII including domain and IP information; and, b) analysis of DNS requests from within the cloud. The experiment operated under several constraining factors:

- **Short duration of analysis** - the project timeframe of just over six weeks was too short to connect initial analysis with an targeted investigation of the identified threat vectors and actors. Time constraints precluded placement of the data discovery/fusion environment within the enterprise as the engineering and legal time required would have pushed us beyond the projects formal end date of 31 March 2011. As a result, the analysis of data was carried out off-line and in a disconnected environment. While this yielded significant results, it did not permit us to demonstrate real-time discovery tools, nor to structure the reporting mechanisms into a common operating picture.

- **Large volume of data** – as the investigation was carried out off-line, we were unable to scan real-time net flows, and as a result had to parse through static data sets which introduced inefficiencies into the analytical method nor to demonstrate real-time entity resolution and persistent search technologies.

- **Need to protect confidentiality of sources and privately identifiable information** - This precluded placing a fusion environment within the enterprise. Consequently, the experiment with structured to test the hypothesis of whether it would be possible to identify threat vectors by unique signatures, which were not dependent on PII. Consequently, the data provided by the sensors was automatically cleaned of all PII before it was passed to the analytical teams.

- **Open-source methods** - the experiment relied on open source methods in order to preserve the ability to publish results in the public domain. While this was not a unreasonable constraint on the research method nor the experiment, short duration of the experimentation precluded further experimentation which would have increased the efficiency, and reduce the time cycle required to test investigation hypotheses. It also precluded access to additional corporate data sets, including human resource records, physical access data, which would have contributed to automated entity resolution, and identification of zero factor vectors within the cloud.

The experiment was carried out between 1 January 2011, and 15 March 2011 and considered a **qualified success**, mostly on account of the constraints placed by the short duration, and need to maintain open methods.

The research was carried out by two analytical teams. The first analytical team worked with visibility on the providence of data sets, and the objectives of the overall exercise. The second analytical team worked with anonymous data and without the knowledge of data providence. The second team focused on determining whether specific threat signatures were sufficient for developing criteria for automated entity resolution.

This report is written in two parts.

Part one provides a summary report of the research conducted under the experiment and its results.

Part two consists of two brief supporting documents: a) A research note summarizing the use of different analytical tools against the data sets by the open-source team; and, b) a summary report detailing the methodology and findings of the Look Back component.

Summary the Experimentation

Objectives:

The objectives of the experiment were to apply all source fusion methods and advanced analytics to the discovery of "dark actor" activity on the infrastructure. The experiment was framed by a number of constraints, including the short duration allocated to the experiment, and the requirement to use open-source methods in order to preserve the ability to make research results public. This meant that the all source fusion environment was not located within the firewall, and the available data sets were cleaned for any personally identifiable information. Likewise, the experiment did not have access to other supporting data sets, which would have aided in automating and creating automated entity resolution systems necessary for real-time detection within a unified common operating picture. The experiment was restricted to analyzing statistically meaningful data sets consisting of Web proxy log files originating from: a) assigned ranges and b) IP addresses associated with the cloud (publicly visible IP ranges).

As a secondary objective of the experiment - necessitated by the constraints on method - was to test and validate a two step methodology for rapidly parsing large-scale data sets derived from operational data, suitable for analysis within an and protected public research setting. This approach protected confidential data, as well as sensitive information relating to the structure/operation of the infrastructure, while ensuring access to operational level network data. It created conditions that allowed the experiment to experiment focus on detection behaviour based on limited data points, limited time, and access to anonymized data. As such, it provided a useful proof of concept for non-invasive analytical tools and methods, which also validated the all-source method for detection of threat factors.

The research was divided into two components to ensure that privately identifiable information, and/or confidential information was excluded from data passed to researchers working in a public university context.

Part 1 - consisted of research carried out by a team with access to data (primarily network topography and anonymous addressing)

Part 2 - consisted of a University-based team, which worked with clean data, but possessed no PII or other means to identify the origin/source of data to be analyzed.

Look Back – was a unified re-examination and correlation of all data by third team of analysts with full visibility and optics over the experiment. This component was carried after the completion of the previous analytical work and leverage knowledge of data providence in the resulting analysis.

The work of all research teams was monitored and directed by principal investigators, legal/privacy and security oversight with visibility on both sides the project.

Methodology and sources

Part 1 - This component of the research analyzed DNS requests to known malware domains originating from within the cloud. The IP ranges analyzed included those provided by the infrastructure (corresponding to IP space, dark space, and public infrastructure. The research relied on data from two SOA sensors and examined data between 3 and 28 February 2011. Sensor "A" - monitored for 56 known malware types, and analyzed data between 23 and 28 February 2011. Sensor "B" - observers ~ 70 MB DNS requests per day from a dynamic DNS network that is heavily used by malware operators. Statistical analysis supports evidence that upwards of 60% of DNS requests to this network originates from malware. Data from the Sensor "B" was observed over 24 hour period, and analyzed into known and suspected malware connections. Suspected malware domains were subsequently cleaned of originating IP/domain information and passed over to the other team for further analysis. The known and identified malware connections originating from bill ranges are passed to the infrastructure team for further investigation. This method provides a snapshot of malware activity on networks corresponding to known and suspected malware. It is not a comprehensive listing of all our connections.

Part 2 - This component of research analyzed file path structures and requests, derived from an analysis of outgoing HTTP proxy logs supplied by the infrastructure. The file paths were stripped of originating IP/domain information, so as to prevent the inadvertent transfer of PII to the research team. However, time stamped data was preserved in order to aid time-series studies of recurrent connections. The data was gathered from four NetApp proxies, between 28 January and 19 February, 2011, in two batches. Batch one consisted of a single day sample (28 January) of approximately 812 MB (compressed). Batch two consists of over 80 GB (compressed), corresponding to two weeks worth of log files (1-19 February). The file path calls were analyzed for signatures known malware, or connections to IP/ domains, suspected/known to be used by specific malware. The resulting list of domain/IPs is compared/ analyzed the list of known and suspected malware domains generated by the previous team. Domains that do not correspond to the previous lists are further analyzed, and where warranted honeypot in order to determine the characteristics of suspected malware, or exclude malware activity.

Suspected/known malware was triaged into four categories: i) known, ii) unknown, suspected targeted APT, iii) unknown, suspected commercial, iii) unknown. All four categories are further analyzed using the Zeropoint and palantir platform to create a typology of malware infections, and identify vector/events which could be used explain: a) nature and origin of threat, b) event/cluster analysis, c) identify possible mitigation strategies.

Research yields comprehensive data on structured requests originating from infrastructures in a manner that shows/protects the identity of the networks, and other PII from public space investigators. The absence of originating IP information, however, makes it difficult to link specific file path requests mixed it difficult to link identified malware with specific infections occurring within the cloud without significant follow-up investigation of the malware command-and-control domains.

Look Back - In early April 2011, a sample of the data was reanalyzed by a third team to provide a baseline of the data and determine which methods best extract indicators that may identify undesirable or malicious traffic. The sample used was limited to 24 hours selected from the larger data pool using criteria which helped isolate potential "dark actor" activity.[89] Look Back validated the findings of the previous research team with respect to the difficulty of matching anonymized signatures with specific threat vectors. While it discovered indications of unwanted and possibly malicious traffic, validation requires an ability to directly link back to IP/domain information and other functional aspects of the affected systems.

Experiment results

Part 1

An analysis of DNS log data was carried out 1 to 4 March 2011, yielding the following results:

- An analysis of data yielded **10,505,603** malware URL requests, of which **3,075,931** corresponded to unique malware URL's.

- Multiple requests to Zeus bottom controller from DNS servers. Two DNS servers made multiple requests to a domain exclusively used for a Zeus botnet between 23 and 28 February 2011.

- Multiple connections to known/malware/APT command-and-control domains from 64 DNS servers within the cloud. As a sample, we examined 379 unique known C&C domains that were requested from name servers over a 12 hour period on 3 February 2011. These were plotted across ASN's in order to visualize and analyze the relationship between CNC domains, DNS servers, and ASN's (figure 1).

89 The data chosen for analysis represents a timeframe from 1100 hrs. sunday night to 1000 hrs. monday morning to exclude normal network noise, and isolate instances of workstation reboot and suspicious traffic flows.

- 6603 requests to domains known to be associated with malware from public DNS servers over a 24 hour period although none appeared to correspond to assigned DNS servers.

These results are inconclusive owing to the structure of the experiment. The structure of the experiment precluded automated data discovery and fusion in order to validate originating IP addresses with other criteria, including workstation location and function. As a consequence, while there is high confidence in the detection of malware behaviour, the research team did not have enough access to the infrastructure to determine whether the traffic was being from assigned ranges, operated dark space (honey nets), or public networks nor to construct an exact entity (profile/signature) of the factor sufficient to create an automated detection profile.

Log Data -I

An analysis of log data-I data was carried out 1- 14 February 2011 by the open-source team who was not aware of the providence of the data and focused on the isolation and identification of vector signatures based upon file path calls. The data consisted of 170 files (about 2.8 GB uncompressed), each of which summarized the number of times a unique file path was requested over a particular timespan. Data corresponded to one day's worth of log file (28 January 2011).

The sample set yielded a number of parliamentary findings:

- The sample contained file path calls, some of which correspond to typical malware signatures. However, the investigation was inconclusive as the script used to strip out identifying and originating IP information also stripped out critical file path information, including those parameters used to define specific filed retrievals and/or the executable to which the path pointed (for example, GET query parameters (i.e. any text after the '?' character in a path).

- Numerous issues of operational security, and other information security practices including login/password sent as clear text, connections containing unsecured/unprotected credentials to services, as well as banking services, file servers, and other web-based sites.

On the basis of the sample, a new script was regenerated and apply to gather data corresponding to two weeks worth of traffic in February. In addition to resolving the truncated file path calls, the data now includes timestamp data, which will enable longitudinal analysis. This traffic is data is currently under investigation.

Log Data -II

An analysis of the second data store was conducted the week of March 25, 2011. This data set consisted of 631 log files for four HTTP proxies over a total of 30 days, including timestamps and GET parameters. Roughly 5.3 million requests per file, altogether about 300 GB uncompressed.

Larger data set provided additional analytical findings:

- The larger sample provided evidence of suspicious activity, but the follow up calls themselves were not sufficient to positively identify malware calls. In total, to file path calls were positively matched up with malware infections - Zeus based bot nets, and a twitter/Facebook worm. These appear to be "garden-variety" opportunistic infections rather than targeted threats although the absence of domain and IP information made it impossible to determine their exact target/activity. The Zeus botnet, for example, was using default parameters, which aided automated discovery in ways which would not be possible for deliberately obfuscated networks.

- Some suspicious traffic was revealed to be encrypted on-line game data and traced back to a server in Germany. While it's possible that this might represent a malware threat, it could also be a representation of usage by users. Without domain and IP information, as well as an ability to correlate this activity with user function is next to impossible to make a positive determination as to the nature/intent of this activity.

The Logs I and II analysis yielded the qualified success. Analyzing file path calls in a big data environment proved challenging when dealing with analyzing anonymized data. In an off-line environment, the analysis of big data creates a problem as entirety of the data set needs to be analyzed for patterns rather than through the creation of persistent searches against pre-resolved entities and target profiles. Without "knowing" what you're looking for, the task of parsing raw data becomes problematic, even with the use of the data pre-processors. At the same time, the experiment provided an opportunity to use several data pre-processors including a customized job application which should be a welcome addition when the system is implemented on a live in stream data set (summarized in part two of this report).

Look Back

This experiment examined a correlation between the all data sets. A sample was selected from the log II data which represented a 12 hour time frame selected in order to reduce network noise and isolate potential malware traffic. This sample yielded a total of 6,063,788 URL file path calls. This was correlated and compared against the 3,075,931 malware URLs from the initial data set. The data was grouped into low, medium, and high probability, based upon direct high probability matching of URL depth level.

The time epic of 12 hours yielded:

- 47 direct matches (level IV depth matches)
- 13,902 medium probability matches (level III depth matches)
- 59,000 low probability matches (level II and I depth matches)

The Look Back exercise was a success and yielded a valuable matching between externally detected malware calls and the anonymized infrastructure data sets. The ability to detect direct correlations and reduce false positives to manageable numbers indicates that it would be possible to build a fusion environment for rapid threat identification and mitigation even without access to data sources.

The Look Back team also constructed a series of preliminary targeting templates that could be applied against high-value threats (level III and IV depth matches), for tracking and mitigation purposes.

Preliminary Conclusions to the Investigation

General security observations - Cloud

1. The data suggests a systematic pattern of infection affecting the cloud, which is not being captured by existing network-based detection systems (IDS), nor filtered by firewalls, et.al.

2. An analysis of log files suggests vulnerabilities arising from poor/insufficient attention to operational security by users operating from within the cloud that could lead to the compromise of systems and loss of data. This is not strictly speaking a problem that can be addressed by technical controls but rather one of user education.

Methodology

1. The component, consisting of intercepting DNS requests to known C and C domains was highly effective against malware using the DNS system. It allowed for the positive identification of file path calls based upon unique URL requests, which could be directly applied, to the identification of threat vectors within the cloud without resorting to PII. However, the system does not capture malware which does not use the DNS system. Consequently, as malware evolves to use multiple channels of communication, including peer to peer network and IPv6 tunnelling this method will decline in resolution.

2. The approach of using anonymized data proved moderately successful in detecting malware connections, but proved inefficient as the analysis of static data does not allow for the creation of on-the-fly persistent searches and or resolve entities that would allow for a real-time assignment of

risk against specific threat vectors. At the same time, the experiment proved that the approach of working with anonymized data can yield usable threat information.

3. The Look Back exercise provided a typology of risk based upon the ability to match derived malware file, path strings with generated file path calls at the unique URL level, and segmented into categories. These categories can be effectively employed as a targeting template within a in stream/online implementation a data fusion environment and provide near real-time detection. This, in turn can serve as the basis for a real-time mitigation system.

Next Steps to the investigation

1. The experiments proved it's possible to create a prioritized threat vector based upon an analysis of off-line information in near real-time. Initial work on templating the risk factors indicates the practicality of implementing the template in real-time on a detection/visualization environment such as Zeropoint and palantir when located within an advanced analytic centre (or with access to such data on demand).

2. Prioritized threat vectors (level IV level III), will be subject to a scanning analysis similar to that undertaken during the Ghostnet and Shadows investigations. We hypothesize that the application of similar investigative techniques, which include domain and IP herding to allow for the rapid mapping of threat vector ecology's and provide decision-makers with a graduated response metric.

3. Implementation of a pilot Zeropoint and palantir-based data discovery infusion instance within the infrastructure in order to pilot real-time detection and develop appropriate mitigation strategies, including a national 'clean pipes' strategy.

Supporting research notes to the Investigation

Visual Analytics and the Dataset

The purpose of this document is to summarize our experience using visualization tools in the course of analyzing the datasets. To give some context I'll briefly describe the data we received and the general approach I took before discussing the three visualization tools I used: a custom Java-based application, Tableau Desktop, and Zeropoint and palantir Government. I'll give a few examples of how I used each and then summarize some of the strengths and weaknesses of Tableau and Zeropoint and palantir.

Data Descriptions

Log Analysis I - The initial data we got comprised 170 files (about 2.8 GB uncompressed), each of which summarized the number of times a unique file path was requested over a particular timespan. This did not include GET query parameters (i.e. any text after the '?' character in a path) or the domain components of the requests. The goal was to see whether we could determine the domain from the requests, and/or whether the request could be considered malicious.

Log Analysis II - The second drop was much larger. 631 log files for four HTTP proxies over a total of 30 days, including timestamps and GET parameters. Roughly 5.3 million requests per file, altogether about 300 GB uncompressed.

DNS Logs - A collection of recursive DNS name server IP addresses and the domains they were observed to be requesting. Some of these domains are known botnet C&C addresses.

General Approach

The large size of the data precluded it from being loaded directly into most graphical desktop applications. We also ran into difficulties trying to load it into a database. I suspect that running database queries would have been quite slow anyway. Log files of this size are most effectively dealt with by using standard unix command-line text processing tools such as grep, sed, awk, cut, sort,

uniq and wc augmented with a general purpose scripting language (in our case Python). The analytic process was structured roughly as follows:

- Inspect the files manually (using less and grep to page through logs)
- Process log files to reduce noise and extract entries of interest
- Generate aggregate and summary data
- Load into desktop tools (spreadsheet, visualization applications) for analysis
- Use other sources (Maelstrom, Google) to check up on requests that looked interesting
- Go back to step 2 and use anything we learned to refine our queries

Visualization Tools

Custom Java application

Upon first receiving the data, we wanted to get a sense of its overall structure. A good way to visualize temporal coverage is with a floating bar chart (like a Gantt chart). We also wanted to display various characteristics of each log in a table, with linked selection between the table and timeline. We wrote a Java application using an open source library called JFreeChart, with some minor improvements to its Gantt chart module. Some of this would be possible to do natively with Zeropoint and palantir, but not all, and the overhead of writing a custom helper would have added to development time and therefore reduced the time spent on actual analysis.

The first version of this tool, designed for the initial dataset, also had the ability to display and drill down on file extension details and display scatter plots for various characteristics. Pre-processing (filtering, splitting up and summarizing) was necessary due to the large amount of data. This was a good exploratory tool in that it allowed us to answer a range of questions about the kinds of files being requested, even if no compelling insights came out of it.

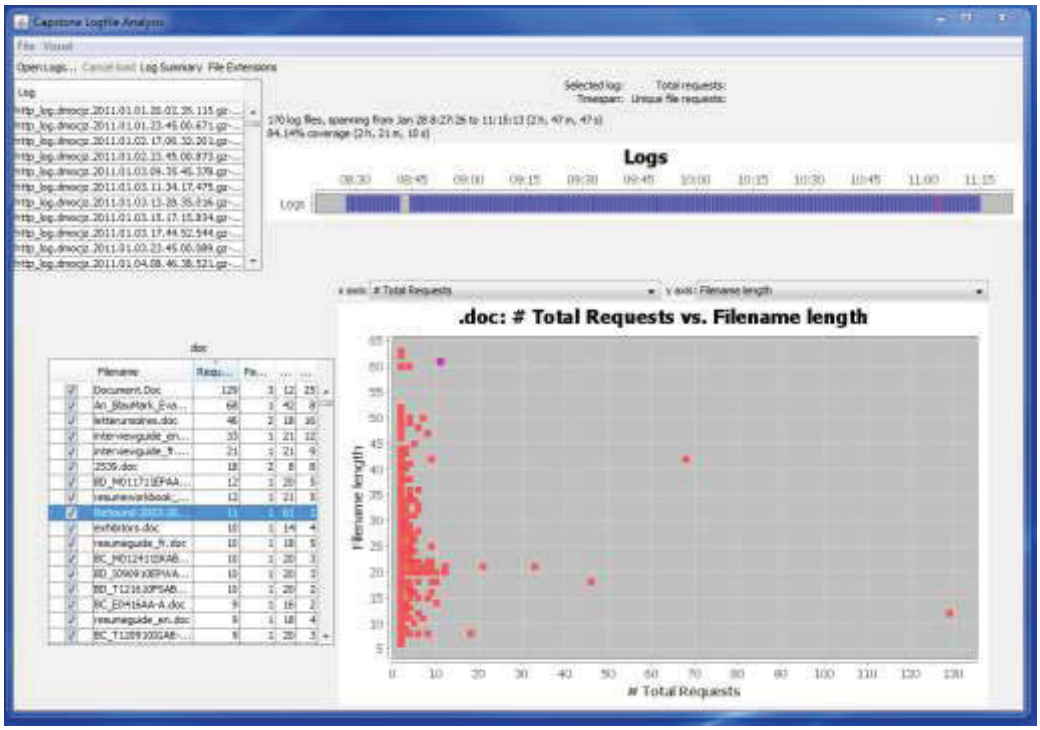


Figure 2 – A custom Java-based visualization tool for the first set of Log data

The second set of log data required some modifications to the application -we wanted to capture the proxy name dimension, and our experience with the first dataset led us to not bother with the file extension portion. Instead, I added the capability to load in arbitrary summary information for each log file from a CSV file so it could be used to sort the table and be seen in tooltips. For example, we wrote a script to calculate the percentage of requests in a log file that corresponded to requests that were found in Maelstrom (a system for capturing the network behaviour of malware). This gave us some indication as to which files might warrant a closer analysis (see Figure 2).

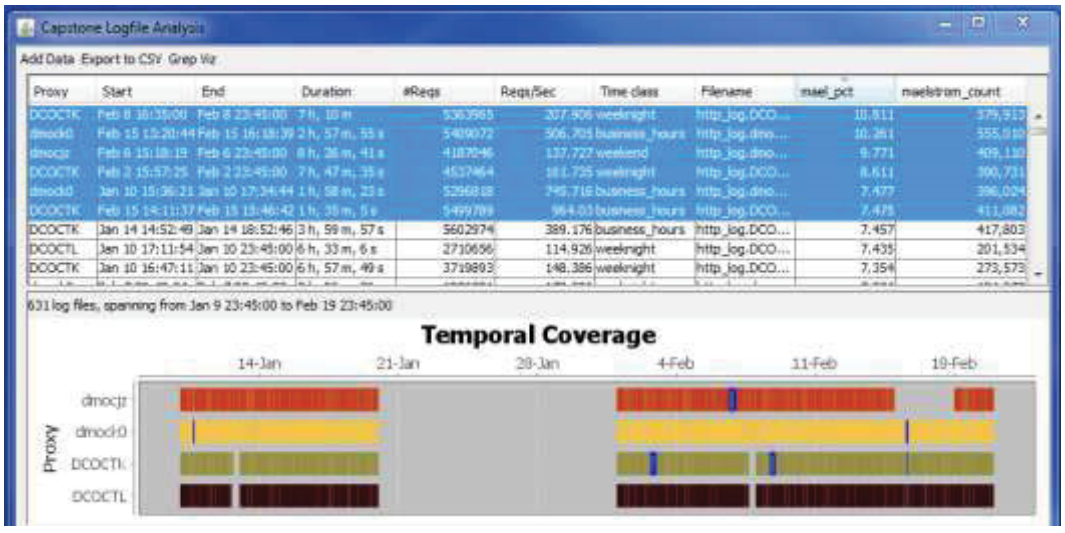


Figure 3 – Log files sorted by % overlap with Maelstrom, with the top six selected.

At the request of another analyst we also added a feature to display the results of a grep search of the log files. This allowed us to very easily check whether a given request string was occurring at regular intervals, and thus the likelihood of the request originating from a human or machine (see Figure 3). Similar functionality would have been possible to do with Zeropoint and palantir's timeline, but more awkward and the stacked bar chart nature of the timeline would make it more difficult to compare across proxies.

As we were already familiar with Java and the JFreeChart library we were able to develop this tool reasonably quickly. Altogether we spent roughly three and half days (twenty-eight hours) writing it, including the time to retrofit it for the second dataset. It gave us a good overview of the data and allowed us to find some interesting temporal patterns. Being able to easily tack on new summary data as our scripts finished running was also helpful. However, for the second dataset there wasn't much ability to drill down into request-level details, nor to visualize the data aside from the floating bar chart timeline. Rather than reinvent the wheel and add more charting features, we wrote a feature to export the table data to CSV format so it could be loaded into other tools. Along with the ability to import arbitrary CSV data for each log file, this gave us an easy way to combine the various outputs of our summarizing scripts into a format that other programs could easily use.

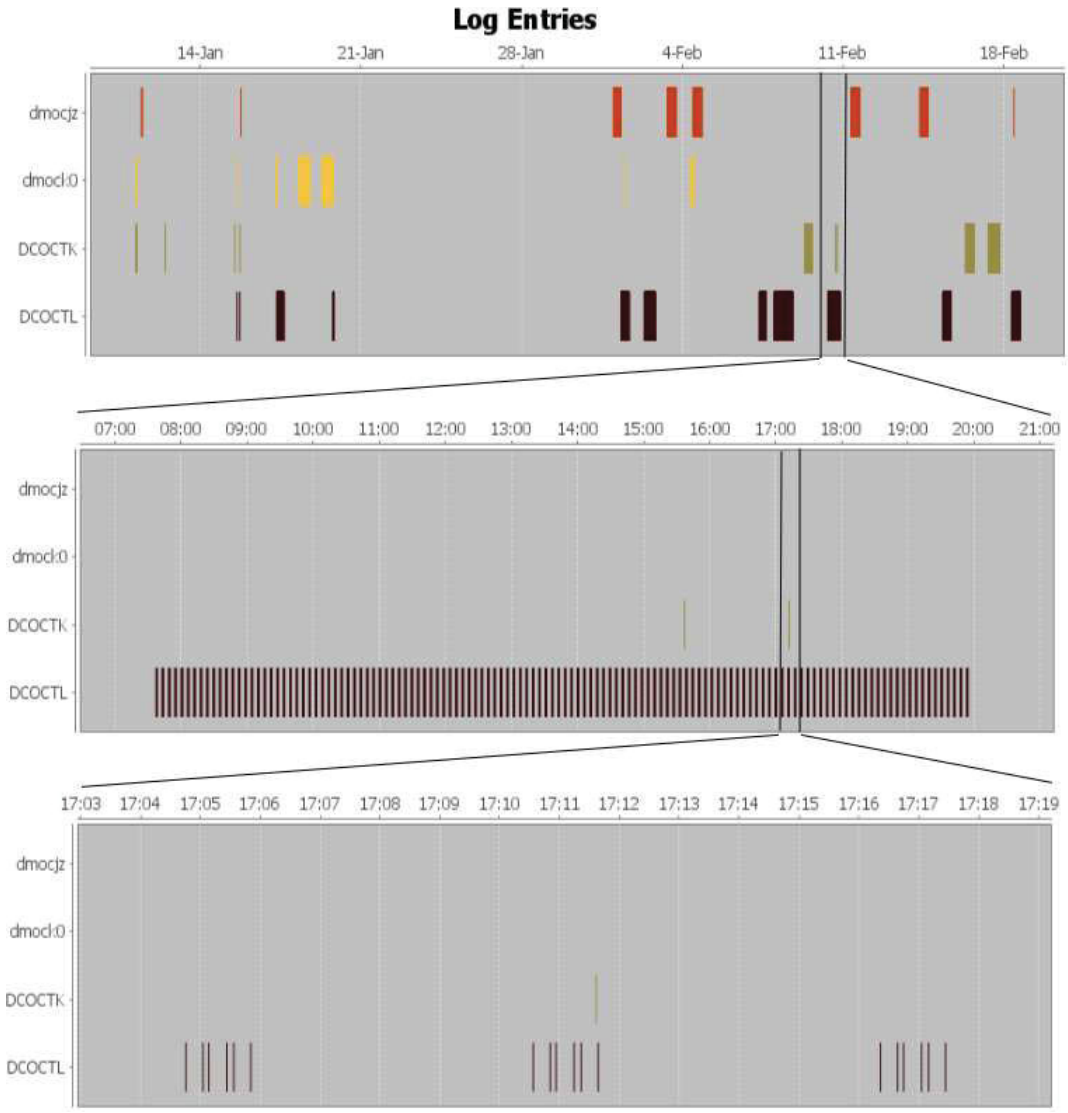


Figure 4 – The results of a grep search for "i.php" in the log files. The ability to zoom in is built in to JFreeChart.

Tableau Desktop use in the investigation

Tableau is visualization software that specializes in business intelligence but is applicable to a broad range of multidimensional data. It could be described as "pivot tables on steroids" and is quite easy to use. It reads CSV, XLS, etc. and the Professional edition can connect to databases. By dragging and dropping the dimensions and measures of interest as columns and rows, then selecting from a number of visualization options, you can very quickly create many different charts. It has "best practices" for charting built in, meaning that it can often select a reasonable visualization for the data automatically and guides you towards creating charts with scales and features that are

appropriate for the data you're interested. Figure 4 shows the UI for Tableau along with an alternate visualization of the percentage of Maelstrom overlap in the second Log dataset.

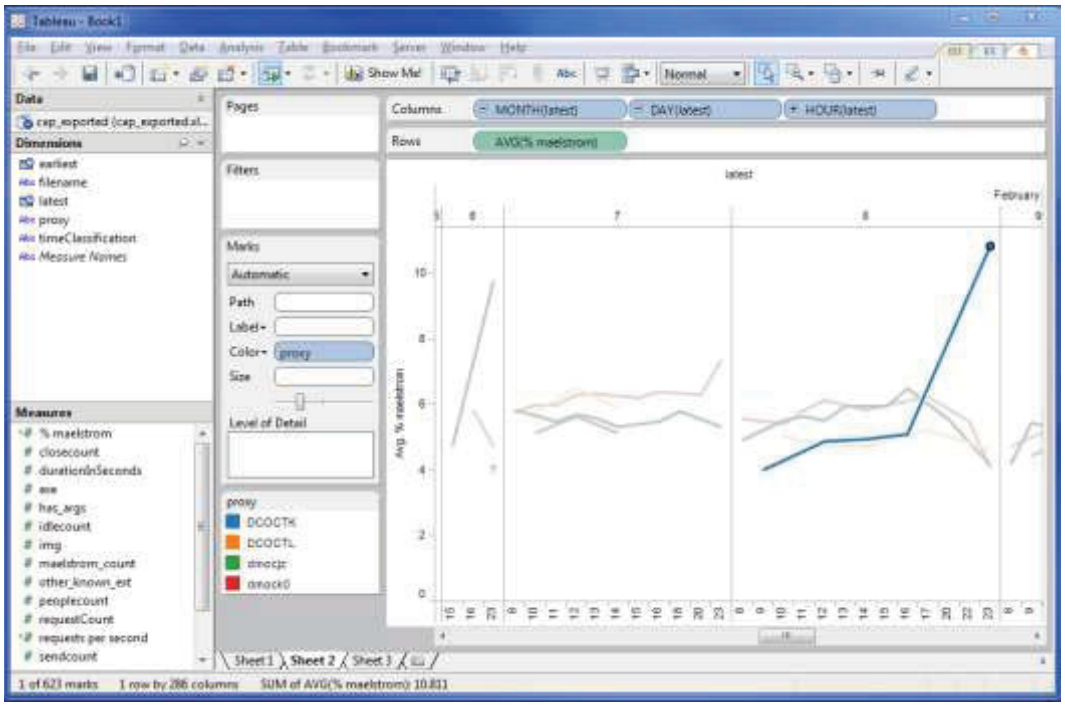


Figure 5 - Tableau Desktop showing Maelstrom request overlap by log file. Obvious spikes appear on Feb 6th and 8th.

Tableau has strong support for plotting multidimensional data. For example, we had categorized each log file as corresponding to business hours, weeknight or weekend and were interested in how the Maelstrom overlap metric varied amongst these classifications as well as by proxy. First of all, we used a similar chart to the one shown in Figure 4 to double-check our classification heuristic and it did in fact expose a bug. After that was fixed, we was able to create a small multiples plot very quickly to answer the question (see Figure 5 - there were no obvious standouts). Another nice feature is being able to define calculated measures – for example, to create a "requests per second" field we simply added a new measure calculated as requestCount/duration.

We started using Tableau relatively late in the analysis phase and have only scratched the surface of its capabilities. It was primarily using it as an exploration tool, looking for any clues in the aggregated data that suggested a more in-depth look. There is a lot of potential for its use in our analysis, both for data exploration and presentation.

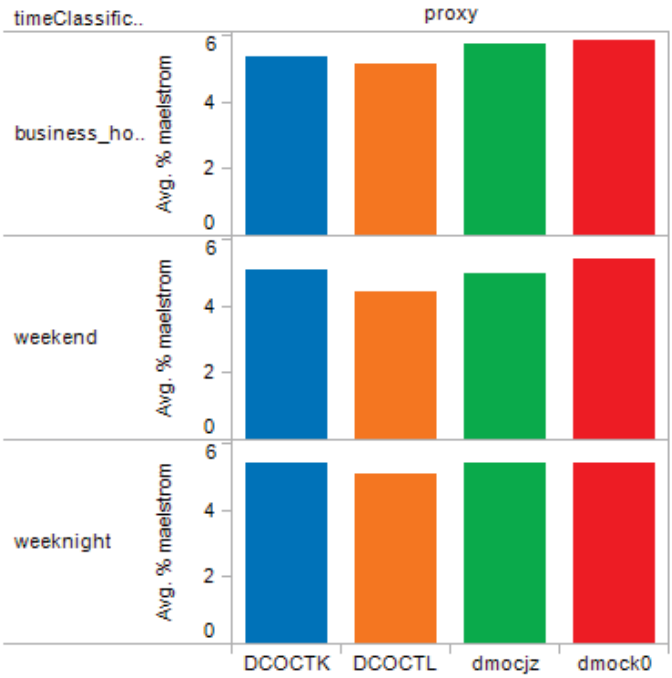


Figure 6 – Small multiples plot in Tableau: Maelstrom overlap percentage by time classification and proxy

Zeropoint and palantir use in the investigation

Zeropoint and palantir is a platform for integrating, analyzing and visualizing data from multiple sources. Its main interface is a graph-based view that allows an analyst to search and discover relationships between entities based on their properties or events that connect them. Various "helpers" are included, such as a timeline view for temporal analysis and a histogram panel for comparing the common features of the currently selected objects. It is possible to create new helpers via a Java API.

A number of other "applications," or primary views, are also integrated. One of these, Object Explorer, assists with interactive exploration of data by letting the user filter on various properties; drill down on data with certain characteristics, and save search patterns for later use. Although this is the most applicable feature of Zeropoint and palantir with respect to analyzing the Log data, it relies

on each record having a reasonable number of already identified features that can be used to drill down and filter on. There are a number of intrinsic properties that could be extracted, such as request length, file type, time of day, day of week etc. However, these are not particularly useful for identifying malware-related requests.

Using Zeropoint and palantir to correlate the Log data with the requests from Maelstrom would have been possible, but we chose not to use it because it does not play to Zeropoint and palantir's core strengths, aside from scalability. The idea of the Object Explorer is to iteratively refine a large dataset into a manageable number of entities or events that can subsequently be analyzed in more detail. Considering a request to be malicious because it was seen by Maelstrom leads to a huge number of false positives, to say nothing of the false negatives (which would almost certainly be the more sophisticated / APT variety). Zeropoint and palantir's charting capabilities are limited to basic histograms and the timeline; although these can be powerful when used in conjunction with other views, they lack flexibility.

On the other hand, Zeropoint and palantir is quite useful when it comes to analyzing and visualizing networks. I used it to look at some of the DNS log data. The graph view, combined with the histogram and timeline, can help make certain patterns apparent and convey a general sense of structure. It is not a panacea; visualizing too many interrelated nodes creates a hairball that doesn't provide any insight. Unfortunately this was the case with the data from the first DNS log sensor. Although not directly related to the goals of the Log project, visualizing connections recorded by the second DNS log sensor provided an overview of which C2 servers were being hit by multiple ASNs and which were more isolated. This is of dubious analytic value for our own purposes, but illustrates how useful spatial clustering can be and shows strength of Zeropoint and palantir – it works well as a presentation layer.

Summary to analyst notes

The key to effectively using visualization, or indeed any analytical methodology during the course of an investigation, is identifying the question at hand and then choosing the appropriate tools and techniques that can help you answer it. Tableau and Zeropoint and palantir are both very powerful applications in their own right, but generally fit distinct use cases and should be considered complementary. The following discussion of the strengths and weaknesses of each encompasses more than just what came out of the Log analysis, but should not be considered exhaustive as there is still plenty for us to learn about both.

One of Zeropoint and palantir's primary strengths is how it enables an analyst to bring in data from multiple, disparate sources and integrate them in a way that facilitates searching for linkages. Its object resolution capability, allows new properties, relationships and events to be added fairly easily.

Zeropoint and palantir is ontology-agnostic, meaning that the entities, events, links and properties an analyst works with are fully customizable. This has the great benefit of making the platform applicable to a wide range of domains; however, it works best when the ontology is entirely pre-defined, which may be an unreasonable requirement when conducting investigations where the exact characteristics of the data encountered is unknown beforehand.

Zeropoint and palantir's graph view is a nice way to explore relationships between objects and display them in an attractive manner. Its layout algorithms aren't as sophisticated as those found in tools such as yEd (yworks.com/yEd), but adopting the workflow of selecting nodes of interest, grouping them as a grid and then placing and pinning them often works well. When dealing with large datasets, it is important to use the SearchAround feature to narrow the scope of searches; introducing too many related nodes can be overwhelming and counteract the benefits that visualization provides, namely exploiting the human brain's ability to recognize visual patterns.

Zeropoint and palantir excels at allowing analysts to discover and visualize links and relationships, and its histogram can be quite helpful when comparing various properties and drilling down on items of interest. However, histograms are just one of many ways to visualize quantitative data.

This is where Tableau comes into play. As a general rule, any time you're interested in visualizing quantitative spreadsheet or database data it is probably most easily done in Tableau or a similar tool (e.g. TIBCO Spotfire). Built-in chart types range from bar charts (stacked or unstacked, with or without lines) to histograms to scatter plots, bubble charts, time series etc. Built-in support for small multiples and being able to drag and drop measures of interest as columns or rows makes it easy to slice and dice multidimensional data. This is useful for data exploration, and once an interesting relationship is visualized it is also very useful for presenting the data.

For both Zeropoint and palantir and Tableau, it is important to recognize that any analysis done with them can only be as good as the underlying data. The Log data was very noisy and we had few effective options for figuring out which requests were malicious with any confidence. Additionally, with these tools the user should recognize that raw data is not always appropriate for importing. Tableau can extract relevant dimensions and aggregate data on its own when given a properly structured table. Importing data that has already been aggregated is typically the wrong way to do it.

Zeropoint and palantir can handle unstructured data such as documents, which is helpful in terms of it being a general information repository. But care must be taken when importing structured (CSV or XLS) data. Doing some preliminary analysis and pre-processing of data before putting it into Zeropoint and palantir is crucial for using the application to its fullest potential. Most important is having clear mappings of properties and relationships to the ontology. Any noise reduction that can be done before import will also be very helpful. In other words, triage and cleansing of data is best

done before importing into Zeropoint and palantir. The process of modifying data after the fact is somewhat slow and painful.

Zeropoint and palantir with the cyber 'zeropoint' component should probably be considered an end-point for the analysis of many types of data, particularly when relationships based on shared properties or events are involved, or a number of different sources need to be integrated. However, other tools and techniques are generally necessary to collect, cleanse, process and triage data before it ends up in Zeropoint and palantir. Tableau is much better than the visualization tools built in to typical spreadsheet software, but it is also dependent on how its data sources are structured. As such other programs, such as text processing utilities and ad-hoc applications, are very useful during the initial stages of analysis.

Look Back Exercise - approach and summary

A standard sample was taken to provide a baseline of the data and determine which methods best extract indicators that may identify undesirable or malicious traffic. This data set represents a Sunday night 11pm and the start of a Monday morning to 10am, this time frame provides a quality perspective of operational traffic as well as workstation boots and resumes.

Database summary tables for the data were defined and an import script was written to extract, log and summarize the data set. A main summary table was established to provide a summary of each URL, first seen, last seen, and count, the script also extracted the last 3 elements of the path(e.g. x/y/z) with each level of detail (x/y/z, y/z, z) treated as a logical shard within the database as key value pairs. Additional modifications and extractions occurred during import to maximize index performance, for overly long strings such as base URL's the MD5 (char32) of the URL was calculated and used as the primary key.

The imported file logged 6063788 Total URL's out of 6071349 lines within the log file. The 7561 records not imported were the result of characters within the URL string escaping quoting during the import process, or with a length greater than 2048 characters (limit set on column). With additional focus on the log formatting and/or parsing (additional quoting of the URL string) these issues can be resolved.

Timing

The sample processed in approximately 25 minutes, additional samples imported into empty databases had similar results. Full URL summaries over multiple samples caused the system to start swapping indexes to disk due to memory utilization slowing the system down considerably; additional tuning was performed but proved negligible. More capable setups could handle significantly more data that can be quickly analyzed. Uncached queries executed full table compares between 5 and 90 seconds, with cached query results returning in milliseconds.

From the **6,063,788** URLs imported, the data was summarized by the URL Path provided the following summary counts

10,505,603 malware URL requests were then extracted in the exact same manner resulting in a summary total of **3,075,931** unique URL's.

Accuracy and Correlation

Due to the data not correlating directly back to an IP address, the depth at which the URL matched represents a correlation to activity related to malware and can be used to gauge overall accuracy of the result. Results with a URL depth of 3 represent the highest match to malware communication.

Correlation was performed between the data sets through the use of joins on the relevant URL depth. Because legitimate sites are requested from malware quite frequently, the results provide only a dissemination of information into a form that may be actionable by other mechanisms to determine maliciousness or ill-intent.

Direct correlation of malware and sample data was performed; this comparison resulted in 47 unique URL matches and provided no real actionable information.

Findings

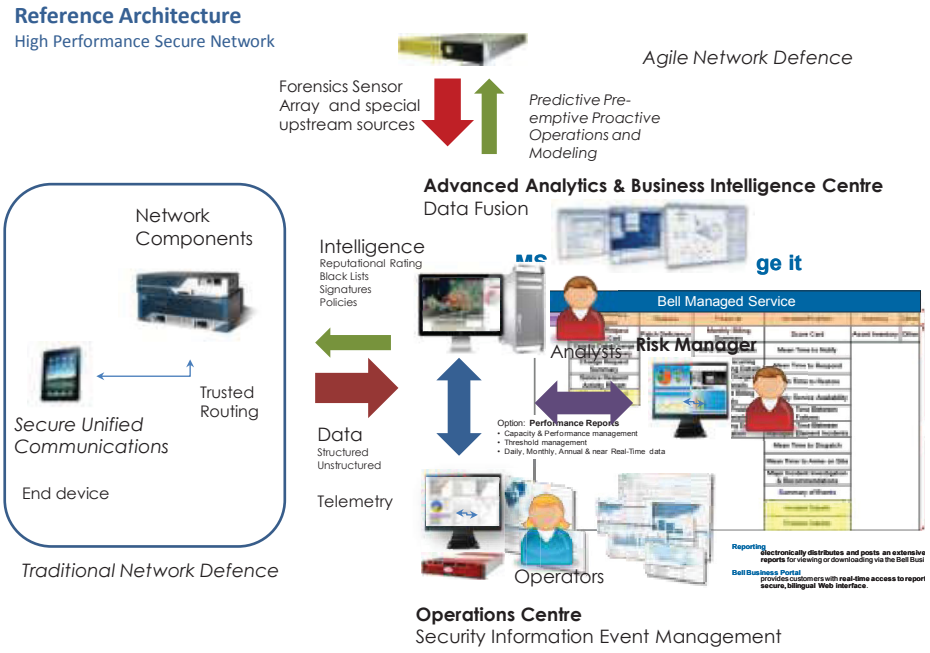
The results show indicators of unwanted traffic. Each view on the depth of the URL provides a different perspective. Ultimately the results would need to be correlated back to real life host activity to determine if legitimate URL's are being abused in some manner.

Scripts with a URL Path Depth greater than 30 were examined, one particular URL pattern was noticed, this pattern examined these 2 URL structures for the directory /uwc 100 times each. This could be a misconfiguration or other random traffic. However, it does demonstrate additional insight that can be gain by modifying the parameters of the path extractions.

/_vti_bin/uwc/auth	/MSOffice/uwc/auth
/_vti_bin/uwc/uwc/auth	/MSOffice/uwc/uwc/auth
/_vti_bin/uwc/uwc/uwc/auth	/MSOffice/uwc/uwc/uwc/auth
/_vti_bin/uwc/uwc/uwc/uwc/auth	/MSOffice/uwc/uwc/uwc/uwc/auth
/_vti_bin/uwc/uwc/uwc/uwc/uwc/auth	/MSOffice/uwc/uwc/uwc/uwc/uwc/auth
/_vti_bin/uwc/uwc/uwc/uwc/uwc/uwc/auth	/MSOffice/uwc/uwc/uwc/uwc/uwc/uwc/auth
/_vti_bin/uwc/uwc/uwc/uwc/uwc/uwc/uwc/auth	/MSOffice/uwc/uwc/uwc/uwc/uwc/uwc/uwc/auth

THE SOLUTION

This chapter discusses effective defensive strategies particularly against advanced persistent threats and sophisticated targeted e-spionage campaigns, in the context of rapidly emerging technologies and threat tradecraft. A reference architecture for high performance secure networking© is provided as is a model for advanced analytics. This constitutes the foundation of a national 'clean pipes' strategy and well as a defacto standard for enterprise security architectures.



MANAGING RISK IN COMPLEX SYSTEMS

Real-time risk management & Enterprise security architecture

Abstract to Risk Management

Modern cyber threats have completely overrun traditional approaches risk management and enterprise security architectures. The evidence clearly shows that the billions Canada spends on IT security is having no measurable effect on the quantity of malicious traffic entering and leaving private and public sector entities. The US has formally abandoned paper certification and accreditation schemes for risk management and security architecture in favour of a real-time integrated risk management system. This is the only way we can managing Risk in 2010 against Advanced Persistent Threats (APT). In the future, networks must adapt to risk automatically because humans are simply too slow.

Relying on policies and standards and traditional threat-risk assessments to forecast and stop an attack is much like consulting the farmers almanac or looking inside your house to predict severe weather events.

Background to risk management

The traditional threat-risk assessment process of today is based around security audits of vintage World War II communications centres. Envision a teletype machine encased in a metal shield room reinforced with concrete walls. The signal from this teletype machine went directly to a link encryption device in an adjoining room. Classified messages from the teletype were printed off, registered and stored locally. There was a network air gap and strict physical document control. A single fibre/copper cable ran out of the building and carried the encrypted signal to a communications node buried a half-mile underground, using leased lines. This was much simpler system than today. There was only one egress point from the organization, a small number of communications nodes, complete logical, physical, and tempest (emanations) isolation and no software. There was a limited number of ways and means to compromise this architecture, all of which were well known. Physically-centric security policies mapped neatly with the system. Therefore, policy compliance could provide a high-degree of assurance that all known risks had been mitigated. This is no longer the case.

Most risk assessments today remain simply compliance audits. The majority cyber-threat assessments are speculatory. They have both become highly-commoditized products with an average market value of $10k, and have a target of evaluation of a single server or application. Few, if any, address real threats or risks in an integrated fashion. Thus, the average threat-risk assessment of today has devolved into a pseudo-science with the accuracy of astrological predictions. We are caught in a race to the bottom, and it is time to pull out of the tail spin.

The following points summarize the criticism of many threat-risk assessments today:

- There is typically no data (threat, vulnerability, work-factors, or likelihood) and the risk calculations are flawed;
- Statements of 'fact' often lack references or the premises are not validated. Sources tend to be circular or questionable. The pop media is too frequently used as a legitimate source. Reports based upon opinion (qualitative) surveys are portrayed as quantitative when the reliability of the source and veracity of information is indeterminate;
- There is no *evidence* in the strictest sense in that the arguments and evidence would not stand up in court or withstand academic scrutiny;
- Premises are based upon irrational belief systems, intuition and contain perceptive ambiguities;
- Analysis suffers from cognitive dissidence;
- Contain common fallacies of Slothful induction, wilful blindness, false generalization, affirming the conclusion and irrational disbelief, etc.
- Recommendations are reactive in nature;
- Fails to use Integrated Risk Management framework;
- Equates compliance audit (Public Policy) with threat-risk and assurance;
- Security policy and standards trail technology and the threat by decades;
- TRAs are sensitive to commoditization;
- Regarded as Pseudo 'junk' science;
- Quazi-quantitative data is based in anecdote, hearsay, irrational believe systems and opinion that is known to be highly inaccurate in resolving complex issues;
- There exists a large perceptual gap. Analysts generally do not have access to real threat data. They don't know what they don't know, and don't measure uncertainty;
- Likelihood, and work factor calculations are mathematically wrong;
- Value assessments are not normalized;
- Assumptions and initial premises are not validated but are presented as 'truths';
- Open complex systems are reduced to closed simple systems;
- Uses vague ambiguous un-actionable language "unlikely, high, medium, low, may, could."

It is also standard practice that threat reports that have Nothing to Report (NTR) then assess the situation as low-risk. Ironically, lack of threat intelligence means high-risk owing to uncertainty.

So what are the topics that should be part of the discussion on the effective approaches to the operational security? Consider the following is a list of pragmatics for accurate real-time integrated risk management, similar to what was used for the 2010 Olympics:

- Risk analysis must strictly adhere to formal Scientific Method including the process of hypo-deductive reasoning, critical and alternative analysis;
- Facilitate evidence-based decision making;
- Establish Key Performance Indicators (KPI) that regulate accuracy in the assessment and influence behaviour;
- Establish a feedback loop for architecture design and adaptive/dynamic defence in real time;
- Render a Return on Investment (ROI) [value of security dollar spent] figure as well as total Cost of Ownership (TCO) for security infostructures;
- Assessments must be real-time and continuous;
- Conclusions should be proactive;
- Show work factor, likelihood, uncertainty and entropy calculations;
- Integrate Threat, Business and operational risks;
- Normalises value and impact to real-world currency $;
- Use correct mathematics particularly statistical validity(T-Tests);
- Complex (Universal) Systems Theory is used to model security ecosystem;
- Theoretical analysis is validated by experimental results;
- Use of primary sources throughout;
- Measurements are taken using upstream (inbound/outbound analysis for critical interdependencies, risk conductors, malicious activity, risk contagion calculations and toxicity of assets);
- Correlation of multi-source threat metrics with perimeter deep pack inspection DPI;
- Vulnerability Assessment and Penetration testing (full spectrum); and
- Risk needs to be normalized to $

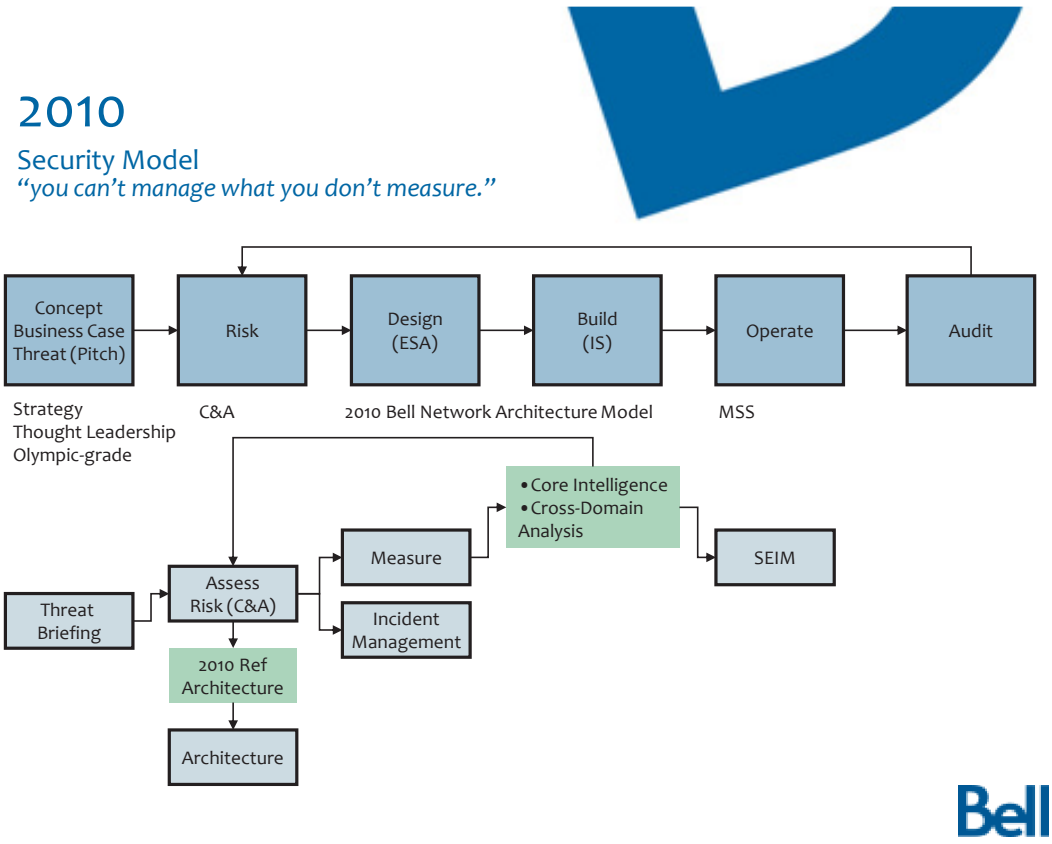
The National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) and the National Aeronautics and Space Administration (NASA) have abandoned the traditional paper-based risk process under the Federal Information Security Management Act (FISMA) as of May 2010, favouring real-time risk processes.

This year, NASA officials won't have to go through a traditional paper-based process for recertifying existing systems as compliant with security requirements, according to a notice from the agency's information technology office. The edict is a significant break with the way agencies typically have measured their systems' security and, if other agencies follow NASA's lead, it could have government wide implications. Agencies are required to get their systems certified and accredited under the Federal Information Security Management Act. However, critics say the paper-based reports that agencies have typically completed to meet those requirements amount to costly, time-consuming, snap-shots of security. Last month the Obama administration announced new standards for agency reporting under

FISMA as part of an effort to get agencies to shift from paper-based reports to real-time monitoring of systems. Citing those new instructions, NASA's Deputy Chief Information Officer for IT Security Jerry Davis sent a memo May 18 that said the agency will not generally require leaders to recertify existing systems with the paper-based process. – Ben Bain, FCW, May 24, 2010

http://fcw.com/articles/2010/05/24/web-nasa-fisma-memo.aspx

A System of Real-Time Risk Management



Establishing a Common Operating Picture

A risk methodology should start with a strategic common operating picture. Global sources and Upstream (cloud) infrastructure providers can provide an organizational view of risk by measuring (logical and physical) connectivity. This would include inbound/outbound net-flow of legitimate communications and malicious traffic. The organization is scrutinized as a block box based on monitoring communications to/from blocks Internet address space and identified physical premises. From this data set, it is possible to:

- determine organizational assurance levels and profiles when compared with statistical norms;
- detect illicit communications channels;
- critical interdependencies and risk contagion;
- zero-in on infiltration and exfiltration paths;
- identify threat agents, attack vectors and infected machines (to a limited degree);
- calculate network performance and degradation;
- assess preliminary loss-impact / revenue at risk; and
- initialize immediate proactive mitigation. Sink-hole attacks and block out-bound exfiltration.

The next step is to place sensor(s) within the enterprise zone and enable security aware ICT components, and correlate global threat intelligence with metrics. This is how you can discover advanced persistent threats (APT) that have beached your firewalls and identify infected machines. Sophisticated sensoring can provide valuable forensics that you will need for the Threat Risk Assessment (TRA).

Any good TRA will generate an incident and investigation. Be prepared to send initial findings to the forensic and incident handling team for immediate remediation.

There are a number of concurrent activities, which can be undertaken while you are gathering threat metrics:

- conduct the full-spectrum of vulnerability and penetration testing of your organizational infostructure;
- Asset inventory, configuration management picture, value assessments of both infrastructure and *info*structure, goods and services, and business operations;
- Draw network infra/infostructure diagrams;
- Determine risk tolerance levels in real currency $;
- Conduct compliance audit of existing security controls and calculate compliance risk (normalize to real currency $);
- Establish assurance targets (lowest standard, common practice, best ROI, best effort); and
- Gather accurate threat intelligence that includes work-factors for attack vectors, black market values, and the means, motives and capabilities of primary threat-agents.

Compare your operational 'network' to a *reference security architecture* that matches your assurance target. Note Δ or deviations.

The risk assessment should be an iterative process. As the threat, vulnerability, network (infra/info structure) configuration and asset-value data accumulates, more statistically value exposure-likelihood mathematical probabilities can be calculated.

Tuning the adaptive-network cycle and real-time risk management

But don't wait for the whole answer before starting to act. You don't have to know it all, to know what to do next. Some exposures, as they materialize, will precipitate immediate remediation. Start by invoking architectural changes that make the most sense in addressing the real measurable threat, particularly with tradecraft or mechanisms, which have shown to have very good ROI (like upstream DDoS protection, SPAM filters and broad policy enforcement, trusted network connectivity and consolidation).

Here we see the importance of a feedback loop between real time risk assessment and security engineering. Measure the effects of malicious traffic/attacks as infrastructure changes are made to a live network. A safeguard or architectural modification, which successfully (and affordably) reduces measurable exposures, is worth keeping. Ideas that do not change (or worsen) malicious traffic loads do not have merit and should be abandoned before you throw good money after bad. In this way, risk analysis is a continuous process that can tune adaptive network defence, and operational security of the organization in a proactive manner. In the very near future ICT components will become security aware, both producing security logs and ingesting global threat intelligence. All network components will be virtualized and pushed into the cloud. Integrated Risk Management can be fully automated and will be able to re-architect the network in real time in response to threat pressure or proactively with good intelligence I&W. Networks will become highly agile and to a degree sentient.

Cyber security is all about manoeuvre warfare, not a thin red line tactic of a historic battlefield.

A System of People, Processes and Technology

Risk assessment and enterprise security architecture are not activities that you do just once at the beginning of a project – they are a continuous process. Nor is a TRA a necessary evil for certification, which an organization goes through in a perfunctionary manner. Incident triage and response is not an episodic group-lead activity. A TRA should save you money and enable business operations. Incident and risk management become synonymous in a real-time system involving people, processes and technology. The objective is to transform an ad hoc manual episodic practice to a continuous process with more accurate results at less cost.

Although there is a lot of technology, people need to be engaged. Too often TRAs and ESAs are performed independently of operational security staffs, corporate security and the Information Protection Centre (IPC) or the Security Operation Centre (SOC). The technology that you put in place to facilitate the initial risk assessment, should be integrated into the SOC, so that it can be easily upgraded to build a legacy capability. Upstream security and core intelligence feeds that are used for the assessment can be continued as subscription services for the SOC. A small Security Event Information Management (SEIM) system is helpful to process the data from deep packet inspection (DPI) devices and correlate findings with upstream/global operating pictures. Red and blue team work can be integrated with threat detection, and proactive defence measures. Remediation efforts such as network design changes, incident response, patch management can be coordinated from corporate security operations based upon the findings of threat and vulnerability sources.

Unfortunately, most TRA work is an expendable commodity. It is a snap shot in time that is obsolete upon publication. Once folks have a ten-thousand dollar compliance checkmark, the assessment goes on the shelf or into the trash. Ideally, you want each TRA to build on subsequent work by building a system.

Traditional Risk Assessments are also so myopically focused they tend to "lose sight of the forest for the trees," in that they don't consider the enterprise as a whole. These background processes also can become technically esoteric. Thus, they are of little use to executive decision makers.

The continuous threat-risk assessment needs to be placed into context of an Integrated Risk Management Framework (IRMF)[90] so that security can be balanced with the cost of doing business and operational imperatives. This picture can be presented on a 'single pane of glass' or executive dashboard.

Network security data can be merged and collated with: network performance metrics, financials, project reporting funnel, time sheets, physical access logs, Internet activity monitoring, voice analytics (telephone calls), World markets, news feeds, intelligence, HR, shipping/receiving, inventory, RFID tagging of assets, configuration management, geolocation information, fleet management, spectral monitoring, etc., to provide the most accurate real-time view of all risks at all time across the whole organization.

[90] See Integrated Risk Management Framework (IRMF) published by the Treasury Board of Canada as official public policy.

A dashboard comes with the ability to drill down as detailed as required or validate the business against the Program Activity Architecture (PAA). Operations security (OPSEC) is a process that identifies critical information can be exploited by hostile forces, and then implements counter-measures to mitigate adversary prosecution of critical infostructures.

Real time risk management systems can also be used in parallel to build high-fidelity models and predictive schemes for managing risk proactively.

These systems exist right now for your enterprise. Alternatively, the whole process can be operated from the cloud as a managed security service with not capital investment. Real time risk management systems are achievable at a fraction of the cost of traditional means of risk assessment and have been shown to be orders-of-magnitude more effective at reducing risk.

Case Study 2010 Olympics

The 2010 Olympics provided a unique opportunity to compare and contrast both traditional and real-time-*enhanced* threat-risk management methodologies.

There were two approaches to security at the 2010 Olympics. One was based upon a traditional harmonized TRA methodology, whilst the other used a continuous real-time integrated risk management framework. The conclusions of each assessment where vastly different as was the disposition of safeguards. The traditional approach failed to predict and defend against the majority of real threats whereas the real-time integrated system was measurably accurate. The infrastructure was maintained 100% operational throughout the Games.

Detailed critical analysis of 2010 threat risk assessments and security was provided in a briefing note - *Risk Management for the 2010 Olympics – A comparative critical analysis of approaches, Bell Canada.*

Conclusion to risk management

Traditional threat-risk assessment methodologies and common enterprise security architecture models are anachronistic throwbacks to an age of simple 'closed' systems that could be managed with policy compliance. The evidence shows that the way most public and private sector entities manage risk is largely ineffective and expensive. Formal scientific method and real-time adaptive open architectures are the only answers in the modern information age of manoeuvre warfare, where the critical interdependencies of vastly complex systems are exploited by sophisticated threats and non-deterministic emergent effects.

HIGH PERFORMANCE SECURE NETWORKING FOUNDATIONAL CONCEPTS

The traditional means of building 'secure' networks has reached its theoretical limit of effectiveness. Quantitatively, the Public and Private sector spends billions in IT security every year, yet there is no measurable change to the level of malicious traffic entering and leaving these organizations. In fact, it is getting worse.

The Internet is a large complex non-deterministic ecosystem, where all systems are inherently open this reality. Thus, securing your network in this environment requires a degree of sophistication in architectural design and risk science not found in policies, standards or common practice. Fortunately, there are some foundational concepts for high performance secure networking that will save your organization money and provide significantly better assurance.

Internet protocol acts like a commons, application development a market and the transit layer operates like guild.

The matrix balancing itself out

Universal systems theory is one means of modelling cyberspace. It rather extraordinary mathematics, but consider one part of the equation as it balances itself out.

Consider that the carrier backbone operates as 99.999996% availability. Over $174 Billion dollars transits this network every day. A fraction of degradation in throughput costs millions and network performance is measured to pico-seconds. In fact, the computers financial markets make trading decisions based upon the instrumentation of host networks. Thus the majority of security decisions are driven on availability requirements.

Network performance is linked to financial reporting systems, which in turn feed HR and salary bonuses, in near-real time. Degradation in network performance immediately incents behaviour to fix the problem. The ROI is evident in the accounting.

In a carrier environment security controls are put in place to increase resiliency and availability. There is a fast feedback loop for ensuring security investment for the sake of availability. However, there are few market incentives to provide six-nines of confidentiality and integrity. There just isn't the demand.

Now what happens when the need for iphone and HDTV over the network forces investment in larger pipes and total carrier bandwidth jumps orders of magnitude? The bandwidth associated with malicious traffic will become insignificant, and the influence (feedback) that cyber threat has on security investment will diminish. There most likely will be a re-lapse in security investment… until rich media content (HDTV) is widely delivered to mobile devices 4G IPV6 IPhones.

Mobility networks are significantly more sensitive to bandwidth disruptions. The emergence of 4G IPV6 botnets and the need to still deliver HDTV to mobile phones from the Cloud without dropped frames will rejuvenate security investment in the core.

At a certain point it will not be practical to achieve six nines availability by just increasing the size of the pipes (especially on mobility networks). Enhanced Confidentiality and Integrity controls will be needed to get the Availability numbers. Then consider that the mobile phone is fast becoming the device for point-of-sale. In this case the carrier holds the credentialing (authentication, identification, authorization) further necessitating the safeguarding of security properties other then just availability. In order for telecommunications carriers to broker financial end-point transactions with clients also entails closer interaction with the financial sector.

The cyber metrics from carrier networks and financial networks are kept separate. This has exacerbated linking criminal cyber and money networks. Integration of these systems in the future will permit the data-fusion of banking and telecoms security and fraud metrics. The correlation of financial and Internet threat network intelligence in real-time is a significant nexus in the winning the fight against cyber crime, provided data matching and privacy controls can be put in place.

In this example, one can see how the security of cyber space might fluctuate as a harmonic through a complex system. Of course, a butterfly could flap its wings in Asia and upset the balance in the equation in Canada.

Taking Secure Networking - Beyond ISO27K

A high-performance secure network starts with common architectural frameworks and standards as a foundation.

"The ISO27K (ISO/IEC 27000-series) standards provide good practice guidance on designing, implementing and auditing Information Security Management Systems to protect the confidentiality, integrity and availability of the information on which we all depend." - www.iso27001security.com

Traditional architectural security design for Information Communication Technology (ICT) calls upon Enterprise security architecture (ESA). ESA in turn, applies rigor and method around organizational security; information security technology business security architecture, performance management and security process architectures. An enterprise's information security architecture (EISA) allows traceability from the business strategy down to the underlying technology.

Common enterprise information security architecture frameworks include:

- The U.S. Department of Defence (DoD) Architecture Framework (DoDAF)
- Extended Enterprise Architecture Framework (E2AF) from the Institute For Enterprise Architecture Developments.
- Federal Enterprise Architecture of the United States Government (FEA)
- Capgemini's Integrated Architecture Framework
- The UK Ministry of Defence (MOD) Architecture Framework (MODAF)
- NIH Enterprise Architecture Framework
- Open Security Architecture
- Information Assurance Enterprise Architectural Framework (IAEAF)
- SABSA framework and methodology
- Service-Oriented Modeling Framework (SOMF)
- The Open Group Architecture Framework (TOGAF)
- Zachman Framework

The International Information Systems Security Certification Consortium, Inc., $(ISC)^2$ for Certified Information Systems Security Professional (CISSP) establishes a Common Body of Knowledge (CBK) that is based upon core information security and assurance tenets: confidentiality, integrity and availability across a number of domains:

- Access Control
- Categories and Controls
- Control Threats and countermeasures
- Application Development Security
- Software Based Controls
- Software Development Lifecycle and Principles
- Business Continuity and Disaster Recovery Planning
- Response and Recovery Plans

- Restoration Activities
- Cryptography
- Basic Concepts and Algorithms
- Signatures and Certification
- Cryptanalysis
- Information Security Governance and Risk Management
- Policies, Standards, Guidelines and Procedures
- Risk Management Tools and Practices
- Planning and Organization
- Legal, Regulations, Investigations and Compliance
- Major Legal Systems
- Common and Civil Law
- Regulations, Laws and Information Security
- Operations Security
- Media, Backups and Change Control Management
- Controls Categories
- Physical (Environmental) Security
- Layered Physical Defence and Entry Points
- Site Location Principles
- Security Architecture and Design
- Principles and Benefits
- Trusted Systems and Computing Base
- System and Enterprise Architecture
- Telecommunications and Network Security
- Network Security Concepts and Risks

- Business Goals and Network Security

The limitations of traditional practice

It is important to appreciate that international standards, public policy and 'common' body of knowledge for security professionals represent a necessary but minimum criterion. Where organizational behaviour is driven by policy compliance and certification there is a regression to the mean. Threat behaviour is motivated by real profit and tempered by risk.

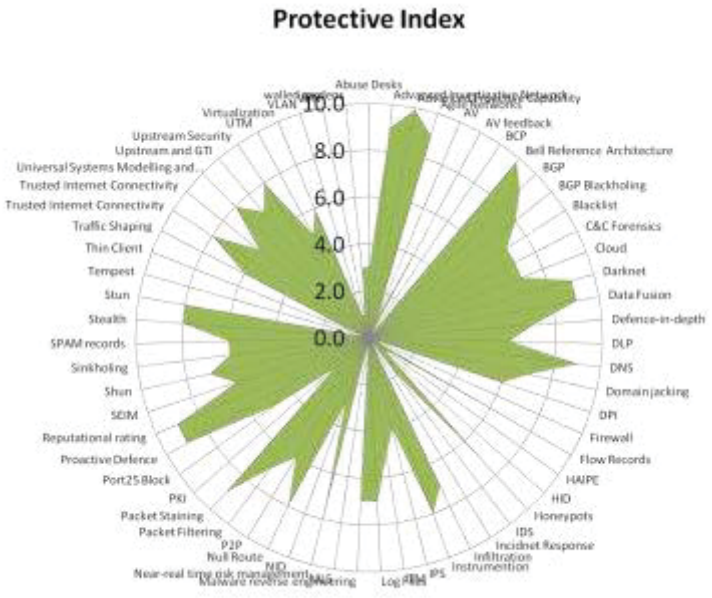
Even, superior Japanese building code and disaster planning could not withstand a 9.0-magnitude mega-thrust earthquake and subsequent 10 metre high Tsunami.

Similarly most corporate networks build to international and professional standards using common architectural frameworks have not survived modern advanced persistent threats (APT), transnational crime or sophisticated state-sponsored campaigns or e-spionage and cyberwar.

Security technologies most of us rely on every day—from anti- virus software to firewalls and intrusion detection devices—are reactive. That is, they are effective usually only after a new threat has been identified and classified. [Takedowns: The Shuns and Stuns That Take the Fight to the Enemy, By Brian Krebs]

An empirical measurement of malicious traffic across critical infrastructures and business sectors in Canada through 2009-2011 was correlated ICT security market data over the same period. A T-test compared malicious traffic with the procurement of security products and services. Analysis would appear to indicate that common Enterprise Information Security Architecture (EISA) and designing to ISO27K is only 20% effective at detecting APTs and has negligible effect at stopping sophisticated cyber attacks.

The graph depicts the relative protective index of traditional and advanced techniques when we measured their effectiveness at countering APT.



Once perimeter compromised, critical systems are being exploited, often for extended periods of time. Malware has evolved over the years into sophisticated code that incorporates error detection, stealth capabilities, as well as distributed command and control capabilities. [Arcsight]

Typical enterprise bandwidth is consumed with 30-50% malicious traffic, including 98% inbound and 50% outbound e-mail that is malevolent. Public and private sectors in Canada spend billions in ICT security each year with no statistically relevant reduction in malicious traffic. Thus, traditional security has reached its level of effectiveness, at about 50% when we apply all threats and measure performance through inbound-outbound threat analysis.

Information Security Has It All Wrong

The Gartner group, in their report *Information Security Has It All Wrong*, appears to have reached independently reached similar conclusions to Bell Canada. Gartner says that traditional information security architecture is not ready for the future we face. Traditional security models are strained: They are what got us here but won't take us forward. What we are looking at is a disruptive transformation of IT infrastructure. The Implications for information security are that:

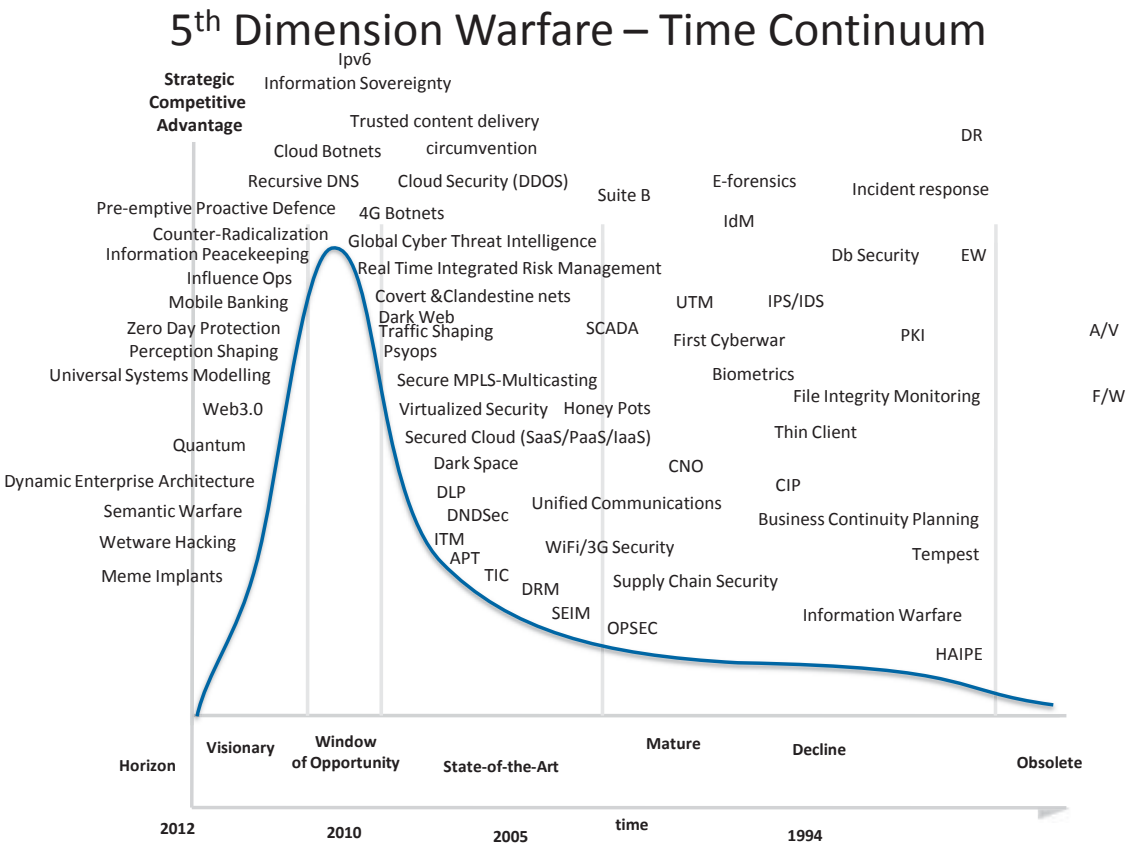
- All elements are potentially hostile
- Mainstays of antivirus and firewall increasingly ineffective
- Decrease in importance of the traditional "perimeter"

- "Inside out" protection as important as "outside in"
- More security policy enforcement points needed
- Security and trust are no longer binary and a need to accept relative "trustability"

Today's perimeter is an illusion, an artefact of the past. More perimeters and moving parts, many of which we don't control, are in our future. [Information Security Has It All Wrong – Gartner]

Someone following the Canadian food guide and a ParticipAction exercise program may meet minimal standards for healthy living but one can also realistically expect to be obliterated by Olympic competition. Analogously, the standard prescriptions for network health are no match for elite cyber criminals.

The following chart places security solution on a timeline from innovative to obsolete. You will notice that many of the commonly deployed solutions are outmoded.



The recipe for secure networking and trusted computing

In the course of this research, the Bell team studied the attributes of ultra-secure high-performance networking based upon quantitative Type 1 evidence and a near-real-time integrated risk management framework. These findings take enterprise information security architecture well beyond ISO27K.

What components, design decisions, architectural elements, methodologies, security science and advanced tradecraft provided the best ROI and were the most effective at addressing sophisticated attacks such as zero day exploits and APT? Certainly, signature based security technologies are not effective against day zero-day attacks.

It is cost-effective for enterprises to achieve a 98% secure solution (covering properties of confidentiality, integrity and availability) using standard products and services deployed as per a reference-architecture. The total cost of ownership (TCO) for 98% clean networks is excellent in that the cost of upgrading security from 50% to 98% is an order-of-magnitude less than the impact of lost bandwidth and availability which inhibit the delivery of goods and services, and limit cash flow, not to mention of loss of confidential information from a compromise. Spending more money on security stuff is not the answer; it is having the right stuff deployed in the right place at the right time.

Cleaning networks of the residual 2% of malicious traffic and improving availability to 'six-nines' is more expensive and requires sophistication in the design, operations and resourcing. Not all organizations have the requisite capabilities to operationalize this level of secure high performance networking. This is when outsourcing is a viable option.

No network can be totally secure. Any organization that says they are not penetrated by cyber threats isn't looking hard enough.

Secure network concepts

In the most trivial implementation of a 'secure' network, you can put a few tempest computers in a locked room and connect them together. So long as there is no connection to the outside world, your solution will adhere to most security policies including those governing highly-classified networks. But isolated networks are not much use except for single purpose processing. The most common 'secure' network' architecture uses High Assurance Internet Protocol Encryptors (HAIPE) to encrypt all traffic leaving a secure physical building perimeter. The network inside the building walls typically uses commercial out-of-the-box with no more intrinsic security than simple password authentication for identification and access control. Authorization is implicit within the confines of the network. Physical zoning, written corporate security policies and Type 1 high-grade link encryptors form primary means of defence. Both architectures are often, and erroneously, dubbed 'closed systems' and risk is mitigated by 'simple' system models.

But here is the problem. Networks are neither 'closed' nor 'simple' systems. In fact, all networks are open, and in one way or another, connected to the Internet on several layers. All networks are connected to the Internet on some level. People still think that their corporate information is confined to their building or control – it is not. External analysis of the corporate info-sphere is rapidly becoming a far more effective tool of intelligence than traditional means of bugging the corporate conference room. Systems are necessarily complex but still dealt with parsimoniously and in a physical manner. (ie., the wrong answer is a bigger firewall). Secure networking policies are based upon communications centre architectures conceived in the Second World War, and are becoming less effective given the manner in which cyberspace has pervaded our lives in 2011. Social networking, consumerization of the workplace, globalization of supply chains and convergence are just a few of the macro-emergent-effects transforming your organization. Written corporate security policies, like a no-wireless policy, are meant for the honest folks but are treated with contempt by deliberate threat actors. In point of fact, restrictive policies can accelerate attacks to the very things that they intended to avoid. An organization with a no-wireless policy will have very little experience managing wireless, engaging the threat in this spectrum and may not even be monitoring compliance. Policies of this sort are taken into consideration in developing a target package that offensive operations will turn to their advantage.

So how does one go about building a 'secure network?' First we must tackle the equivocation with the lexicon 'network' and 'secure'. What is a network and how secure do you want it to be? Before you spend money securing something, it is always wise to agree on what that 'something' is, and identify critical dependencies - like building a luxury home on a flood plain.

Network scope (breadth). Is the network just the hardware components of your LAN within your building? Or does it include the physical cable plant, firmware, software applications and the information? Is the design scope limited to local network infrastructure, or does it extend into dimensions of the info-structure, info-sphere, and knowledge-sphere? Are you securing corporate information only within the building perimeter or universally? How are you protecting intellectual property assets when they leave the building or ensuring the veracity and trustworthiness of information/signals entering the premises? Even now, are you securing all the layers of the OSI model, or ignoring some, given that the model is only as resilient as its weakest layer? Does your network security plan consider critical system interdependencies; comprised of people processes, technology and information at an organizational level? How does your secure network architecture integrate with the operational security plan of the organization such that it considers spheres of control, influence and interest?

Security scope (depth). How secure do you want to be? The degree of security that folks feel obliged is influenced by their perception of risk. Risk comes in many forms. The fastest ways to get yourself into the 'penalty box' is to: fail a compliance audit, be exposed for being less secure than your peers or have a very public breach. Meanwhile, insidious Advanced Persistent Threats (ATP) and

systematic compromise state-sponsored e-spionage[91] are rarely addressed so long as they don't show up in an audit or newspaper.

The two most common influences of system security requirements are:

- Passing compliance audits (adherence to policy) and avoiding the threat of punitive sanctions; and
- Mitigate of reputation embarrassment owing to comparative scorecards of public breaches. In other words, making sure that you are as secure as your peers, but no more or no less.

Both these objectives, taken in isolation, are flawed in that they do not address the real risks or costs to the organizations. They may even introduce additional risks and costs into the design. All of the major networks in Canada fallen to the enemy in 2011 cyber attacks were fully compliant.

Networks built exclusively to meet minimum policies, standards, and doctrine, do not meet best practices by definition. Security standards tend to lag both the threat and technology by decades. There is also a great deal that is not in books. Therefore, System Security Requirements (SSR) derived from standing policies and compliance audits, masquerading as threat–risk assessments, are largely ineffective in mitigating today's threats.

Designing to the common practices of your peers follows a regression to the mean. Perhaps the attacker may be left with an embarrassment of riches in that they have so many victims to choose. Although this defensive tactic is used by herds of animals on the savannah, this is rarely an effective strategy in cyberspace.

The path to an right answer starts by expanding your definition of network to include your information space, then secure it the level that yields the best Return On Investment (ROI) (security per dollar spent) or best effort. As a starting point, you should have an accurate inventory, configuration management and value assessment of your information assets, perform a quantitative measurement of your risk[92] and calculate Total Cost of Ownership (TCO) for your 'info-structure.'

At some point early in the process, you will need to determine your *tolerance for risk* (including uncertainly) and establish *target assurance levels*.

The certification and accreditation is a formal attestation of risk, whether you choose to mitigate, accept, transfer, ignore it. More often than not, C&A is a formality rather than a 'formal method' of risk science. There are many networks with a letter of certification, with no body supporting evidence – or it is specious at best.

[91] E-spionage whitepaper, Sec Dev and Bell Canada Jun 2010

[92] Risk is a function of exposure (threat x vulnerability x likelihood), impact (value x sensitivity) and uncertainty. Integrated risk combines business, operational and threat risks.

Secure Network design needs to talk in terms of Key Performance Indicators (KPI), work-factors, Return on Investment (ROI), Total Cost of Ownership (TCO) and revenue at risk, rather than compliance to policies, common practice and lowest standards. The decisions upon which security decisions are made must be evidence based, which means quantifiably measurable and scientific.

The ROI approach optimizes the cost of security expenditures within the context of the business risks. You wouldn't spend more money on car insurance than the value of the car, or the risk of damage, amortized over its lifetime. Similarly, if the extrinsic and intrinsic value of a document is $1000, it would not be cost-effective to spend more in security. The other thing that the ROI perspective brings is measuring how effective various safeguards actually are. Is diet or exercise more effective at losing weight, health or fitness? How much time and effort should be invested in each one? What is the best blend? Similarity, is a firewall more effective than deep-packet inspection or DNSsec or security awareness? Does it matter where I put my firewall? How much more effective is proactive defence compared with a reactive one? What are the Key Performance Indicators (KPI) for network security?

The selection and implementation of security safeguards based upon ROI can measured by the relative work-factor to the threat and the quality of malicious traffic it reduces. It is possible to validate ROI and effectiveness of security architecture components using models, quantitative analysis of network traffic and active security testing during design-build phases. Meanwhile initial draft architectures can benefit from the lessons learned from operational networks with exceptional ROI and TCO.

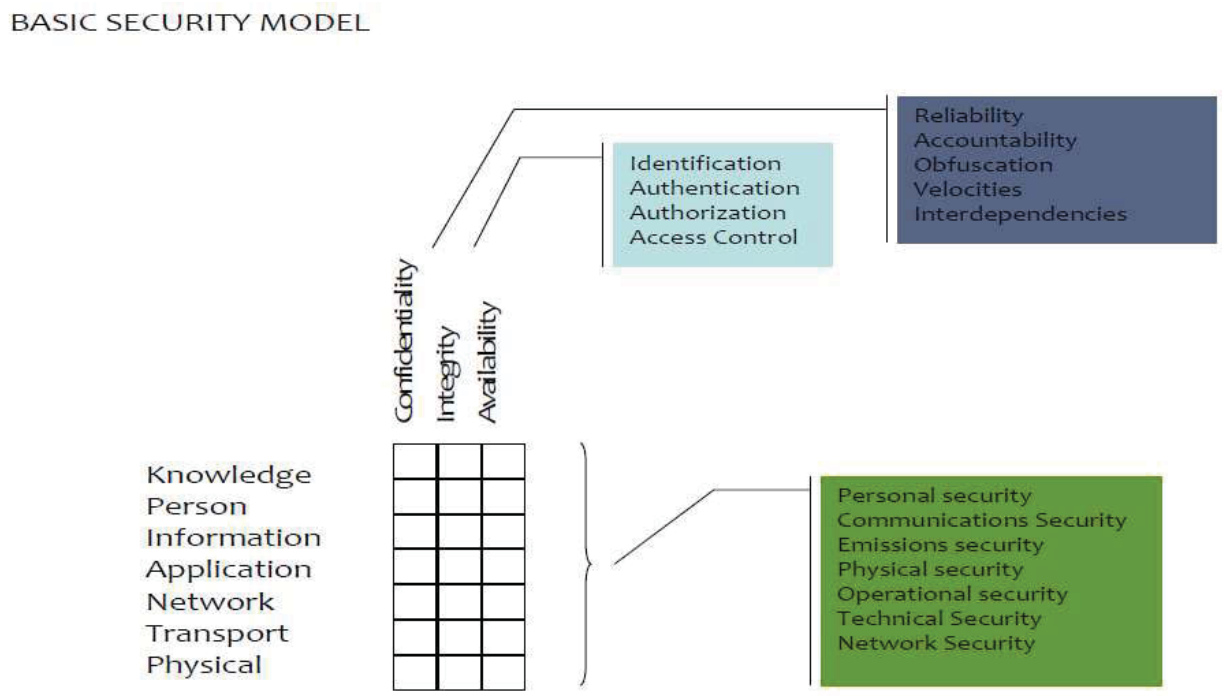
The Best-Effort approach is applicable to particularly paranoid organizations with healthy budgets, or ones operating in risky environments; one where security becomes a large cost of doing business. Essentially, you borrow the ROI concept in choosing safeguards that are most effective in reducing risks to the lowest practical levels or point-of-diminishing returns. Essentially, you build the most secure network possible. In many cases this is only practical for limited high security enclaves or Sensitive Compartmented Information Facilities (SCIF).

The best advice is to design to the right mix of Compliance, Peer, ROI and Best Effort approaches. Foremost, your network must pass C&A, and meet minimal standards, and you should be as secure as your peers. These two steps will keep the auditors off your back and you out of the penalty box, but may not keep you out of the papers or prevent infiltration. You must go further. No one is able to hide in 2011.

Convoluted designs do not solve complicated problems; instead they increase level of complexity, uncertainty and risk. Conversely, naive point-solutions like firewalls and policy won't help much.

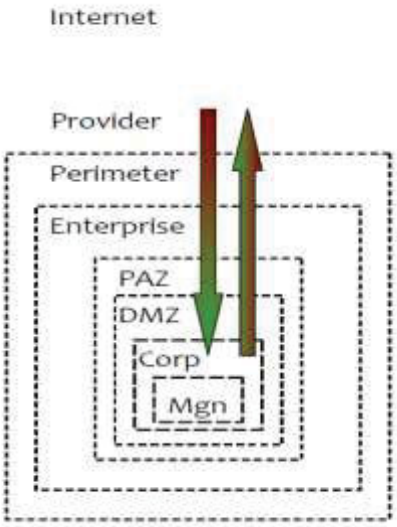
Enhanced Enterprise Security Architecture

In the most basic constructs, trusted security engineering must consider the security attributes and properties at every layer; from the physical to, synaptic, semantic and abstract.



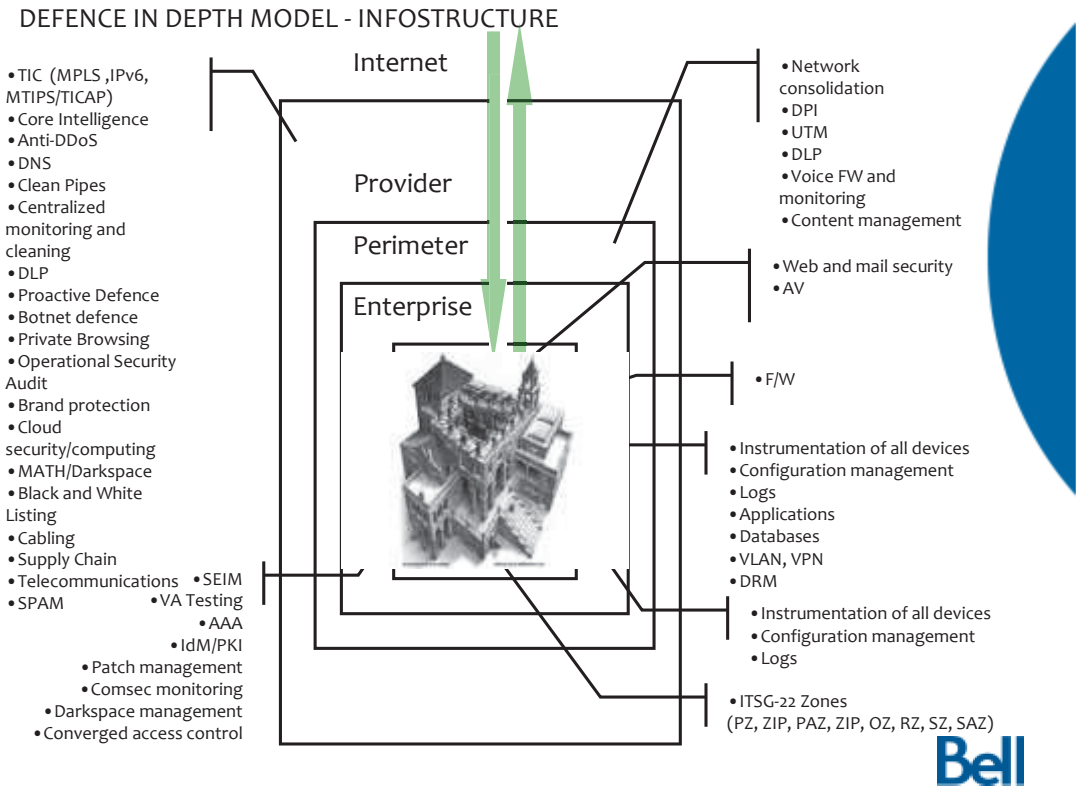
The traditional model of enterprise security architecture is based upon a simple (special) closed system model. External interdependencies are not considered and the cloud (upstream or external zone) does not exist. The public Internet closes in around the enterprise and malicious traffic permeates this zoning model in all directions. Quantitative analytics confirm this hypothesis through inbound-outbound monitoring of autonomous address spaces. The reasons for this failing in this model is that all systems are in fact open, there is no defined perimeter and traditional security mechanisms can neither detect nor prevent the majority of cyber attacks today.

CURRENT MODEL

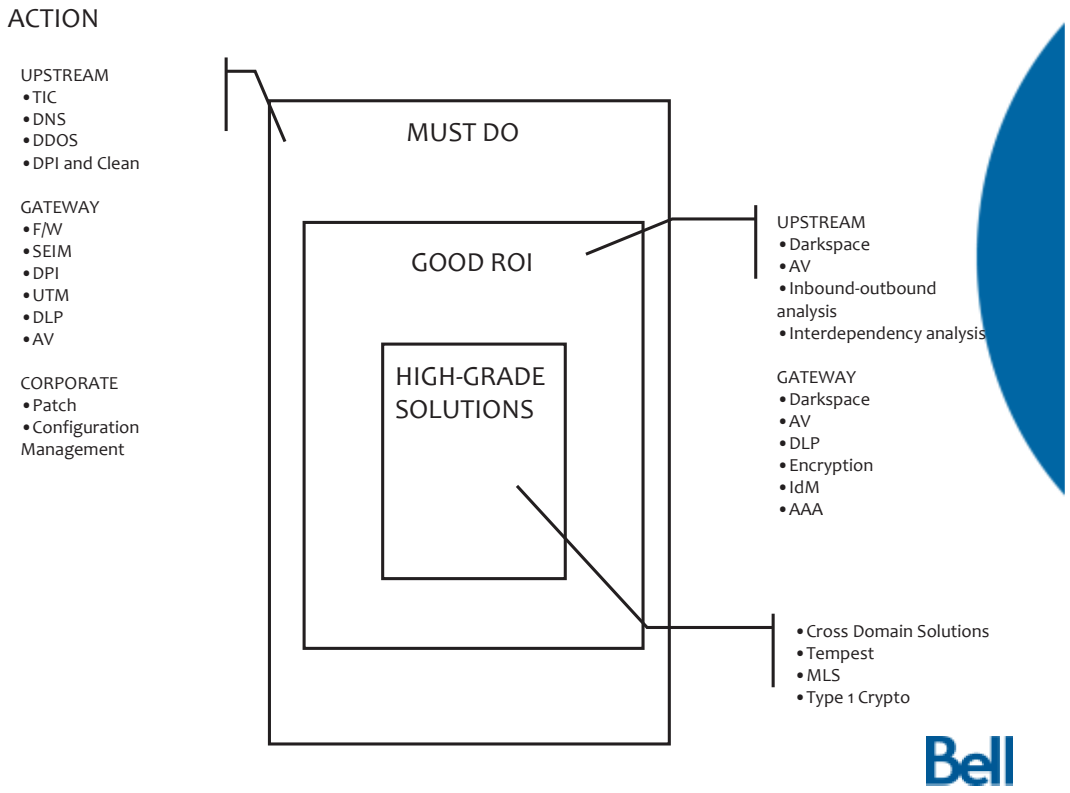


Now consider a new general[93] or enhanced model for enterprise security model that addresses open architectures and complex systems that exist with the cloud zone. We begin by managing control planes on the network like DNS and trusted routing upstream. By layering on upstream security services at all layers; from the cable plant to the knowledge-sphere the architecture is provided true defence-in-depth. Proactive defence operations that detect botnets using darkspace, and interdict and disrupt emerging threats like DDoS only become possible in the cloud. The organizations under this protection can achieve close to 99.999995% security when we measure percentage of malicious traffic.

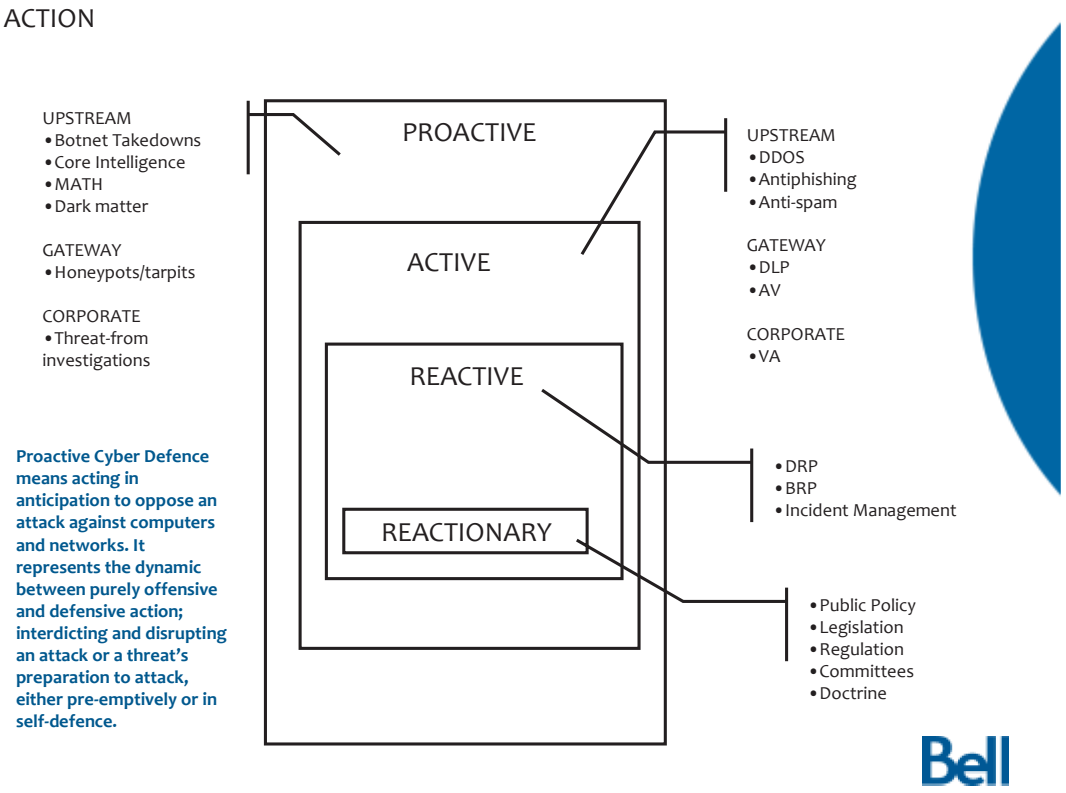
[93] Proactive Cyber Defence and the perfect storm, Bell Canada 2009



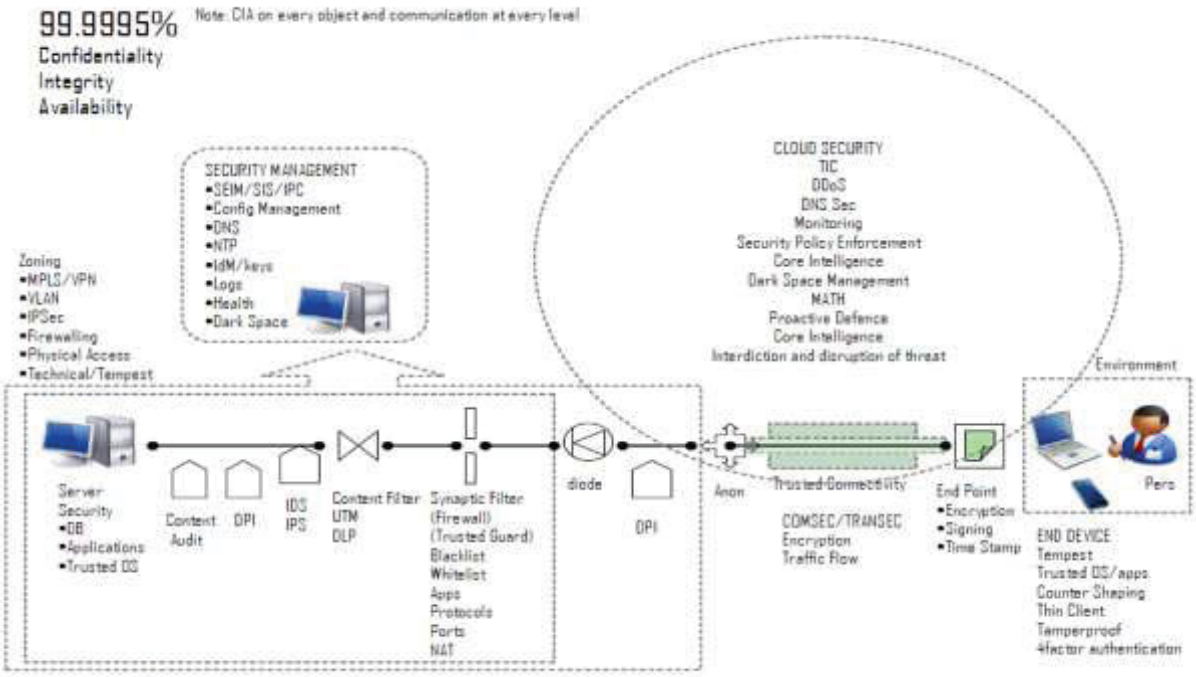
The manner that one migrates away from a traditional (special) or limited protection model to general (enhanced) security architecture can make the difference between success and failure. Traditionally, managers have deployed point solutions until they exhaust their security budgets. Expenditures happen with no regard to security ROI. The order in which you secure your organization is important. We propose that architects first do the things that will eliminate the greatest amount of malicious traffic. Let's call this the must do list. With the remaining budgets choose solutions that generally provide good security-value for dollar spent. Should you still have money to burn, or are sufficiently paranoid, then consider some high-grade safeguards. There is a law of diminishing returns that takes place where absolutely security becomes unaffordable and rapidly increases business risks. Currently, most organizations have there priorities backwards; spending an inordinate amount of funds on things like type 1 cryptography, multilevel security and tempest cell-phones, when their networks cannot withstand the most rudimentary DDoS attack or Botnet penetration.



A parallel model to consider is one of proactivity. The money you spend on preventing an attack is far more effective that recovering from an incident. Ironically, nearly all the public security initiatives to date focus on response, disaster recovery and prosecution rather than prediction and prevention.



The major difference to the models is to design a protection path from the cloud, to enterprise ingress/egress point and the end-user. Emphasis proactivity and implement according to security ROI at all layers.



Inter-network Security in the Cloud

The Internet Service Provider (ISP) cloud forms the first and most important security zone of any organization. On a national perspective; trusted internet connectivity, core intelligence, centralized monitoring & cleaning, DDoS protection, DNS security and supply chain/operational security form the foundation of a National Cyber Security Strategy as published by the US Comprehensive National Cyber security Initiative (C&CI).

Managed Trusted Internet Protocol Services (MTIPS), Trusted Internet Connection Access Providers (TICAP) and upstream security services provide Enterprise networks the effective defence-in-depth that they require to fight cyber threats.

Cyberspace is composed of a number of large peering "tier-1" carrier networks. These large carriers provide wholesale services to smaller "tier-2" networks such as Internet Service Providers or enterprise wide area networks. At the end are millions of users and devices. A large carrier like, Bell Canada for example maintains over 27 million connections and an IP space of around 50 million – about 46% of market share in Canada, 99% banking and 90% of government.

The aggregation of services and control planes to large national carriers as the centre of cyberspace brings unique capabilities for cyber defence.

Traditional network perimeter and host based defences have reached there theoretical limitations. Quantitative metrics at a national level have demonstrated that 80 per cent of zero-day and 99 percent of sub-zero day malicious exploits are undetected using traditional means of Anti-Virus, firewalls, unified threat management systems, or intrusion detection systems. Furthermore, the current mean volume of malicious traffic in public and private sector bandwidth is around 50% and a host infection rate of 5%-12%.

Most net-centric attacks are invisible because the malicious payload is imbedded in legitimate looking content over high-velocity services such as web or mail. Neither heuristic nor signature-based detection systems can keep up with the 80,000 new zero-day exploits every 24 hours. The end user has very little visibility into the scope of the attack and does not have enough data points to triangulate or identify the source.

Zero-day attacks are measurable at the network centre to within 99% accuracy. A major carrier can filter approximately 98% of the malicious traffic and attacks without unnecessary intrusiveness. To clean the pipe to 99.999995% confidentiality and integrity would require explicit permission of the clients for it would involve filtering based on content and invoking highly restrictive security policies. This level of assurance has been achieved on some corporate networks. Internet safety is ironically limited by a price sensitive market, net neutrality and privacy.

Fortunately, malicious activity can be identified at "upstream" confluence points in core or choke points where all traffic must pass. The full extent of the attack can be determined by identifying patterns in a much larger dataset. Once detected, sub-zero-day attacks can be managed through a variety of advanced techniques in the cloud at much greater efficiencies then traditional perimeter defences – and at a fraction of the cost.

High performance Secure Network architecture

Advanced Architectures need to address complexity with simple, yet elegant, solutions[94] that are based upon sound foundational concepts. The 2010 Olympics is a good example of a spectacularly complex security problem and a secure network solution that worked, but one that you won't find in books or standards.

These are the foundational concepts for secure network architecture that we have tested the effectiveness (protective index) through empirical measurement:

Defence-in-depth.

Your most exceptionally sensitive network operations (classified information processing for example) should take advantage of all the security safeguards afforded by a well-engineered enterprise network. The enterprise network should, in turn, be built on a trusted carrier infrastructure that stops the vast majority of malicious inbound/outbound traffic. Corporate security policies can be enforced in the cloud and performance should be measured through service level agreements (SLA). This design provides economies-of-scale for security as well as defence-in-depth. For example, if the Internet Service Provider (ISP) filters 99% of the traffic, the enterprise may not need the same size of spam filters etc., and can reallocate security budgets to provide more effective overall assurance. A defence-in-depth architecture consisting of concentric security zones, slows the attackers advance and escape, and facilitates early detection. The majority of rudimentary attacks would be culled, leaving a manageable number of incidents to manage by security staff. To present a practical example breaking through a MPLS and trusted routing infrastructure to get at a corporate network is a hard problem. Add a regular VPN and *upstream security* to the architecture and very little malicious traffic is going to even reach the perimeter of the corporate network. Don't bring the enemy to your doorstep

"You want to engage the enemy at a distance and in time."

Too often, classified enclaves are hung out on the Internet, and bare the full brunt of attacks without warning.

Given an infinite amount of monkeys typing on computers for infinite amount of time, any networks can be compromised. One sophisticated threat agent can achieve the same result in considerably less time.

"The only defence against surprise, is not to get surprised."- Bruce Lee

[94] Scientific proof found in 'complex systems theory.'

The alternate dimension to defence-in-depth is that *sophistication*. Your organization's tools, techniques and tradecraft have to be good enough to detect and defend Advanced Persistent Threats (APT). Traditional enterprise security architectures that are based upon public policies or common standards, and built with plug-and-play security appliances, have reached their practical efficacy. These traditional solutions are not effective at detecting APT, let alone, eradicating them.

"Building a secure network in the traditional way is like bringing a knife to a gun fight."

Defence-in-Breadth – 360° Security

There is no reason to have steel doors if you live in a glass house. Analogously, using expensive Type 1 high grade (HAIPE) link encryptors or VPNs as your primary means of defence, just accelerates the threat towards more vulnerable areas. Why would someone waste their time breaking code when there is unguarded access elsewhere in your network (WiFi, USB, Cellphones, illicit backchannels, e-mail, and web) and vulnerable PCs that can be turned into zombies? No DNSsec, IDM, DLP or DRM? This is the biggest criticism of high-end networks today, and subject of another white paper called "Laying Seige to Fortress Architectures." A network should be uniformly (homogeneously) defended from deliberate threat agents. Remember, ***your network is only as secure as the weakest link, not your strongest safeguards.*** A broad defensive perimeter slows the threat agent's decision-cycle, plugs fast-compromise points in the network and gives higher overall ROI for security dollar spend. One practical example is: rather than relying on a Type 1 appliance to provide confidentiality to data leaving your premise and some intrinsically weak authentication, why not use encryption ubiquitously throughout your organization on all communications and data storage or employ security packet staining. Information should never be stored or transmitted in the clear. The document itself should be encrypted and signed thus providing confidentiality, integrity, non-repudiation, authentication, identification. Users should be identified authenticated and authorized to applications, processes and data using strong cryptography, two, three or four factor authentication mechanisms. SSL, VLANs, IPv6, GetVPN routing and other mechanisms can also be used on the corporate network to make it difficult for deliberate threat agents. Fortified pill boxes will just be circumvented by a fast moving attacker and manoeuvre warfare.

"Steel doors don't help if you live in a glass house."

Full-spectrum defences.

"To a hammer, every problem looks like a nail."

Too often security is applied one-dimensionally. Defence-in-depth and defence-in-breadth concepts are good in only as so far that security properties are applied in all dimensions, at all layers, to all threats and vulnerability classes. All it takes is one gap, for an attacker to slip through your defences. Just as biological viruses can go airborne and mutate, information and toxic content can be engineered to jump air gaps in network design. Only a multidimensional or full-spectrum approach can provide the necessary threat attrition and detection. Attacks against your infostructures are not limited to external TCP/IP hacking. They can also include HUMINT assisted technical operations, flooding, shaping, fortuitous emissions, social engineering, 4G handset botnets, dumpster diving, EMP disruptive weapons and various other progressive indirect attacks. The attacker will often follow the path of least resistance and risk. They will not play fair.

So what are all the permutations and combinations of network components, layers, security properties, threat and vulnerability classes, which need consideration in every threat-risk assessment and enterprise security architecture? How do you protect against toxic content, viruses of the mind, memes and social engineering?

Common Operating Picture –Integrated Coordinated Defence

Defensive zones, mechanisms and processes must be integrated and coordinated to provide interlocking situational awareness and a common operating picture (COP). The whole security apparatus in your organization should know when any part of the *info*structure is under attack. It is no good when an advance guard comes in contact with the enemy and does not report it to HQ. Similarity, the forward edge of the battle space (front line) would appreciate being informed when the enemy parachuted in behind the lines. In a network scenario, intelligence from upstream darkspace monitoring can be used to reprogram deep-packet inspection (DPI) sensors within the enterprise zone to detect zero-day activity. Traditional security sensors are made aware of the persistent threat, signatures and blacklists can be generated black, and then URL filters, routers, IPS and F/W and stop the malicious traffic or exfiltration of sensitive materials dead it its tracks. Similarly, malicious activity detection, core intelligence and mitigation efforts in the cloud need to be fed to enterprise to provide warnings and indicators. Security safeguards across all zones can act in a coordinated fashion to disrupt the threat.

"Upstream intelligence gives your organization time and precision."

Dynamic Defence - Temporal considerations and controls

We must appreciate dynamic nature of threat-ecosystem when applying security properties to: network components and layers against all possible exposures (threat-vulnerability classes). Safeguards must provide historical context, be real-time, forward looking and dynamic. Are your security mechanisms tightly coupled with an Observe, Orient, Decide,

and Act (OODA) loop so that you can respond to a cyber-threat striking your organization at the speed of light? In real terms, this may mean restricting general security policies, focusing detection and mitigation on specific attack vectors (domains, IPs, circuits etc) or quarantining the infected.

"Static defence will quickly fall to the enemy practicing manoeuvre warfare."

Proactive defence strategy.

Reactionary strategies that rely on static defence, incident response and disaster recovery offer the enterprise few choices and all of them expensive. Network defences must be adaptive, predictive, proactive and pre-emptive.

"An ounce of prevention is worth a pound of cure."

Proactive Cyber Defence means acting in anticipation to oppose an attack against computers and networks. It represents the dynamic between purely offensive and defensive action; interdicting and disrupting an attack or a threat's preparation to attack, either pre-emptively or in self-defence. Proactive cyber defence will most often require operationalizing upstream security mechanisms of the telecommunications/Internet providers.

A proactive defence strategy is one of the most effective means of countering systemic-victimization and keeping the predatorial response in check. If you act like a victim, by never fighting back, then you will by played like a victim. It is said that weakness invites attack. We see this every day in both natural and cyber ecosystems. The lion will gradually and systematically test the herd's defences first, before attacking head on. Similarity, China, Russia and other threats constantly launch attacks against Canada and measure our response. The lack of counter-attack has given room for hostile nation states to manoeuvre, and has encouraged more bodacious operations like hijacking 15% of the World's Internet traffic, turning off a power grid, launching all out cyber wars (Estonia, Georgia) without retribution, mounting DDoS attacks against official government networks, and e-spionage operations against Canadian and US companies.

By closing with, and engaging the threat at a distance; at a time and space of your choosing, you can interdict and disrupt their attack networks and prevent attacks from ever reaching your outermost perimeter. Otherwise, left unchecked, attacks will gain in momentum, scale and impact the closer they penetrate into your organization. Proactive defence is key to mitigating operational risk and ought to be part of your high performance secure networking strategy.

Organizational Operational Security

Sensitive corporate information exists outside of the enterprise perimeter and your sphere of control. In fact, it can be argued convincingly that more useful intelligence can be derived on your organization from an external perspective than an one. Inbound/outbound analysis of data flows (communications, financial records, goods and services) and interconnectivity, can accurately assess critical interdependencies, corporate capabilities and assurance levels. Critical cyber infrastructure interdependency research has a dual purpose in target-templating large organizational infrastructures including nation states. Critical analysis of social networking, blogging, posts, articles, supply chain, contracting records, resumes, and outsourcing practices say a lot about an organization. The intercept of and traffic flow analysis of your communications outside your enterprise, in the cloud and across hostile network space, can yield valuable intelligence. This is why many companies invest in brand protection and social media monitoring, and counter with aggressive market campaigns, deception planning and competitive intelligence programs of their own.

Classified information does not spontaneously appear in a Sensitive Compartmented Information Facility (SCIF). It comes from the outside, most likely from hostile zones and the

threats themselves. There is an electronic path to nearly every classified e-document to the Internet and less than 6 degrees of separation to the enemy's computer system. Most of this path is outside your area of control, but it should be within your sphere of interest.

Building a secure network may start with the building itself. New facilities are prime targets for infiltration.[95] Information can move freely in an out of a building. Through covert channels, illicit Internet connections, mobile phones, fortuitous conductors, non-stop highjacking, electromagnetic flooding, shaped hardware/software, water pipes, power-lines, CCTV, teleconferencing equipment, off-hook telephone receivers, computer zombies, spys, refuse, postage/shipping, USB keys, paper documents, cameras, security/fire systems, wireless hubs, non-cooperative radio transmitters (bugs), sound transmission, cleaning staff, cable-plant, or covert entry etc. All the kit from Q's lab.

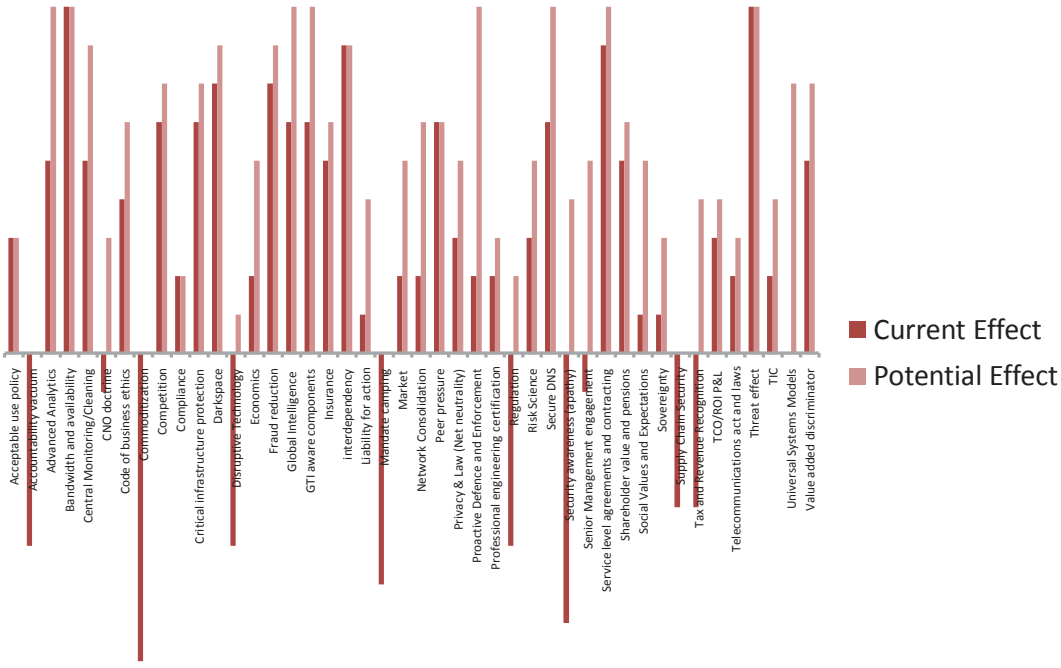
A secure network can be compromises in the most inane manner such as photographing a computer screen from across the street with a 400mm camera lens. It is embarrassing to spend a billion on technology only to have the system compromised by the cleaner and momentary physical access. Therefore, secure network design is only in part technical. It must be undertaken in the context of operational security[96].

Architectural attributes of a secure network

This research monitored the flow of malicious traffic at a national scale for over two years, identified the key influencers on this traffic and observed the positive and negative effects. A system model was created and combined with previous research on critical cyber interdependencies. Cyberspace, like the matrix, is an equation constantly trying to balance itself out. The equation of security and insecurity in cyberspace is influenced by technical and not technical variables. Each one of these variables has a protective index (multiplier) associated with it. The components (variables) must be addressed in both national cyber security strategy and enterprise information security architectures.

The following chart provides a relative rating of current and potential effectiveness of technical and non-technical controls against malicious traffic in Canada.

[95] Safeguarding Government Information and Assets in Contracting of the October 2007 report of the Auditor General of Canada. Report of the Standing Committee on Public Accounts. April 2010. In the matter of security compromises of the NORAD above ground complex North Bay, and "failure to address security in the construction phases."
[96] Operational Security, White Paper, Bell Canada, Jun 2010



Reference Architecture – Comprehensive National Cyber Security Initiative©

Planners must address the aforementioned foundational concepts for secure network architecture but the details need to be pragmatic, contemporary and technology centric. There are some bits of security technology, tradecraft, programs and initiatives, which have been demonstrated to yield particularly high Return on Investment (ROI) and lower Total Cost of Ownership (TCO).

A high level design

The following represent the most critical technical components of a high performance secure network architecture. These components align with fundamental strategies of network defence:

- Defence-in-depth
- Upstream Security
- Trusted Internet Connectivity
- Instrumentation
- Virtualization
- Cloud
- SEIM
- Cyber Intelligence
- Near-real time risk management
- Agile Networks
- Stealth
- Advanced Investigative Network
- Proactive Defence

Defence-in-depth

Defence-in-depth is a well-accepted strategy in network design. The concept is that consecutive layers of restrictive security mechanisms are engineered in between an adversary and the information assets. The true test of defence-in-depth architectures is in they must demonstrate a measurable reduction of malicious traffic at each layer.

In the past, a defence- in-depth strategy—a layering of like technologies—was sufficient. Today's approach, however, needs to harness correlated threat information from around the globe and across all threat vectors. That intelligence needs to be driven into a broad array of security products, enabling those products to enforce local policies based on the latest threat activity, and to share information so that the overall security infrastructure works in concert. [The New Era of Botnets, By Zheng Bu, Pedro Bueno, Rahul Kashyap, and Adam Wosotowsky, McAfee Labs]

Although the notion is sound, the pragmatic implementation of a true defence-in-depth strategy for many corporate infrastructures has been elusive.

When we look at the actual security market in Canada we find that, in general, enterprises and governments purchase security in silos and deploy orphan solutions. Many different point-solutions, do not constitute defence-in-depth, nor do they appear to reduce risk. Having multiple security zones with similar security mechanisms will appear as just one zone to an attacker.

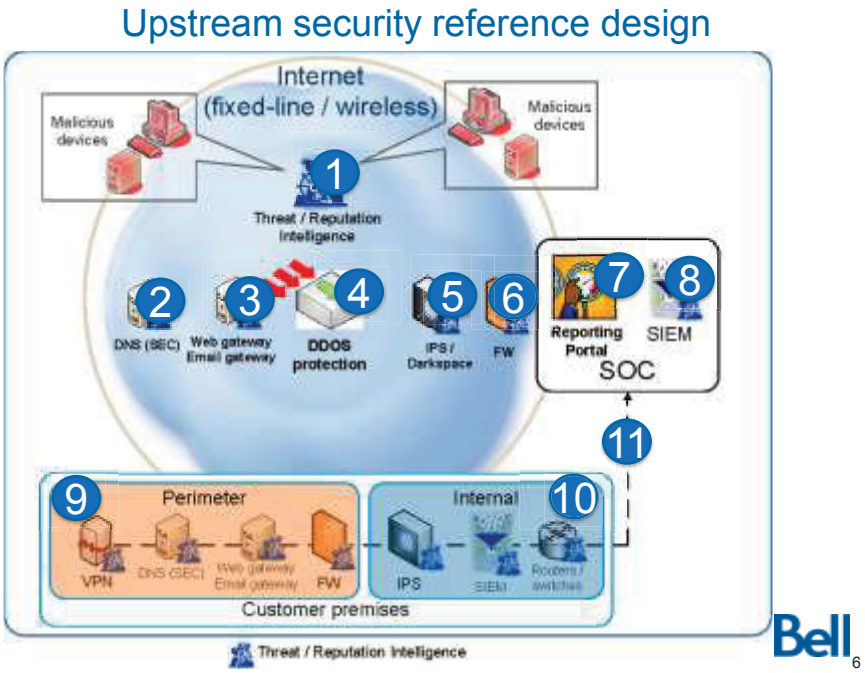
If a user can go directly to a web site and the content is served to their computer without introspection or filtering, then you have no defence-in-depth.

The conceptual challenge is that in cyberspace, attacks move through logical layers, not physical ones. Risk contagion is conducted by interdependencies, which bypass the 'pill boxes' of a traditional fortress defences and physical mindset. Toxic content finds its way into an organization through social engineering and zero-day malware.

Organizations often fail to appreciate operational security, their degree of interdependency, the extension of their supply chain or the providence of information upon which they depend. It is disquieting how many information security professionals ignore the care of corporate information once it have left the building, nor do they have visibility, influence or control of the inbound communications before reaching their civic address. Operational security research (purple team testing) can show the degree to which sensitive corporate information and competitive intelligence about an enterprise can be acquired from non-intrusive sources and methods outside an organization's sphere of control. CIOs and CISOs are often shocked at the findings.

Upstream (Cloud) Security

Defence-in-depth starts by upstream (cloud) security from your Service Provider who can tap use enlist global assets to clean the pipes. An organization greatly reduces risk by pushing enterprise security policies into the cloud and stopping attacks before they ever reach their organizational perimeter whether that is malware filtering, anti-phishing, reputational filtering, web integrity checks, DNSsec, or DDoS protection. Conversely, traffic egressing the enterprise can be monitored for and cleaned of malware, spam covert channels, or the leakage of sensitive data (DLP). The enterprise can benefit from carrier-grade security capabilities; one's which they normally could not afford. Corporate information in the wild can also be monitored with brand protection services. Surveillance of threat networks (dark web) for your corporate data or targeting information is useful intelligence to indicate compromises or provide early warning.



Cloud Annotations

1. Upstream Intelligence seeded from vendor and carrier sources about known, bad addresses, domains, hosts and ASNs
2. Domain Name Services are hardened against compromise, monitored and seeded with UI and set to alter when devices attempting to connect to malicious sites on the Internet
3. Web filtering inbound and outbound for illicit content, acceptable use violations, and device attempting to connect to malicious sites on the Internet
4. DDOS protection to protect gateways to cloud sources from public networks (Internet), and to protect branch gateways to public networks supporting cloud-access.
5. Intrusion prevention and darkspace monitoring for external probes and attacks , outbound command-and-control communications for compromised devices, randomized scan traffic to unassigned addresses.
6. Application-level firewall applying Upstream intelligence sources to deny connections despite the apparent legitimacy of sessions and payloads.
7. On-line, two-factor authenticated security event portal providing interface to the SIEM.
8. Security Information and Event Management (SIEM) engine aggregating and correlating logs and alerts from all devices under management.
9. Alternative or augmentation to pure cloud-based security: perimeter devices on premises managed from the Security Operations Centre (SOC), and reporting through the on-line portal (#7 and #8). Management can occur over the internet or through dedicate private connections (#11).

10. Alternative or augmentation to pure cloud-based security: devices on premises managed from the Security Operations Centre (SOC), and reporting through the on-line portal (#7 and #8). Management can occur over the internet or through dedicate private connections (#11).
11. Dedicated, private network link to SOC for out of band management,

Trusted Internet Connectivity

Corporate Internet access is not a commodity. Organization's who treat it as such and have unrestricted pervasive access have significantly more compromises as shown in high rates of malicious traffic. Thousands of ad hoc Internet access points is untenable for any defensive perimeter.

Perimeter Defence Control Points

The bidirectional clean-pipe from the Internet ought to connect to the organizational perimeter at known control points, where the enterprise can further monitor and clean. Upstream intelligence can be correlated with enterprise metrics to identify specific infected hosts or users. This information would not normally be available to the carrier.

Security is only as strong as your weakest link, or layer. So once information is within the enterprise it must be protected while in motion and at rest. Confidentiality, integrity and availably must be assured at all network layers.

Perimeter security solutions are impacted by cloud computing in that they will need to interface with the carrier grade intelligence-loop linking the combat operations processes of observe, orient, decide, and act (OODA) as part of responding to threats, vulnerabilities and compromises. At a minimum, information about detected zero-day compromises will prompt security administrators to quarantine systems and deploy and change rule-sets expeditiously. For enterprises deploying this methodology within their own enterprise network, interfacing with a tier-1 carrier in order to access intelligence, is required. Depending on how the enterprise network is managed, more or less of the carrier intelligence may be re-applied to security configurations both within the enterprise core and on the perimeter; especially if the enterprise has multiple gateways to independent carriers and service providers, or supports network gateways to partner enterprise networks.

Instrumentation – Logging and Intelligence Led Enforcement

Information Communications and Security Technologies have a primary function whether that is routing, load balancing, firewall, anti-spam, intrusion detection, etc., for which then are purchased and deployed within an infrastructure.

But they have two other very important network health and security functions that are rarely turned on. Security aware network components can produce logs (monitor) and enforce security policy based upon real-time intelligence.

The future lies in between in the infinite "shades of grey" between something we absolutely know is bad and something we absolutely believe is good. The question is one of "trustability." Reputational ratings that place trust on a particular logical entity (user, virtual appliance, virtual machine, browser plug-in, service, application, e-mail, and so on) in this context (time of day, value of the transaction, behavior exhibited, characteristics of the code, digital signatures, metadata, and so on) to be allowed to do whatever it is trying to do (run, execute a transaction, access a piece of information, access a network port and so on). The notion of "reputation services" is already used in URL and spam filtering solutions (where we routinely deal with unknown logical entities, web pages and e-mail). This will be extended to applications, user identities and even information itself. [Information Security Has It All Wrong – Gartner]

Each network component, down to a laptop or iPhone can act as a well informed neighborhood watch.

Virtualization

An important consideration is that all network components and processes can be virtualized and easily scaled to enterprise or national levels. The significance of virtualization is that enterprise's information security architecture can be designed, built and turned on, or moved with keystrokes. Virtualized infrastructure can be engineering to be highly-resilient and can be modified to adapt to a dynamic threat environment.

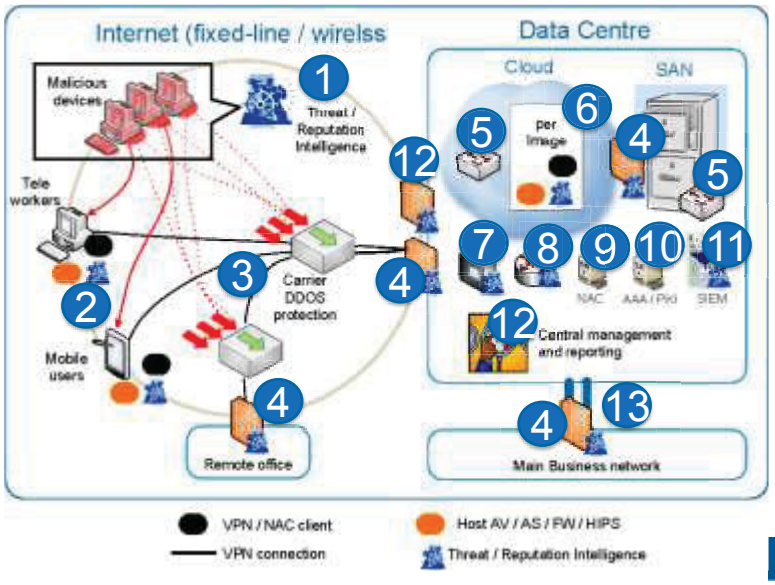
Boxes are a relic. Most security controls will be virtualized… convergence [however, should come] first, virtualization second. Virtualization enables introspection, parallelization and throttling; hybrid protection as needed. [Information Security Has It All Wrong – Gartner]

Hardware-based organizations whose computers and servers have been compromised with APT and rootkits often have to abandon millions in ICT investment.

Cloud

Elastic cloud super-computing offers on-demand dynamic processing, storage, bandwidth and Internet addressing. A trusted cloud can be provisioned across a backbone network of hardened in-country data centres; connected at the speed at light with geographic diversity. The beauty of cloud security is the flexibility and resiliency that it affords. Communications within the cloud provides six-nines of availability, which is more reliable than your computer's hard drive. Network agility a major tenet of maneuver warfare in cyberspace.

Cloud-computing security reference design



Cloud Annotations

1. Upstream Intelligence seeded from vendor and carrier sources about known, bad addresses, domains, hosts and ASNs
2. Remote devices loaded with security software bundled, including Upstream Intelligence sources to deny connections despite the apparent legitimacy of sessions and payloads.
3. DDOS protection to protect gateways to cloud sources from public networks (Internet), and to protect branch gateways to public networks supporting cloud-access.
4. Application-level firewall applying Upstream intelligence sources to deny connections despite the apparent legitimacy of sessions and payloads.
5. Platform soft-switches applying ACLs between zones and within zones at the image-level
6. Virtual images loaded with security software bundled, including Upstream Intelligence sources to deny connections despite the apparent legitimacy of sessions and payloads. Dormant (offline) images scanned and patched.
7. Data centre network IPS loaded with Upstream Intelligence
8. Data centre routers (and switches) loaded with Upstream Intelligence
9. Network Access Control (NAC) – users, devices, addresses and ports
10. AAA / PKI / IDM – credentialing, key management
11. Security Information and Event Management (SIEM) – servers, network elements, security elements

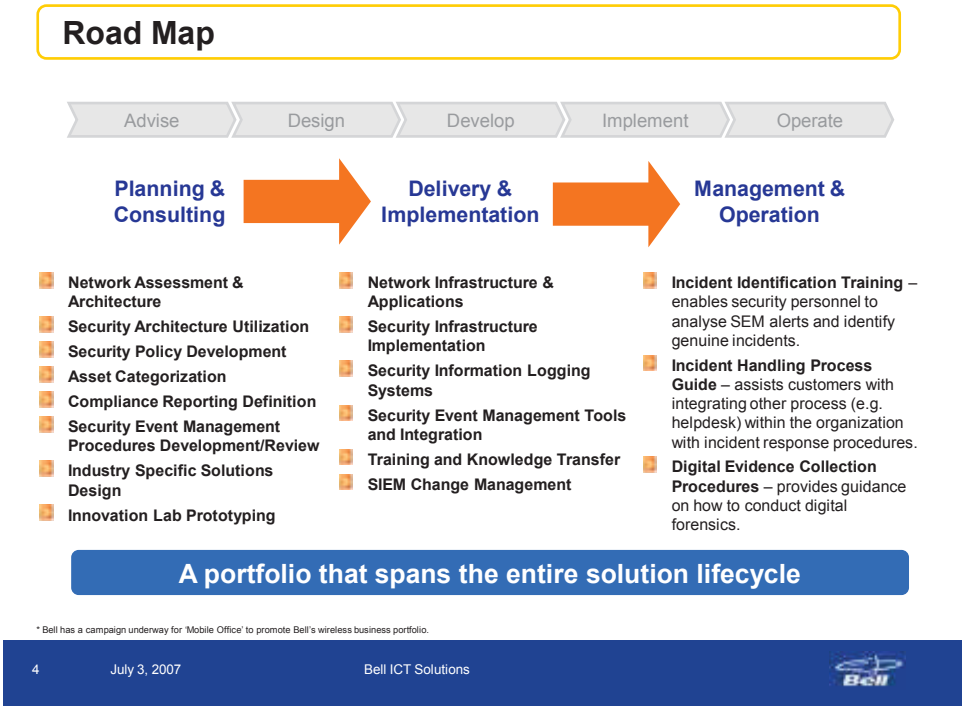
12. Centralized tool for both managing security elements (config / update), monitoring and reporting events and alerting.
13. Diverse (redundant) network connections – internet connections and private connections

Security Information Event Management (SIEM)

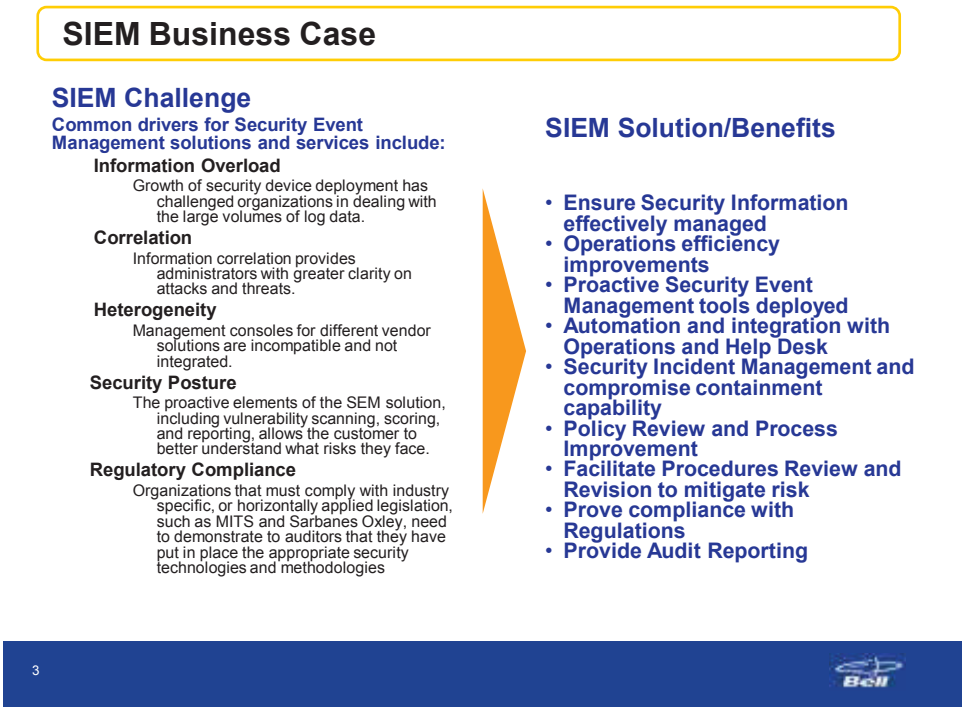
A large network can have thousands or millions of security enabled sensors creating terabytes of logs every day. It is impractical for any system administrator to analyze this massive data stream. So, often logs are turned off, overwritten or sent to ground. Only when there is a noticeable incident, such as a network failure are the logs consulted.

All outputs and logs from an enterprise level network need to be fed into a Security Information Event Management (SIEM) system. This seems intuitive but most large organizations do not have operational SIEM nor do they outsource Managed Security Services (MSS).

A SIEM when integrated with a risk management tool can provide operators and executive with a common picture for the entire organization. The network is running blind without SIEM or MSS.



Security staff can attempt to consolidate security data for viewing purposes, but this approach lacks the scalability, efficiency, real-time analysis and correlated intelligence to provide meaningful information, and it tends to be reactive. Organizations are also challenged in staffing the security expertise required to process this data. The ability to analyze and automatically respond to events provided by security products around the clock in real-time is often the differentiator between the success and failure of threat mitigation.



Common drivers for Security Information and Event Management solutions and services include:

- Information Overload - Growth of security device deployment has challenged organizations in dealing with the large volumes of log data.
- Correlation - Information correlation provides administrators with greater clarity on attacks and threats.
- Heterogeneity - Management consoles for different vendor solutions are incompatible and not integrated, and log data formats are disparate.
- Security Posture - The elements of the SIEM solution, including vulnerability scanning, scoring events according to security policy, and reporting, facliltates better understand what risks they face.
- Regulatory Compliance - Organizations that must comply with industry specific, or horizontally applied legislation, such as MITS and Sarbanes Oxley, need to demonstrate to auditors that they have put in place the appropriate security technologies and methodologies to address compliance.

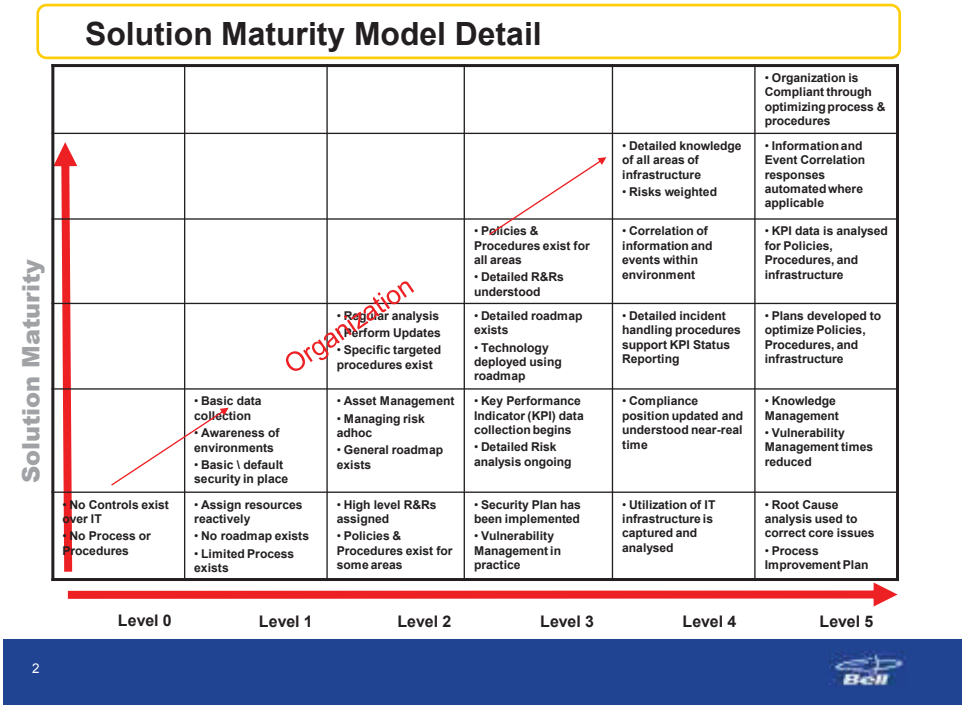
A Security Information and Event Management (SIEM) Service provides a solution to manage and correlate large amounts of disparate log data generated by equipment such as: Firewalls, switches and routers, IDS/IPS, URL Content Filtering, Anti-Spam and Anti-Virus systems, VPN gateways, Servers (i.e. syslog), Physical Access Control systems, etc.

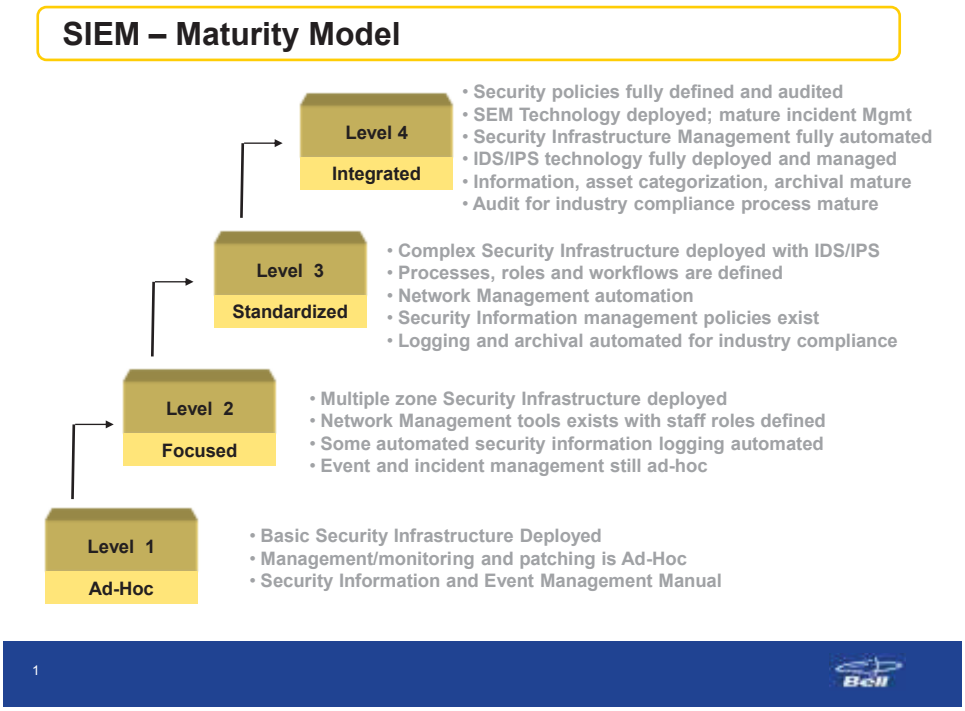
A MSS SIEM Service is designed to overcome the challenges of managing and deriving value from these Security Information sources by automating the processing and aggregation of the massive amounts of data generated by system and security devices throughout an enterprise.

The synthesized data is then correlated against vulnerability scan results, asset risk profiles and security intelligence knowledge bases to generate an accurate threat assessment for any given event monitored 7x24x365 by Security Operations Centres. Holistic threat assessment and alert notification provides the information security staff with the intelligence and incident handling support services that they need to understand and respond to security threats in real-time.

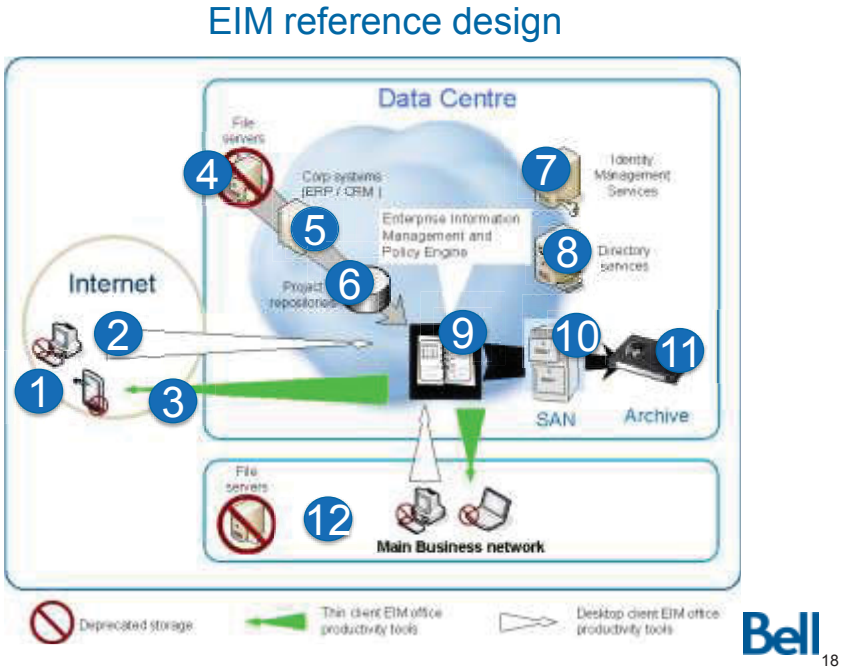
SIEM High Level Functions consist of:

- Data Collection - The service collects data from multiple event sources and maintains logs for ongoing review.
- Normalization - The data is normalized into common and consistent event schemas.
- Aggregation, Scoring & Correlation - The data is filtered and aggregated to reduce the large quantity of data.
- Event Management - The administrator has real-time access to the service for monitoring and incident handling.
- Information Management - Historical data access is maintained for forensic and review analysis.
- Protective elements of the SIEM solution, include: vulnerability scanning, scoring, correlation and reporting,





Security Information and Event Management (SIEM) solutions can be designed to address these challenges by automating the processing and aggregation of the massive amounts of data generated by security devices throughout an enterprise and correlating it with unique threat intelligence from the core. Proactive cyber defence including Botnet interdiction and disruption, DDoS protection and covert channel detection can be instigated within the cloud where they are most effective. The synthesized data is then correlated against security policies, vulnerability scan results, asset risk profiles and security intelligence knowledge bases to generate an accurate threat assessment for any given security event. The holistic threat assessment provides the information security staff with the intelligence and incident handling support services that they need to understand and respond to security threats in real-time. This is the basis for a Detection, Analysis and Response Infrastructure Conceptual Architecture.



EIM Annotations

1. Data storage on end-point devices disabled or limited by policy and audit procedures
2. Desktop office productivity software manages content (email, vmail, documents, collaboration, other) and interfaces with EIM
3. Thin client office productivity software loaded from EIM manages content (email, vmail, documents, collaboration, other)
4. Legacy file servers have data cleansed and loaded to EIM for management, then decommissioned.
5. Corporate systems such as ERP and CRM systems transfer closed records and event logs to EIM.
6. Project and service repositories such as databases and collaboration applications transfer closed records and event logs to EIM.
7. Identity Management service to define access controls on users, roles and groups.
8. Directory services for user and application account management.
9. Enterprise Information Management engine to enforce logging, retention and disposal policy established by legal/records management/IT departments.
10. Storage Area Network supporting EIM for active (subject to review or revision) records.
11. Long term archive for non-active records.
12. Devices on business network as either desktop or thin clients. Local file servers have content cleansed, transferred to EIM and decommissioned.

Cyber Intelligence

These systems are only as good as the quality and coverage of the sources of data, and that is where carrier grade upstream security and intelligence services are vital in providing situational awareness in the information battle-space, manage incidents and undertake effective proactive defence-in-depth.

The output from security appliances is esoteric, and lacks the real-world context required for predictive threat assessments. It falls short of delivering relevant intelligence to businesses operating in a competitive marketplace. Global cyber threat Intelligence provides unique and accurate insight into the Cyber-Risk ecosystem. Global threat intelligence uses all-source collection and analysis methods to produce and deliver precise and timely intelligence; guiding not only the "business of security" but the "security of the business". It is built upon accurate security metrics (cyber and physical), market analysis, technology forecasting, and are correlated to real-world events.

In-the-cloud engines can collect and correlate threat data from across all threat vectors, constructs a complete threat model, and delivers protection to local engines and policy-based enforcement mechanisms. [The New Era of Botnets, By Zheng Bu, Pedro Bueno, Rahul Kashyap, and Adam Wosotowsky, McAfee Labs]

Core Intelligence is important for any SIEM system to identify sub-zero-day cyber threats and vulnerabilities which are passing un-detected by security products operating at the network edges; firewalls, Intrusion Detection Services (IDS), and anti-virus tools. These threat and vulnerabilities become visible at the carrier and root network level – at the access, distribution and core layers of the World's largest carrier networks. This should be of interest to not only network administrators and security practitioners, but to those concerned with wider Operational Risks related to issues such as liability, privacy, data loss prevention, brand and reputational risks. The architectural methodology must still be integrated with good perimeter security, it must be supported with security event management tools for visualization and reporting, and it must be coupled with incident response capabilities and more importantly, proactive defence.

Near-real time risk management

A risk methodology should start with a strategic common operating picture.

Upstream infrastructure providers can provide an organizational view of risk by measuring (logical and physical) connectivity. This would include inbound/outbound net-flow of legitimate communications and malicious traffic. The organization is scrutinized as a block box based on monitoring communications to/from blocks Internet address space and identified physical premises. From this data set, it is possible to:

- determine organizational assurance levels and profiles when compared with statistical norms;
- detect illicit communications channels;
- critical interdependencies and risk contagion;
- zero-in on infiltration and exfiltration paths;
- identify threat agents, attack vectors and infected machines (to a limited degree);
- calculate network performance and degradation;
- assess preliminary loss-impact / revenue at risk; and
- initialize immediate proactive mitigation. Sink-hole attacks and block out-bound exfiltration.

Sensor(s) within the enterprise zone and security-aware ICT components, are enabled by global threat intelligence, and the resultant telemetry (logs) from an enterprise network can be correlated with upstream sources. Sophisticated sensoring can provide valuable forensics that you will need for the Threat Risk Assessment (TRA). Any good TRA will generate an incident and investigation. The initial findings are directed to the forensic and incident handling team for immediate remediation.

There are a number of security activities that should be performed concurrently and in a coordinated fashion:

- conduct the full-spectrum of vulnerability and penetration testing of your organizational infostructure;
- Asset inventory, configuration management picture, value assessments of both infrastructure and infostructure, goods and services, and business operations;
- Draw network infra/infostructure diagrams;
- Determine risk tolerance levels in real currency $;
- Conduct compliance audit of existing security controls and calculate compliance risk (normalize to real currency $);
- Establish assurance targets (lowest standard, common practice, best ROI, best effort); and
- Gather accurate threat intelligence that includes work-factors for attack vectors, black market values, and the means, motives and capabilities of primary threat-agents.

The operational 'network' ought to be compared to a reference security architecture that matches the organization's assurance target. Note Δ or deviations.

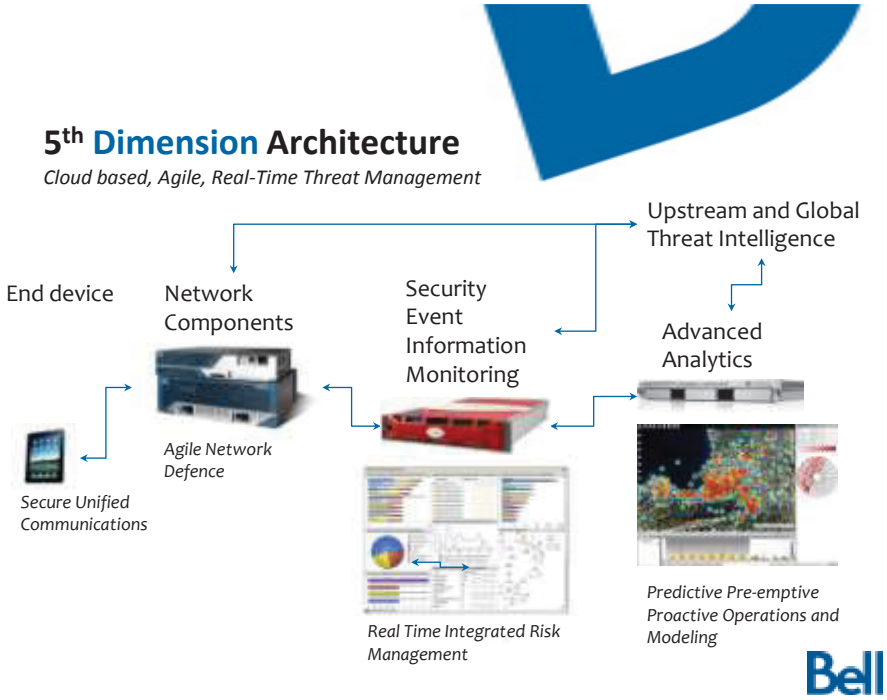
The risk assessment is an iterative process. As the threat, vulnerability, network (infra/info structure) configuration and asset-value data accumulates, more statistically value exposure-likelihood mathematical probabilities can be calculated.

Let's look at tuning the adaptive-network cycle and real-time risk management. Exposures, as they materialize, will precipitate immediate remediation. Architectural changes should be made on the basis of a real measurable threat, using solutions, which have shown to have very good ROI.

The feedback (OODA) loop between real time risk assessment and security engineering is critical; the effects of malicious traffic/attacks are measured as infrastructure changes are made to a live network. A safeguard or architectural modification, which successfully (and affordably) reduces measurable exposures, is worth keeping. Ideas that do not reduce malicious traffic loads do not have merit and should be abandoned. In this way, risk analysis is a continuous process that can tune adaptive network defence, and operational security of the organization in a proactive manner. Risk assessment and enterprise security architecture are not activities that you do just once at the beginning of a project – they are a continuous process. This process of threat detection, risk assessment, and architectural tuning can be virtualized and automated.

Integrated Risk Management Services (IRMS)

The real risks experienced by an organization have traditionally been viewed in silos of: financial risks, business risks, operational risks and threat risks. An integrated risk management framework establishes a formal analytical practice that correlates various perspectives of risk and delivers an unequivocal and unified assessment of risk. Thus, tuning the business towards optimum efficiencies. A number of systems exist that can interpret the esoteric risk outputs from financial, network security, HR, and sales forecasting systems, etc., perform clever data-fusion and present a unified integrated risk picture to the enterprise.



The Gartner Group describes Adaptive Security Infrastructure using a biological allegory. As networks become more complex they behave more like biological systems. By examining security and defences in a body or ecosystem, scientists can hope to develop advanced cyber security solutions.

The human immune system relies on a set of layered defence technologies (a "defence in depth" strategy) where the layered defences function as a system. Most threats can be blocked at the perimeter. The human immune system is thought to accomplish this by using a modeling of everything that is "not self." Although this approach minimizes false positives, the number of sensors required to accomplish this in the human body is high (approximately

4x109 and 11x109 per liter), achieved with a level of parallelism that's not possible with computing technology. In multicellular organisms, cells constantly engage in orderly "programmed death," known as apoptosis. On average, the entire human body regenerates itself once a year with no apparent loss of the information we carry (DNA). In information security, we often forget that our goal isn't protection of individual devices, but the protection of workloads and information that is our fundamental charter. [Information Security Has It All Wrong – Gartner]

Agile Networks

Cyber security is all about maneuver warfare, not the thin red line tactic of a historic battlefield or the notional impenetrable fortress that the enemy can then lay siege to.

The most effective and expedient defence against an attack is to move out of the line-of-fire, then adapt your defensive posture to the attack. Networks have architecture and occupy IP space. Vulnerabilities in the architecture are exploited through an IP address faster than a human can respond. So change the architecture and IP addresses in response to a threat. Do it in real-time and automate the process.

This process because feasible once the real-time integrated risk management framework is established. The algorithms and decision engines are programmed and tuned and monitored by security experts. Over time, the fidelity of the model improves. That being said, some high-impact or risky decisions, would likely rest within the hands of a human.

The most advantageous moment to act is during the enemy's preparation to attack. This is possible with good global (upstream) intelligence warnings and indicators.

Stealth

Manoeuvrability (network agility) is an important defensive capability, but stealth is even better. It is difficult to target an infrastructure that is not advertised on the Internet. Non-attributable, covert, and clandestine access to the Internet through anonymizing proxies, private TOR networks, botnets or IPv6 carrier network translation, can hide the enterprise from deliberate targeted attacks provided that the service include persona management, trusted internet connectivity, consolidated network access points, content inspection, cleaning and secure DNS.

Now the challenge with stealth is that the network becomes conspicuous by its absence and can be re-acquired through null-steerage techniques. An 'avatar' network can be used to fill in the hole that was made. Pragmatically, would take the form of creating a honeynet and advertising it on the Internet as the corporate network. This 'avatar' network would also act as a darknet which can be used to detect probing and malicious activity from external threats with a good degree of precision.

Advanced Investigative Network

The gold standard for security architecture including the complete instrumentation of the network with security aware ICT devices fed by global intelligence sources and monitored by a SIEM can provide the 98% solution to network security.

Once we have established how a cybercrime operation may be impacted by changing the risk/effort/reward ratio, we need to have clear-cut methods of manipulating those factors. The tactics will vary depending on what type of criminal operation is targeted. [Beyond Takedowns: Offense in Depth By Joe Stewart, Director of Malware Research with the SecureWorks Counter Threat Unit.]

Sophisticated APT and complex attacks require a highly skilled team and an advanced investigative capability consisting of:

- Access to all corporate data sources and SIEM
- Special sensor network and sources consisting of DPI, honeynets, recursive DNS etc.
- Covert Access to the Internet
- An advanced Data Fusion Platform
- Specialized forensic tools
- Tradecraft

Network and security operation centres would use a SIEM tool to manage network health, performance and security 24/7. Typically, the staff does not have the time, tools or tradecraft to undertake deep-dive investigations or develop specialized countermeasures against sophisticated threats. Their day is consumed with putting out fires not strategic initiatives or proactive measures.

The mission of the advanced investigative capability is to

- Conduct deep-dive forensic investigations
- Provide analytical support to the SoC
- Program signatures and decision engines into the integrated risk model
- Develop and implement sophisticated mitigation strategies
- Proactive solutions

Proactive Defence

Proactive Cyber Defence means acting in anticipation to oppose an attack against computers and networks. It represents the thermocline between purely offensive and defensive action; interdicting and disrupting an attack or a threat's preparation to attack, either pre-emptively or in self-defence. Canada is currently decisively engaged in a cyberwar, and the only effective national defence strategy is a proactive one.

A modern fighter-jet has agility, maneuverability, stealth, but needs firepower and the ability to project force. Why would a network be so different in a cyber-war.

The whitepaper, *Proactive Cyber Defence* published in 2008 [Bell Canada] provides a primer for the science and pragmatics of proactive cyber defence based upon zero-day proof and quantitative threat metrics. It begins with a rich historical perspective that demonstrates the maturation of the discipline and operation global programs. Subsequently, the discussion tenders definitions and theoretical models, and exposes common misinterpretations and stratagems. The calculus of droactive cyber defence is that it ultimately buys your decision-making time and precision with the lowest costed options.

Computer Users Need 'Offensive' Security [McAfee Security Journal Issue 6, 2010]

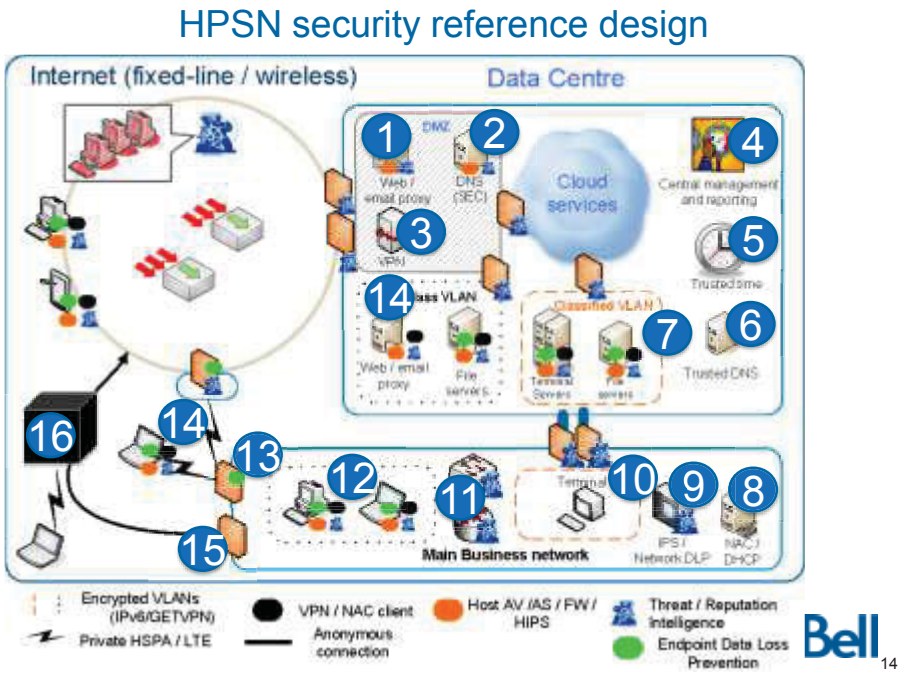
Proactive defence should concern: enterprise security architects responsible to design and build robust infrastructures; legal counsel and privacy advocates may achieve a deeper understanding of liabilities and responsibilities, particularly related to dangerous institutional policies and risk-adverse practices that perpetuate inactive or retroactive defence. Executives need to know that there is an incontrovertible business case behind their proactive programmes and a realization that the issues are not technical or financial. Security analysts need a clear threat perspective on a national scale, workable precepts for calculating risk and actionable intelligence.

Ironically, most organizations have invested heavily in treating the symptoms and not the cause. Words like 'react', 'respond', 'recover', and 'restore' are expensive ideas that we can ill afford to take priority. Cue to the adage "an ounce of prevention is worth a pound of cure" and take it to heart.

Furthermore, predicting and interdicting an attack before it occurs, provides more options at lower cost, than detecting and reacting to an impact, which presents few choices and all them costly.

The Reference Architecture for High Performance Secure Networking ©

The following diagram and annotations summarize an engineering architectural view to a high performance secure network that we have found to be highly resistant to advanced persistent threats.



HPSN Annotations

1. Inbound connections to public webservers (not shown) and email servers (not shown) are scanned for malicious code and source reputation.
2. Hardened external DNS (incl. DNSSEC) available for authoritative domains.
3. VPN concentrators for remote access over the internet
4. Centralized event monitoring and security device management
5. Trusted time source for endpoint coordination
6. Hardened DNS (incl DNSSEC)
7. Cryptographically segregated network zone (GETVPN / IPv6) for highly sensitive data - terminal servers to prevent sensitive data from residing on end-point devices, including DLP, malware and Upstream controls.
8. Network access and DHCP for users, devices and ports at LAN-level
9. IPS and DLP at LAN/WAN level
10. Cryptographically segregated VLAN (GETVPN / IPv6) for most sensitive data with "dumb" terminal
11. LAN/WAN routers (and switches) loaded with Upstream Intelligence

12. Desktops and laptops loaded with DLP, malware and Upstream controls.
13. Non-internet gateways on carrier MPLS network with in-line DLP
14. Non-internet cellular wireless connection for unclassified devices and alternate connection from branches
15. Egress gateways from unclassified VLANs with DLP, malware and Upstream controls.
16. Trusted unlisted internet access

ADVANCED ANALYTICAL CAPABILITY

Building an Advanced Investigative Capability

The principle challenge facing law enforcement and national security institutions addressing cyberspace is an absence of appropriate of tools, tradecraft, and permissions enabling clear and credible path from detection through to prosecution. The staggering growth of the Internet over the past 20 years has outpaced the capacity for law-enforcement and security institutions to adapt their procedures, obtain sufficient political guidance, and build the necessary capabilities to sustain effective policing within this domain.

In part, this challenge is inherent to the architecture of cyberspace, which emphasizes resilience over security, and where relatively frictionless global connectivity allows perpetrators to act locally, while hiding globally. The misuse of cyberspace is evident to telecommunications operators tasked with managing network flows. However, at present, institutional, legal, cultural and regulatory boundaries make it difficult for law enforcement and security agencies to gain a Common Operating Picture (COP) of national cyberspace, and gather sufficient pre-warrant awareness to rapidly and effectively respond to criminal and national security incidences occurring in this domain. Consequently, cyberspace represents a global platform for criminal and espionage activities, whereas law-enforcement and security actors are presently bound by institutional and national jurisdictions and hampered by limited global reach.

Cyberspace also represents a unique challenge in that threats can occur to the network, and through the network, requiring unique skills and permissions:

- Threats to the network - which includes bot nets, malware, and other means to exploit or disable computer systems - require technical skill sets not commonly available within law enforcement and security community. Moreover, standards of evidence are not fully developed or consistent across national boundaries. Collection can be problematic as often information gathered in the pre-warrent phase may be critical, but inadmissible as evidence in a criminal case.

- Threats through the network - such as the exploitation of women and minors, illicit value transfer, wire fraud, radicalization and information sharing among militant communities, and other activities that leverage cyberspace - require capabilities to conduct covert and undercover work in cyberspace.

They also require skills and capabilities to conduct rapid entity resolution, pinpoint attribution, and collect evidence according to standards, which are admissible, resilient to charter challenges, and likely to lead to successful prosecutions.

Addressing these challenges will take time. It requires changes at the policy and institutional level - to establish new standards of evidence, investigatory powers, and legal permission to allow law enforcement and security actors to monitor national cyberspace to a level sufficient to enable effective policing without impacting privacy. It will require the adoption of new tradecraft and techniques relevant to conducting investigations in cyberspace, and the training of personnel tasked with these duties. Finally, it will require law enforcement and security actors to enter into collaborative relationships with private sector actors to source evidence, provide ongoing situational awareness, and to support and conduct investigations and related activities, with suitable oversight.

Situational Understanding and a Common Operating Picture

Creating an effective policing mechanism for cyberspace, such as that required counter threat of bot nets, is dependent on attaining situational understanding and a Common Operating Picture. A rough analogy would be the establishment of a national air traffic control centre for cyberspace, but one tasked with monitoring rather than directing traffic. Establishing such a capacity requires access to relevant data sources, and an ability to 'fuse' and analyze these in a meaningful way, and in real time. Situational understanding by the collection and processing, a presentation of data in a way which would make it meaningful to decision-making requires two levels: the national jurisdiction - that is to say the jurisdiction over which national law enforcement and security actors have direct enforcement authority; and, of global level (which is necessitated by the common protocols and routing infrastructure of the Internet). At present, attaining situational understanding is difficult. Ownership over data is fragmented, and most of it resides with the private sector, including telecommunications operators and firms specializing in gathering network metrics and intelligence.

A Common Operating Picture by contrast, would encompass multiple views onto the status of the national infrastructure but segmented by specific needs of intelligence, law-enforcement, defence, and telecommunications actors. In the UK, one of the early adopters of such an approach a the all-of-government level, this function is handled by the Cyber Security Operations Center (CSOC), a multiagency fusion center which will operate out of the GCHQ facilities in Cheltenham which incorporates feeds from both private sector actors, and government sources.

Advanced Investigations

Research into botnets has expanded in recent years, from a relatively small cottage industry involving primarily technical experts to a budding cyber security industry, which now includes academia, defence, intelligence, law enforcement, and private sector actors. The rapid rise of this industry is in part recognition of the significant threat that these criminal ecosystems represent to critical infrastructure, government systems, personal privacy, and defence. Several high profile cases and events, including the release of the Ghostnet study detailing alleged Chinese cyber espionage, the breaches at Google, as well is the way in which DDOS attacks were successfully leveraged during the Russian Georgia war of 2009 - have underscored the growing threat environment.

Countering advanced persistent threats, criminal bot nets, and DDOS events is a time-consuming and labor-intensive process. The challenges facing law enforcement are numerous. They include: access to appropriate tools with which to conduct investigations, access to relevant data and collection methods, clearly defined standards of evidence that will withstand charter and court challenges, and, a properly trained workforce capable of undertaking these investigations in a cost-effective manner is likely to lead to successful prosecutions. They also encompass methodological approaches, techniques and tradecraft appropriate to gathering evidence, analyzing data, and building cases involving complex cybercrime were multiple jurisdictions may be involved.

At an operational level, an investigation of Advanced Persistent Threat (APT) and Botnets can be broken down into four phases, each requiring specific tools, tradecraft, and process. (The table below provides a summary of an APT investigation process and associated requirements).

Detection and triage of cyberthreats (APT, Botnets)

APTs and botnets are part of a broader global ecosystem of crimeware whose size and scope is impressive. For example, the size of the cloud of computers currently infected by the Conficker virus exceeds that of the largest commercial cloud-based providers such as Google and Amazon by a significant margin. Consequently, early detection of threats is dependent upon the constant monitoring of the ecosystem, which includes monitoring for the existence and or emergence of criminal crimeware kits within national cyberspace, and awareness of overall global trends. It is also dependent upon an ability to conduct open source monitoring of known hacker forums, and other online sites used by cyber criminals and others distributing malware code. Finally, it is also dependent upon maintaining up-to-date awareness of specific signatures and other characteristics of targeted malware (APT). Often, this information will reside in private sector, or other difficult access sources. Law-enforcement actors need to seek appropriate permissions for access to this data, and often the process required to do so is difficult, and costly. Finally, it requires a trained workforce

capable of rapid processing of open source intelligence, and making it available to investigators and other agencies.

Evidence collection

This is critical to combating APTs and botnets but can be difficult both in terms of the means required to harvest relevant data, and the resulting size and quantity of data sets that must be processed and analyzed. Often, investigators can not capture very large data sets because it is difficult to anticipate ahead of time which streams of packets may be specifically important to a particular investigation. Commonly used packet capture programs such as wire shark are problematic, because they capture the entirety of the data stream and may inadvertently record traffic and data belonging to third parties. Collection may also have to occur against a variety of different devices. These can include personal computers, cell phones, or embedded devices such as smart meters. The requisite skills, and tools required to recover data from these systems are quite wide, and challenge law enforcement agencies with limited resources and skills. Finally, evidence collection presents investigators with a problem of determining the status of evidence, and whether it is captured during an intelligence phases, or for criminal prosecution purposes. In general terms, evidence collection in cyberspace investigations can be divided into three broad streams:

- In-stream technical data collection - This is typically obtained through capturing data streams between targeted systems and or communications pairs and is usually accomplished through the use of packet capture program, or devices. Data can be collected at the carrier level, under warrant. Data obtained from the source can be rapidly parsed and analyzed and imported into advanced link analysis and visualization software for further analysis, provided that you have the right tools and skills.

- Forensic extraction - obtained from seized systems and or devices, including cellular phones. The data could be used to reconstruct communications, established geo-temporal timelines and a social and link analysis, and recover other critical data relevant to the investigation. Advanced forensic extraction devices allow for rapid exploitation of data in a format that can be readily analyzed and exploited by advanced link analysis and visualization software.

Analysis

This step is most crucial, and perhaps most challenging component of an APT investigation. Often it requires access to, and the ability to manipulate and correlate disparate data sets. Some of these would be obtained from existing criminal intelligence and information systems. Others require access to private sector data sources, such as the ability to do

locate IP addresses and other technical data. Establishing identity in cyberspace is particularly challenging because a single entity can take on multiple personas. The ability to perform entity extraction and entity resolution is daunting, and difficult to do without the necessary tools and methods. Investigations are also iterative, and often information sources need to be added and/or eliminated throughout the lifetime cycle.

The evidence and data used for APT investigations is heterogeneous. It will include technical data obtained through network and technical evidence gathering techniques (as described above), Conventional policing techniques and investigation methods including (DNR and Part VI records), GPS tracking evidence, investigator notes, impossibly evidence gathered through warrants and MLATs will form part of the evidence base. This evidence will need to be correlated and analyzed using a number of different techniques depending on the nature of the case: geo-temporal analysis, to establish timelines and locations; Social network analysis (often incorporating wiretap and data stream information) to establish attribution, and complex analysis in order to demonstrate the operation, function, and victims of particular APT's. This latter form of analysis can be quite daunting, as it requires both a good understanding of the fusion and visualization environment, as well as a substantive understanding of how APTs function at a technical level.

The field of data fusion analysis is rapidly evolving, but few of these systems have been adapted to work with the very large and complex data sets required for conducting investigations in the cyber environment.

Reporting and Case Management.

Communicating the results of complex investigations is critical. Unless the presentation of evidence is clear, compelling, and understandable, legal challenges can tie up prosecutions, or lead to the dismissal of cases (are pleading to lesser charges). The ability to render the salient and relevant components of an investigation in a manner that is easy to communicate by a prosecutor, is key to successful prosecutions. The form in which analysis takes place, as well as the way in which it can be represented - as a timeline, as a chain of evidence leading to a perpetrator and as a means to describe the significance of an act or event, all form critical components of building a successful case. The majority of existing analytical packages, like Zeropoint and palantir, offer an ability to export snapshots of the investigation as PowerPoint slides, or other data simplify and highlight aspects of the investigation.

Archiving investigations, as complete data sets, is also an important component of building a knowledge base that can be applied against future investigations. Often the modus operandi, technical characteristics, or attack vectors will fall into specific patterns. The ability to mine and apply these patterns as whole, rather than their technical components can often shortened and simplify the investigation process in future iterations.

Consequently, analytical environments that permit storage and archiving of investigations as persistent search modules are preferred over those, which only store a representative level of the outcome of an investigation, rather than the underlying data and relationships.

Network Access

The network connection to the Internet that police use to conduct investigations or undercover operations needs to be trusted, secure and non-attributable. It has to be robust enough to withstand the most sophisticated attack and invisible so that it never has to. For much the same reason that the US Comprehensive National Cyber Security Initiative uses Trusted Internet Connectivity.

The Trusted Internet Connection (TIC) initiative was formalized in November 2007 by the USA with the goal of drastically decreasing the number connections to the Internet. The fewer connections to the Internet, the easier it is to monitor and clean traffic. Under the TIC initiative, all agencies must either work with an approved MTIPS (Managed Trusted Internet Protocol Service) provider (AT&T, Sprint, Verizon, or Qwest have been approved by GSA thus far) or be approved by The Department of Homeland Security to provide their own consolidated service by passing 51 requirements known as a TICAP (Trusted Internet Connection Access Provider).

Conclusion to solution-set

The most important consideration in high-performance secure network design is to address the foundational concepts first.

Too often, folks rely on fashion technical point solutions and soft policies to solve a remarkably complex problem. We must address the complexity of the system with an elegant yet simple solution. The error is analogous to choosing medication and surgery, when one should lead with proactive healthy lifestyle choices.

"*An ounce of prevention is worth a pound of cure.*"

The efficacy of an operational high-performance secure network is the confidentiality, integrity and availability that it provides. Today it is possible to achieve six-nines (99.999995%) in network efficiency. Networks also ought to be designed to achieve the best Return on Investment (ROI) and Total Cost of Ownership (TCO) as calculated based upon Key Performance Indicators (KPI) like the bandwidth of malicious traffic mitigated per security dollar spent. Active real-time risk management systems facilitate evidence based decision making during the security architecture phases in a tight OODA loop to create adaptive network security operations.

"You can't manage what you don't measure."

In addition to being proactive, security must provide integrated defence-in-depth and breadth by linking global and upstream security services through the enterprise to the desktop, at synaptic and semantic levels. Network design must be coherent with an overall operational security program that perceives the organizational infostructure from your spheres of control, influence and global interest.

It is important to review your network designs from the perspective of the threat and bolster attack vectors, which offer a path of least resistance into your organization. Similarly, in complex systems, risk contagion is a function of critical interdependencies, risk conductance and toxic content (assets). The way we measure risk and predict its impacts needs to be re-engineering along the lines of universal systems theory, weather forecasting, biological ecosystems and global financial markets. Traditional Threat Risk Assessments (TRA) and Enterprise Security Architectures (ESA) that are based upon qualitative assessments, policy compliance have seen their day.

All systems are inherently open and no system can therefore be entirely secure. Thus the ultimate objective of security engineering is to reduce the residual risks (business, operational and threat risk) to the cost-of doing business. In the matter of security engineering, the overall viability of business operations must always be of primary concern.

References:

2010 Olympic Threat Risk Assessment, Bell Canada, 2007

HostExploit – CyberCrime Series, Top 50 Bad Hosts and Networks, December 2009

PSTP08-0107eSec Combating Robot Networks and their Controllers, 19 April 2010

Cyberthreat, Publisher: Warwick Publishing (August 1, 2000) ISBN-13: 978-1894020831

The Interdependencies of Payment and Settlement Systems, Bank of International Settlements, June 2008

Assessing the Risks of our Interdependent Critical Infrastructures, Front Line Security Magazine, July 2008

Securing Converged IP Networks (Hardcover) ISBN-13: 978-0849375804, Auerbach Publications, 2006

Cyber Critical Infrastructure Interdependencies and State of Readiness Studies, Cyber Security Secretariat, PSEPC, issued 2006-04-28

Network Security Chapter for the Certified Information Systems Security Professional (CIISP), International Information Systems Security Certification Consortium ISC2, 2009

Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies (Hardcover), CRC Press, ISBN-13: 978-1420068351, 2008

The Perfect Cyber Storm, Canadian Security Magazine, August 2008

Proactive Cyber Defence, published Bell Canada 01.02.2008.

Enhancing Strong Enforcement with Active Policing, November 2007

Laying siege to Traditional Fortress Network Architectures, Analysis, Bell Canada, February 2008

National Proactive Cyber Defence Strategy for Canada, May 2008

The next Cyber Pandemic, June 2008

Intelligence Led Policing in a Converged World, Ontario Association of Chiefs of Police Magazine – Winter 07/08

Proactive Cyber Defence - an ounce of prevention is worth a pound of cure, Front Line Security Magazine, Spring 2008

FUTURES

This chapter presents a critical analysis of research and development in cyber security science and technology in Canada over the past five years. The addresses emergent, convergent and disruptive technologies and a crafts a future vision for worthwhile cyber security research based upon return on a real-world measurement of Return on Investment (ROI) and the Protective Index of a given S&T solution.

CYBER SECURITY FUTURES

A scientific and evidence-based process for establishing priorities for Science and Technology

Background to Public Sector Science & Technology (S&T) strategy

There are three pillars to the Federal Government's Cyber Security Strategy:

1. Securing Federal Government Systems;
2. Partnering to secure vital cyber systems outside the Federal Government; and
3. Helping Canadians be secure online.

It is understood that lead security agencies, public safety and the military shall continue to invest the bulk of efforts and resources in Pillar 1 - Securing Federal Government Systems as will tradition support centres within defence research. Federal Government funding to date has been spent on Pillar 1 activities.

The Public Safety Technical Program (PSTP) and Centre for Security Science (CSS) has focused Research and Development resources to support Pillar 2 - Critical Infrastructure outside of the federal government and Pillar 3 - Combating Cyber Threats – Helping Canadians to be secure online.

Imperatives

Moreover, combating cyber threats and securing vital Cyber CI outside the federal government has been a stated objective of the federal government and public safety Canada for the past decade. The Speech from the Throne, Federal Government's Cyber Security Strategy, the CIP Strategy, the Canada first Defence strategy and the Federal Government's stated commitment to a national 'Clean Pipes' strategy all support the requirement.

Outcome

The desired outcome of the CSS program would be to measurably combat and reduce cyber threat activity in support of pillar 2 and 3. Initiatives should be identified, prioritized and focused on based upon: Imperative, Requirement, Obligation, and Need (Type A IRON). Solutions must deter, detect, defend or recover from illegal cyber activity It is important to have a single strong focal-point to achieve the desired impact

Implications

The implication of a scientific and evidence-based process for establishing priorities for Science and Technology is profound. The private sector, CI owner-operators, stakeholders, academia and a wider community of interest that reflects all of Canadians would be engaged in government -funded cyber security research.

Mission of CSS and PSTP

The proposed Cyber S&T focus area for CSS is Cyber CI and Cyber Crime Science.

To deter and combat Cyber facilitated Crime and Improper activity on cyber CI, CSS will directly support the development of leading-edge science and technology to strengthen businesses, CI owners and law enforcement agencies' and the judiciary's ability to combat cyber crime by developing and providing science and technology based cyber-forensic tools to investigate and aid in successful prevention, prosecution of cyber crimes, and enhance cyber deterrence as well as indirectly:

- Contribute to global cyber security and managing threats
- Sustain Canada's economic prosperity
- Protect Canada and Canadians in cyber space

A methodology with mandatory and rated/weighted criteria would be used to measure prospective research areas/projects that align with the CSS mission. These priorities would be justifiable based upon measurement and evidence.

Capability Deficiencies and Gap Analysis

The force/capability development gaps can be categorized into:

- Enhanced **Situational Awareness** (a national/global real-time threat-risk picture);
- **Common Operating Picture** that includes critical cyber infrastructure owners;
- Rapid transition from policy instruments to scientific and **evidence-based strategy**;
- Providing **Context** and relevancy of programs within a quantitative risk framework (threat-risk);
- Re-Focus on **national level objectives** that will serve all Canadian; and
- **Proactive Cyber Defence** including research into offensive CNO for peaceful purposes.

Specific gaps include:

- Measurable reduction of malicious traffic loads in Canada;
- Cyber security programs require *statistically relevant* positive effect to organizations;

- Means to prioritize or measure the real effectiveness of cyber security expenditures. Success most often measured on the ability of a department to spend budget on time and within mandate.
- Public sector financial support to Critical Infrastructures, Businesses or the Canadian Public initiatives;
- Common body of science in the field of Critical Infrastructure Protection, particularly cyber interdependencies;
- Perception of the risks and the evidence;
- Further capability deficiencies that have been highlighted include the ability to:
    - Measure assurance levels, state-of-readiness, program effectiveness and critical interdependencies;
    - Quantify losses;
    - Accurately forecast emerging threats and disruptive technologies;
    - Build a Protection measures index (PMI) for technology;
    - Adopt a national system engineering approach to Cyber Security;
    - Apply Complex systems theory and modeling;
    - Consider powerful emergent strategic effects (globalization, convergence, consumerization, commercialization, etc);
    - Establish Key Performance Indicators.

The 'federal government' Cyber Security Strategy and Critical Information Protection Strategies are public policy documents written to align with existing departmental mandates. A systematic examination of the threats and traceability to solutions is required. Industry and the citizenry will need to be consulted in public sector strategies. Similarly, prioritisation of Cyber security /CIP projects by the public sector will need to include the owner-operators of CI or cyberspace, academia and citizens in the process.

The cyber ecosystem is constantly rebalancing assurance levels based upon complex variables, such market forces, help desk calls, malicious traffic loads and disruptive technologies. The volumes and velocities of cyber threats are global. Risk, in the form of toxic assets, is commuted through interdependency, and there multi-dimension effects of which are very difficult to model. The solution sets are evolving more organically through a creative commons than through any hierarchical policy driven program from Nation States.

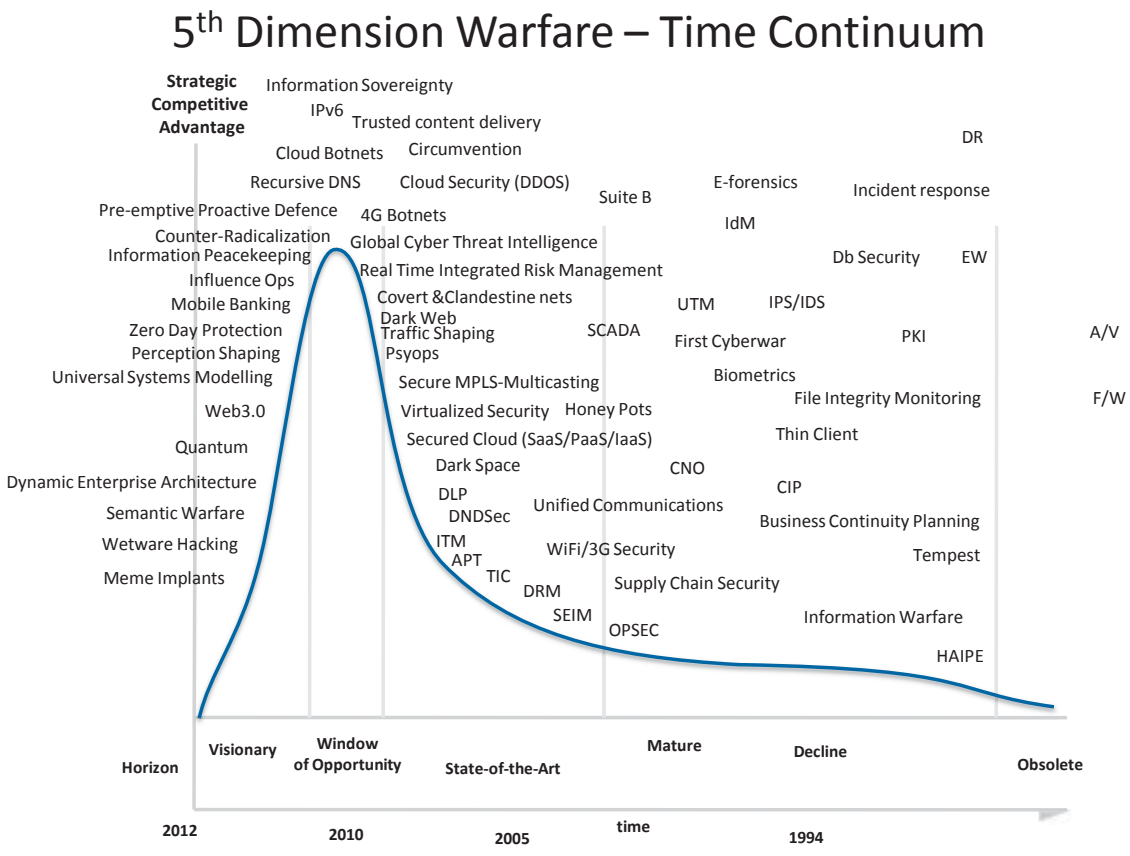
Transitionally, organizational cyber security initiatives have taken three flavours:

- Development of policy and security frameworks (MAF, MITS, Zachman Framework, Department of Defence Architecture Framework (DoDAF));
- Major crown projects focusing on esoteric security solutions (MLS, HAIPE);
- Commoditized Purchases of point solutions (firewalls, thin clients)

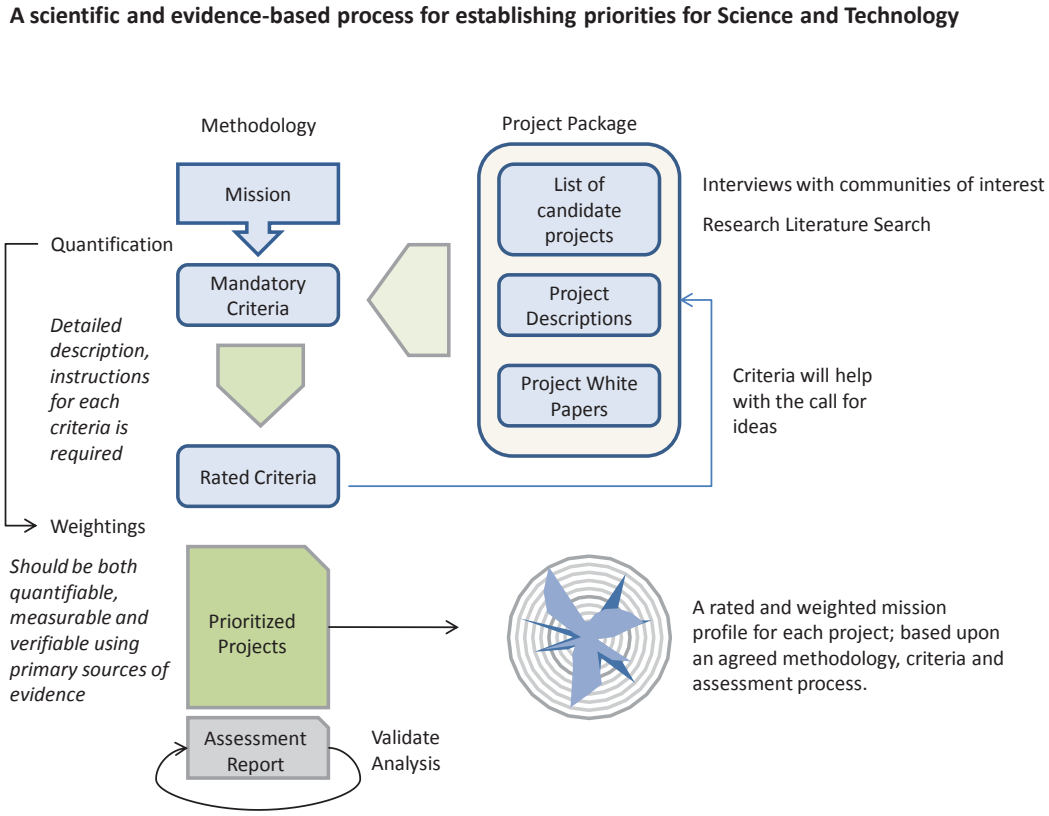
There is continuity gap from high-level generic frameworks to procurement. The most costly security programs are perhaps the least cost-effective at stopping the threat. R&D is required to bring programs back onto target.

Cyber priorities ought to then be established based upon inclusive scientific and evidence-based process. Projects need demonstrate real quantifiable value and traceability to the overall strategy and mission.

The following diagram places evolving cyber security on a time-line from over-the horizon science and technology to its obsolescence.



S&T Process

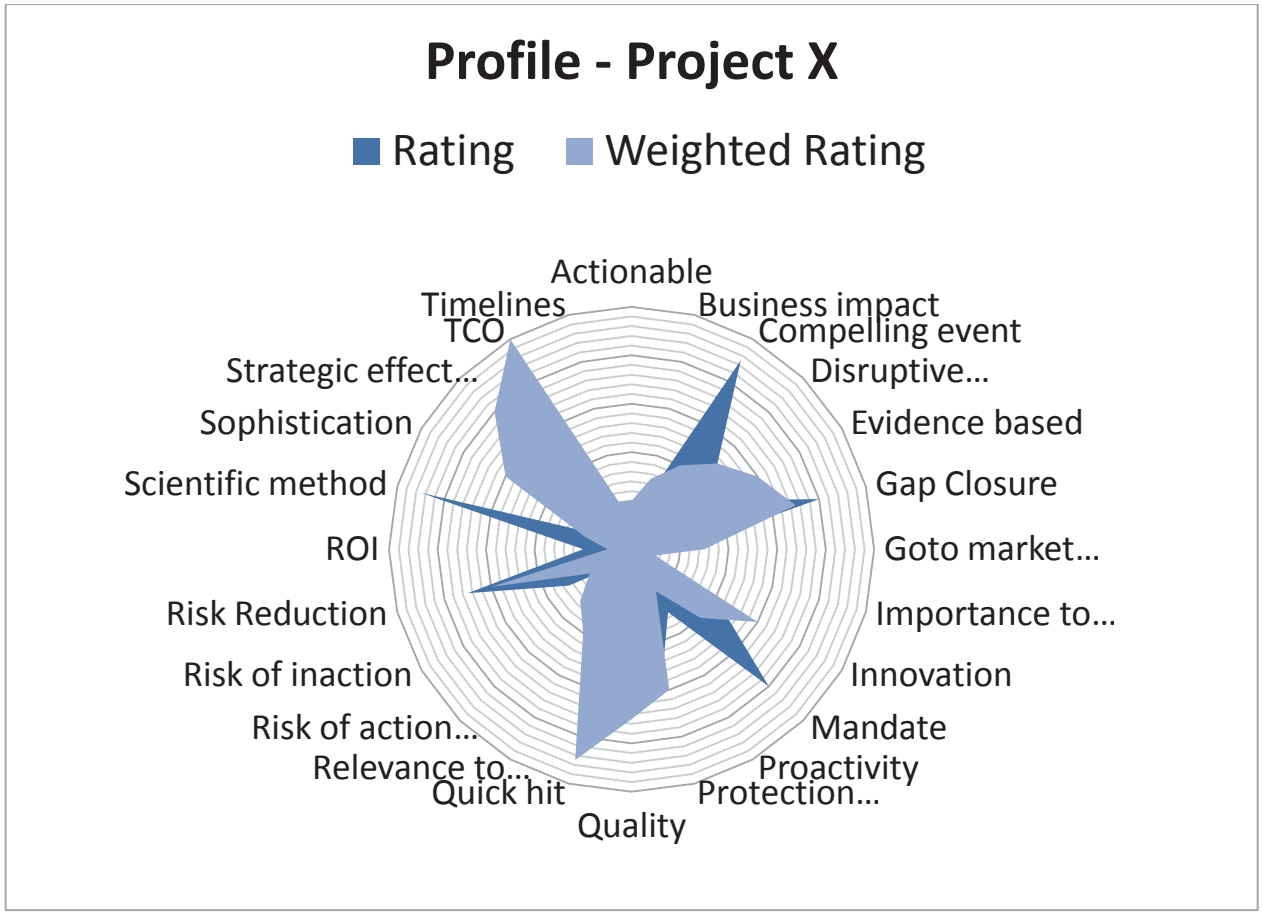


It is envisioned that the R&D process will follow the following logical steps:

1. Define and Clarify Mission Statement;
2. Quantify the mission in terms that can be measured
3. Further develop a methodology;
4. Derive mandatory and rated Criteria;
5. Determine weighting to that criteria;
6. Prepare a project briefing package that consists of: Lists, Project Descriptions and White Papers;
7. An assessment team to apply criteria to project list; and
8. Measure and Prioritize projects.

The process and analysis (assessment report) will need to be validated to eliminate bias. Projects may need to be re-assessed a number of times.

The result will be a rated and weighted mission profile for each project; based upon an agreed methodology, criteria and assessment process.



Criteria

Project must be assessed based upon a clear objective criteria that aligns with the singularly focused mission.

Mandatory Criteria

Mandatory criteria can act as a binary gate that eliminates projects from further consideration. Law and ethics are examples of a mandatory gate.

Rated Criteria

Rated requirements define the relative and absolute importance of the project as it relates to the mission. They represent desirable attributes and variable upon which a successful outcome can be measured. Rated requirements should be logically linked to the mission, be measureable (preferable in quantitative form both absolutely and relatively to other criteria), allow for discrimination and prioritization of projects. The rated criteria should also be weighted based upon Protection Index values because not all criteria will have the same impact. It is important to choose criteria well and educate assessors so they understand it. Example criteria may include:

- TCO
- ROI
- Protection measures index (PMI) absolute and relative
- Missions
- Strategic effect and levers
- Evidence based
- Imperative, Requirement, Obligation, Need (IRON)
- Scientific method
- Goto market strategy (productization)
- Importance to Canadians and business and CIs
- Disruptive Technology Impact
- Timelines (not to short, not too long)
- Proactivity
- Quick hits
- Innovation
- Quality
- Sophistication
- Compelling event
- Relevance to Industry and citizenry
- Business impact
- Actionable
- Gap Closure
- Risk Reduction
- Risk of inaction
- Risk of action (program)
- KPI
- Emphasis Pillar 2-3
- Measurable Threat reduction percentage
- Unique capability development
- Strategic (game changing)
- Certainty and confidence level
- Cost

- Corporate responsibility
- Cybercrime
- Counter-Espionage
- CIP
- Operational Security
- Degree to which it solves hard problems

Project Package

A project package may start off with just a list of topics. But in fairness to the assessment process, the assessors will need to be educated on the context of proposed work and its significance. It is desirable that detailed project descriptions and white papers accompany any list. Furthermore, criteria should be communicated to those submitting ideas so they can self-select topics and frame the descriptions for better assessment.

Models for Innovation

There are a number of successful innovative models, which may be of interest:

- In-Q-Tel (prospecting and incubating technologies of interest)
- Innocentive.com
- Red Cell - In response to the events of 11 September, the DCI tasked the DDI to create a "red cell" that would think unconventionally about the full range of relevant analytic issues. The DCI Red Cell takes a pronounced "out-of-the-box" approach and produces memos intended to provoke thought rather than to provide authoritative assessment.

Why Innovate

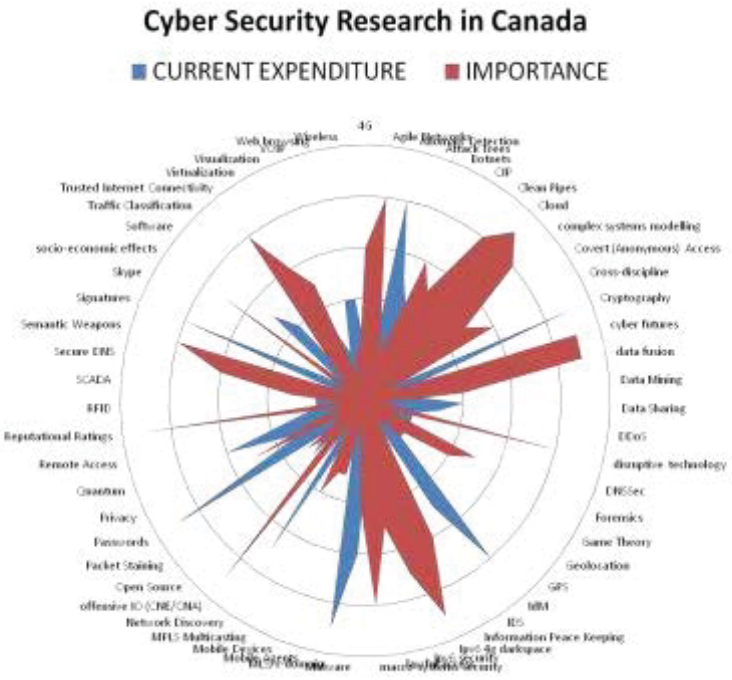
Innovation is the most cost effect and impactful means of shaping the global cyber threat environment. Too often S&T priorities are reactive, expensive and driven by traditional mandate, not disruptive technologies and emerging threats.

How do we measure success?

- Accuracy of prognostications (confidence levels)
- Volume and sophistication of attacks stopped

Examination of current state of Cyber Security Research in Canada

The following chart represents a cursory analysis of cyber security research conducted in Canada over the past five years. We examined 400 research projects from Universities, Government centres and Industry. Data was acquired by literature searches of published work, interviews with research leads, tracing funding and contracts. The Bell team also had unique insight to into the product development plans of all the major industry leaders as partners under NDA. Bell university labs funded over $2.5 Billion in external ICT research in the last five years, and we were able to access all external and security related programs. Bell Canada is buys and sells more cyber security products and services in Canada than all others including governments. Details of cyber security research were available from sales metrics. We examined tens of thousands of cyber security projects and extracted those that we would categorize as research.



Several hundred cyber security research projects were reduced into 38 research themes based upon common titles not any logical ontology. We then scored each themes for current expenditure and importance.

Current expenditure rating was derived from the number of research projects on that topic, the overall budgets and resources that appear to be allocated.

The importance rating is based upon a protection index derived from the ability of the method/technology being researched to effectively reduce advanced cyber threats. The

protection index is created by empirical measurement on the a large scale network infrastructure.

Observations:

Nearly all cyber security research in Canada is conducted out of a hand full of Universities. And although, all together brilliant, the work would greatly benefit from much closer ties to industry programs and government funding.

The lion's share of the public sector cyber security research funding has gone to esoteric multi-level/cross-domain and cryptography themes. Whereas commercial grade cryptographic solutions are pervasive and offer the same work factor as high-assurance programs, MLS has a very low protection index and utility in today's networks give today's threats.

Nearly all the research is defensive, and lacks the insight necessarily gained by offensive knowledge.

Research would benefit from operating on real World systems with real data sets. There appeared to be very little evidence based research. Most quantitative (experimental) was created in the lab. This can lead to solutions and conclusions that are erroneous, unscalable or impractical. Size matters, and labs often do not scale to address emergent macro effects or model a complex systems, as is cyberspace.

A high percentage of research is being conducted in areas, which yield very low ROI or protection indexes when applied to real-World systems. There are the number of 'research' projects that are being pursued when a COTS product already exists or the problem has already been solved. Our immediate observation is that academia, the public sector and industry appear to conduct research and development in their own communities of interest. We see immense synergies and economies of scale with much closer interaction and joint programs.

Communities of interest need to expand to welcome multi-discipline scientific researchers from engineers, sociologists, neurologists, and evolutionary biologists, etc. Cyber security research is not just the domain of technologists. Ironically, a lot of the research is preoccupied dealing with a better solution to yesterday's problems. We need more research (cyber security futures) which address tomorrows threats, disruptive technologies and evolution cyber security and insecurity.

POTENTIAL CYBER SECURITY RESEARCH TOPICS - NARRATIVE

Evaluation of targeted cyber-threats against the organization – The study would require examining log files from sample networks and correlating the findings with upstream global cyber-threat intelligence data to *empirically* measure malicious cyber activity directed at or originating from compromised machines within the organization. *The work could also be limited to a non-invasive external investigation or to the design and architecture of such a system.*

Provide a national-level operational perspective of Cyber Crime in Canada – including a synopsis of the level, and sophistication of cyber threat activity occurring in Canada over the last year, supported by ongoing investigative evidence and quantitative research.

Development of a cyber investigation capability for the Cyber Crime Fusion Centre – consisting of the design and demonstration of an advanced investigative capability consisting of collection management systems, safe trusted Internet connectivity, automated (robot/agent) collection and analytics. The design would introduce an extensible enterprise targeting and analytical intelligence platform that can be used at the strategic, tactical operational levels within Law Enforcement Communities. The proposed system would enables the organization to store, search and share knowledge and information gained in the field and conduct investigations with greater speed and fewer resources. The system can handle structured, semi-structured, and unstructured data from multiple disparate data repositories and sources all at once. Functionality would also include the integration of any data (structured, unstructured, and semi-structured) into a single environment without requiring "one database to rule them all"; relational, temporal, geospatial, statistical, behavioural, predictive, and network analysis to turn raw data into actionable intelligence; a revisioning Database to see how data has changed, how it varies by classification, and how reliable a source has been historically; and the ability to share intelligence securely across teams, agencies, and borders, with fine-grained access control and multi-level security.

Proactive Cyber Defence – Examine the implications and application of proactive cyber defence strategies. This includes pre-emptive proactive and preventative measures, , interdiction and disruption of threat networks whether they are domestic or foreign. The study will outline the required technology and tradecraft and well as the return on investment.

Emerging trends and disruptive technology – What imminent science and technology that will by its very nature disruptive to law-enforcement? How will it adversely affect the organizations ability to fight cybercrime? What are the potential solutions?

How to find cyber criminals in Canada – It is recognized that prosecuting cyber-criminals is difficult owing to anonymity, attribution and jurisdiction. The study will look at ways and means of identifying and targeting Canadian hosted cyber-crime.

Global threat intelligence and information sharing – evaluation of the availability, providence, and reliability of current sources of cyber threat intelligence and the veracity of the data potentially available to the organization. The study will also design the mechanism whereby the multifarious cyber intelligence sources can be acquired and managed including data fusion, correlation, analysis and dissemination.

Reference architecture model for high performance secure networking © **-** The organization's enterprise network is the cyber-investigators most powerful tool. It supports operations with ICT, it is the means by which threat/attack metrics can be gathered and ultimately identify criminals, it is also a weapon to takedown criminal enterprises.

The art-of-the-possible in cyber security – what science and technology is just over the horizon or already deployed that can be used to enhance cyber-security. The study will identify out-of-the-box reapplications (dual-use).

Convergence, Consumerization, globalization, and virtualization - represent powerful forces having sweeping effects across the business of security, intelligence, law enforcement and defence. The community is at the cusp of radical changes involving: the emergence of disruptive technologies, dual-use opportunities, and the commercialization and criminalization of information operations. There is also a confluence of technological convergence and social networking of post 9/11 threat groups.

WEB3.0 Security - The next generation of the Internet, or Web 3.0., is envisioned to provide a 3D interface combining virtual reality elements with a persistent virtual world. If such a version of Web 3.0 is realized, it is likely that the current barrier between online gaming and the rest of the Internet will disappear, allowing gamers to access all Internet applications through a game-like console. This could revolutionize the way people will experience the Internet and would likely transform activities such as research into more interactive experiences. The work could perform accurate technological forecasting of Web3.0 and assess the potential security concerns, emerging threat activity and exploitation.

Advanced Risk Methodology - Modern quantum physics can make predictions equivalent in accuracy to measuring North America to within a width of a hair. However a current risk methodology assessment of the security of a single PC is still just an educated guess. We propose to create a risk methodology for critical infrastructures based upon: a solid and incontrovertible theoretical foundation, notably the synthesis of Critical Infrastructure Protection (CIP) and sophisticated risk analytics with the Universal Systems Theory that most correctly addresses the chaotic behaviour of complex dynamic and open systems like Cyberspace. The pragmatics of real infrastructures is that they are influenced by advanced research in contagion-borne interdependences, technological and threat convergence,

globalization, risk conductance, and critical node analysis. A new methodology would be validated by qualitative statistical findings from thorough consultation with CI owners, and comprehensive quantitative (empirical) metrics from synaptic and semantic coverage of the cyber infrastructure. The outcome is to design an adaptive model of high-fidelity and capable of predictive accuracy. What is proposed represents an essential departure from relying on doctrine and security policy as the common means of managing risk - from faith to fact.

Business Case

The study to this point has presented a real security problem, defined an effective solution and a drawn a future roadmap. So this chapter, argues the case for security on the basis of cost recovery, fraud and integrated risk management framework and as an enabler to new business.

TOTAL COST OF OWNERSHIP

The majority of money spent on Information Communications Technology Security in Canada today is not effective because it fails to: establish key performance indicators (KPI) that permit information officers to measure the true Return on Investment (ROI) for security dollars spent, nor does it appreciate the Total Cost of Ownership (TCO) for the organization. Organizations typically buy the cheapest, dirty bandwidth, and either accept or ignore the risks and impacts that are borne deeper with the organization. This is measurable by a high rate of detected compromises within these organizations, and inbound/outbound malicious traffic loads. For this reason, provisioning of foundational corporate network services should not be treated as a commodity. Bandwidth should be assessed by cost per clean megabyte. Furthermore, risk management should be begin proactively upstream and not based upon a reactive strategy of incident response and disaster recovery once the threat has penetrated your infostructure.

Prologue

A $700 car sounds like a bargain on the surface, but you just know that there will be hidden costs under the hood and down the road.

Ask yourself, what things in life you buy based solely on lowest price? Even buying the cheapest toilet paper has its consequences. If the quality of gasoline was not regulated, you would think twice at the pumps, or you may find yourself filling the tank of that $700 car with gasoline cut with water.

Yet, organizations often purchase the voice and data network services over which their entire business depends, from the cheapest sources without any security. The network is not a commodity. To treat it as such, has risk and consequences that are borne at the heart of your organization. We have seen a number of spectacular cases in the past year.

Bean counting analog

Imagine for a moment, that you own the only coffee shop in town. There is a line-up of customers before the doors open in the morning to closing time.

Seven out of ten employees are on coffee-break at any given time. One manager is on duty, leaving two staff to serve customers. The coffee machine breaks down 1.5 hours over a 7.5 work day and five-per cent of the coffee is spilled. One customer is burnt.

How much revenue is at risk? Choose one option.

a. None. The coffee shop is run by the municipality. How much coffee that is sold or lost is irrelevant so long as the budget is spent;
b. Risk is limited to direct losses and thus equal to the value of the spilt coffee; or
c. The total revenue at risk is at least: the cost of spilt coffee + the time/cost spent cleaning up the mess + cost to pay employees that are not working + lost of potential revenue not serving everyone in line by the end of the day + cost of managers salary not managing effectively, and of course the law suit from the scalded customer.

Network scenario

Now picture yourself as a CIO responsible for a busy network over which e-goods and services are delivered, and funds are transferred electronically.

You have an IT security staff and budget yet, seventy-percent of the Internet connection is filled with illicit and malicious traffic. The average data network availability is 80%. Five to twelve percent of your computing base is compromised at any given time.

How much revenue is at risk? Pick one:

a) None. This is a public service and P&L is not relevant;
b) Risk is limited to direct costs associated with disaster recovery and external contracting support incident handling; or
c) The total revenue at risk is at least: 70% of your total network costs (bandwidth and infrastructure) that are consumed transporting malicious/illicit traffic + 20% of your operational costs owing to downtime + lost revenue (24% of potential) + cost to clean repair and recover 5% of computers + value of data lost + legal risk + brand risks.

National Scenario

The aforementioned calculations scale equally well to a national level. The concepts have been a matter of open publication.[97] The transactional value of goods and services in

[97] The Economic Impact of Cyber-Attacks, Report to Congress, 01 April 2004

Canada is known and reported with a good deal of statistical accurately by official bodies such as Statistics Canada, and trade organizations. Similarly, electronic funds transferred over networks, is measured precisely by the financial sector. Meanwhile, the telecommunications sector has clear visibility into the flow of e-commerce and network performance.

Therefore, the effects of network degradation owing to (cyber) threat pressure and financial impact is measurable, in real-time, should one choose to look. E-commerce that is impeded by poor network performance (throughput, availability) must be regarded as a loss, at the close of business day, as is the cost of wasted bandwidth (malicious) based upon tariff rates. Business operations (salaries, revenue) are duly affected. The percentage of infected (compromised) computers in Canada has been measured at 5%. The security industry (Microsoft, McAfee et.al) quoted as high as 12% of Computers globally are compromised. Either the cost to repair and rebuild an infected machine can be estimated or standard actuarial numbers can be applied. The amount of money that is spend on network security in Canada every year is also a well published figure, and must be applied as a sunk cost towards to total cost of ownership. The sub-total of revenue-at-risk at this point is already rather alarming. Other metrics that top-up the total losses are: the value of the information lost/compromised, piracy/copyright/IP, identity theft, card fraud, toll fraud, liability, brand and reputational risk.

Using this calculus, the total revenue at risk for Canada owing to cyber threats is estimated at $100B per year[98]. Most of this figure is attributable to lost potential revues. The cost of telecommunications fraud last year was $200B in North America[99]. For toll fraud the subscription ID theft and voice PBX hacking top the list of incidents. Both voice and data networks are affected. The magnitude of the risk is consistent with corporate e-fraud statistics, measurements of the black market economy, USA and global statistics. Some folks react to the $100B figure with irrational disbelief; without compelling evidence to the contrary or doing the math. Organizations should self-assessment, using the same logic to calculate TOC within their own organization.

Public Sector

The formula works equally well for public institutions. The total amount on tax collection and expenditures are network-sensitive, as is the productivity of the workday. The total operating expenditures, goods and services, security budgets and telecommunications costs are known. However, the value of the information, liability, brand and reputational risk are not. One can also argue that public institutions do not have reputational risk

[98] Proactive Cyber Defence, Before Day Zero and the Perfect Storm, White Paper, Bell Canada, published 01.02.2008

[99] Source: Communications Fraud Control Association 2009 survey

because services are mostly mandatory or non-discretionary to the taxpayer. The total revenue at risk owning to cyber threats across the public sector has been through the same estimate.

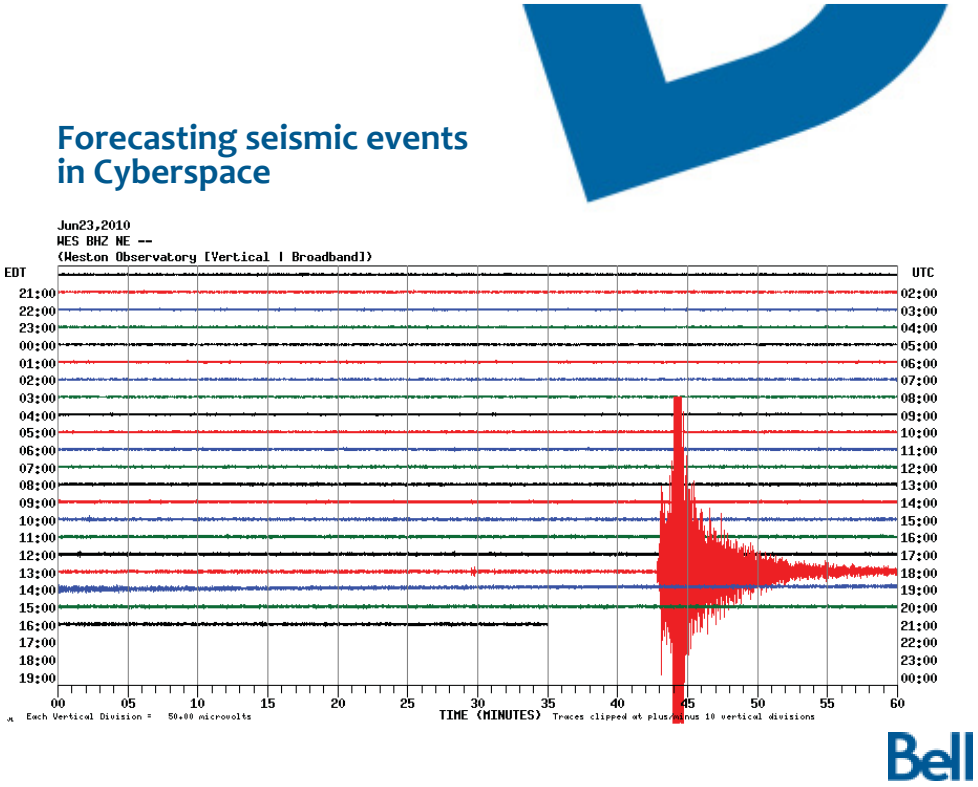
General Network Risk

Too often, people limit their network security to an inward view from a notional organizational perimeter. This model confines an organization's situational awareness to within their *perceived* sphere-of-control whist ignoring most layers of the OSI network model from a security perspective. The irony is that these days the organization perimeter has disintegrated. All systems are open to the Internet and vulnerable to it.

The Internet is a vastly complex non-determinist system like quantum mechanics, biological ecosystems or global weather patterns. Yet, most organizations manage interconnectivity risks with most basic of security constructs like public policy.[100] Organizations place their WAN over the Internet in an indiscriminate fashion without understanding the risks or total cost to their organization. This is comparable to using the Farmer's Almanac to predict severe weather events, or building a high-rise in an earth-quake zone. A secure foundation[101] is important.

[100] Managing Risk within Complex Systems, Bell Canada, 2010

[101] High performance secure networking Foundational Concepts, Whitepaper, Bell Canada 2010



Organizations do not fully appreciate the security significance of critical interdependencies[102] that extend into their organization for which they have little control: physical cable plant, provisioning of network telecommunications services, Internet routing, domain name registration, network time, or the global supply chain. A nuclear power station an meltdown owing to a Tsunami wipes out their backup generators.

Frequently, risks of these sorts are ignored because there is a belief that they cannot be managed. Therefore, foundational network services are treated as commodities, and, in a price-sensitive (lowest cost) market, security is stripped out. It is a race the bottom, at the same time the threat is paying top dollar for top talent.

"Proactive defence[103] is not incident response. That is what losers do after getting owned."

[102] Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies (Hardcover), CRC Press, ISBN-13: 978-1420068351, 2008, by Tyson Macaulay,

[103] Proactive Defence is interdicting and disrupting an attack pre-emptively before it reaches your defences.

Most of the malicious traffic on corporate networks today can be attributed to failing to manage critical interdependencies.[104] This is a new way of seeing risk for IT traditionalists, but standard practice in the global banking community when they talk about risk-contagion and toxic content (assets). Building an information infrastructure on untrustworthy computing and telecommunications foundation[105] is the fundamental reason why many networks are lost. Classified networks[106], banking, control systems are particularly sensitive.

Security studies[107] have clearly shown that the magnitude and velocity of risk conductance is a function of interdependency, external assurance levels and very little to do with safeguards. Government reports[108] have come to similar conclusions.

What you do proactively within your sphere-of-influence and see from beyond your network perimeter (sphere-of-interest), buys your organization time and precision in overall reducing risk. In a military context we would call this 'force projection.' Manoeuvre warfare is the only viable tactic information battle-space.

In the cyber world, organizations have their heads down in trenches, and are easily overrun by the enemy during the night.

If you sent a million-dollar cashier cheque through regular air mail to an overseas office marked valuable and confidential, would you be surprised if the envelop arrived empty or late? Yet many organizations conduct business online using untrusted connectivity. They connect to the Internet not knowing or influencing how their packets travel to their destination. Canada has some of the worst ISPs on the planet[109] – have you done due diligence? Security metrics show that large providers are orders of magnitude cleaner than average Internet values, in the consumer space. This figure is even better for bandwidth that these carriers provide to enterprise space, because more stringent security policies can be enforced in the cloud and managed by SLAs. This is within your sphere of influence.

[104] Assessing the Risks of our Interdependent Critical Infrastructures, Front Line Security Magazine, July 2008

[105] HostExploit – CyberCrime Series, Top 50 Bad Hosts and Networks, December 2009

[106] Laying siege to Traditional Fortress Network Architectures, Hacking HAIPE, White Paper February 2008

[107] Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies (Hardcover), CRC Press, ISBN-13: 978-1420068351, 2008

[108] Cyber Critical Infrastructure Interdependencies and State of Readiness Studies, Cyber Security Secretariat, PSEPC, issued 2006-04-28

[109] HostExploit – CyberCrime Series, Top 50 Bad Hosts and Networks, December 2009

Domain name resolution is the map and compass of the Internet. It is a pivotal control plain of network communications. Yet, few organizations give any thought to DNS security and verified delivery through trusted routing. If an enemy controls DNS they own your network.

The cavalier use of uncertified networks, unvetted/approved providers, unknown routing and core services like domain name registration has been identified by the US government[110] and to the Canadian government[111] as a pressing matter within a national cyber security strategy.

Comprehensive National Cyber security Initiative

The US Comprehensive National Cyber security Initiative (CNCI) has a number of components:

- Trusted internet connectivity (TIC) the Secure Channel and MTIPS (Managed Trusted Internet Protocol Service) and TICAP (Trusted Internet Connection Access Provider);
- DNS, DDoS, Clean Pipes;
- Einstein III (central monitoring and cleaning);
- Intrusion detection -Intrusion prevention;
- Research and development;
- Situational awareness;
- Cyber counter intelligence;
- Classified network security;
- Cyber education and training;
- Implementation of information security technologies;
- Deterrence strategies;
- Global supply chain security; and
- Public/private collaboration.

Trusted Internet Connectivity (TIC)

Every organization must have a control of all Internet access points through a trustworthy provider. Traffic passing through a reduced set of official access points can be monitored and cleaned more efficiently and far more cost effectively than delivering dirty traffic all the way into the enterprise. Bandwidth ought be purchased based upon cost/clean megabyte and the telecommunications circuits should be certified and accredited. The US has allocated $40B towards their Comprehensive National Cybersecurity Initiative (CNCI). Trusted internet connectivity (TIC) using MTIPS (Managed Trusted Internet Protocol Service) and TICAP (Trusted Internet Connection Access Providers) is the cornerstone of the

[110] US Comprehensive Cyber Security Initiative
[111] Information Technology Association of Canada (ITAC) submission to PSC on the draft national cyber security strategy

CNCI. There are clear parallels with Canadian Secure Channel, Perimeter security, SEIM, and upstream security programs. The vector for most successful botnet attacks has been shown to follow untrusted or rogue connections and paths of critical interdependencies. Purchasing untrusted bandwidth at for the sake of lowest cost per mbyte, but filled with malicious traffic is dangerous and far more expensive to an organization than purchasing clean pipes. For this reason security should be part of a network contracts.

"Upstream security is more important than a firewall."

Letting the cloud handle security by Edward Amoroso, Senior Vice President and Chief Security Officer AT&T:

"The vast number of users with broadband access, have little or no security. That's how thousands of unsecured PCs are commandeered to send spam e-mail and distribute malware. It is the No. 1 problem on the Internet in my estimation. The potential danger of a volume-based DDoS attacks is still high. Maybe 95 out of 100 (enterprises) probably don't have sufficient protection (against DoS attacks). Gigabit Ethernet connections among data centres, virtual private networks and the like are still vulnerable against an attacker who can round up – by organizing or compromising – enough machines to bombard the network. If you get enough traffic at that gateway -- and it's not that much traffic, it's easy to overwhelm the gateway. The individual enterprise approach of hanging a technological defence onto a connection won't stand up to a 3Gbps attack. Carrier companies got into just pushing light – focusing on packet loss and latency -- and letting the intelligent edge worry about everything else. But attacks pass through the carrier infrastructure and that's where the focus should be. Security is one of those things that's best attended to in a centralized area. But selling upstream security to enterprise, which has an ownership attitude toward security regimes, gets pushback. Not a little bit of pushback, a lot of pushback. This message is a very bitter pill to swallow. But if an enterprises want to try to stop denial of service attacks without working with their carriers, he challenges them to explain how they'll do it. How do you keep children off inappropriate Web sites, when you can't be there all the time and they're often more technologically sophisticated than you. In partnership with the carrier at the DSLAM or the headend, and that applies to the enterprise connection, too. Firewalls and intrusion detection systems are evolving to do tasks they weren't conceived for in the first place. A typical enterprise might have 100 gateways to untrusted connections. Originally, a firewall was designed to act as a choke point for a single connection. A firewall is no longer a firewall, I don't know what it is."

CNCI, TIC, and Networx Background

After numerous cyber attacks on several federal agency computer systems in the time period following 9/11, The White House determined that the government needed a more comprehensive strategy to defend government networks and sensitive information from hackers and nation states. On January 8, 2008, President Bush launched the Comprehensive

National Cybersecurity Initiative (CNCI), by issuing National Security Presidential Directive 54.

The CNCI is the most thorough and far-reaching effort which the government has ever undertaken to improve the management and security of its IT infrastructure. As one of the 12 components of the CNCI, the Trusted Internet Connection (TIC) initiative was formalized in November 2007 with the goal of decreasing the number of connections that agencies had to external computer networks to 100 or less. Officials believe that the fewer connections agencies have to the Internet, the easier it will be for them to monitor and detect security incidents.

Under the TIC initiative, EVERY agency must either work with an approved MTIPS (Managed Trusted Internet Protocol Service) provider (AT&T, Sprint, Verizon, Qwest have been approved by GSA thus far) or be approved by The Department of Homeland Security to provide their own consolidated service by passing 51 requirements known as a TICAP (Trusted Internet Connection Access Provider). Currently, there are 96 agencies 'seeking service' through MTIPS providers and 20 agencies who have registered to become TICAPs.

The program contract vehicle for government agencies to pursue the TIC initiative is called Networx. Networx is the largest telecommunications program in the history of the federal government. It is the replacement for the previous contract vehicle known as FTS2001. It is divided into Networx Universal, with a ceiling of $48.1 billion, and Networx Enterprise, with a $20 billion cap. Both contracts are indefinite-delivery indefinite-quantity (IDIQ) with four-year base periods and two three-year options.

The Consolidation Imperative

Based upon current tariffs in Canada, having ten 10mb connections to the Internet is four times more expensive than one 100mb connection.

The most fundamental aspect of the TIC initiative is consolidation. Driven by space, power, budget, security, and other constraints, consolidation has become both a tactical and strategic imperative for government. Most of the buzz about consolidation concentrates on its application to the data centers. But this focus overlooks an area where consolidation offers even more dramatic advantages: network security.

Consolidating network security also delivers notable cost benefits, another primary goal of the Networx program vehicle. According to Gartner, in 2008, the most important way information security organizations could save money would be to leverage the convergence of established security functions into network security to protect against an evolving multitude of network and content threats.

Conclusion

Analysis based upon quantitative measurements of malicious traffic, network performance and residual risks has demonstrated that the Total Cost of Ownership (TOC) of Internet and voice circuits purchased form certified infrastructures, like Secure Channel or the US TIC model under CNCI, is substantial lower, by several orders of magnitude, than untrusted internet connections. Since telecoms-procurement offices in large enterprises are incented to buy the cheapest bandwidth (without security), the ultimate cost is borne by the operational business units within the enterprise who are flooded with attacks, most of which are undetectable by traditional means.

Organizations should calculate the 'cost per clean megabyte per month' and assess the real return on investment (ROI) for security based upon 'the amount of malicious traffic stopped for every security dollar spent'.

There are ample case studies, which demonstrate that failure to engage the threat at a distance places substantial risks and costs at your doorstep. Many voice and data networks are on the brink.

THE BUSINESS CASE FOR AN ENTERPRISE CLEAN PIPES STRATEGY

CRITICAL FINDINGS

'Clean pipes' was coined a decade ago to describe carrier-level initiatives to filter 'toxic' content from Internet. The process consists of detecting malicious traffic in the carrier cloud (upstream), fusing the threat data with global sources, and using advanced analytics to produce and disseminate cyber threat intelligence as a value-added service to businesses, and for real-time mitigation within the cloud as upstream security services. The prime business drivers for 'clean pipes' are direct losses, brand risk, and creating new value-added revenue streams to otherwise rapidly commoditizing connectivity services.

There is incontrovertible documented evidence of a clear aggressive and sophisticated threat, widespread attacks and measurable losses. The business case for 'clean pipes' is substantiated by a compelling a body-of-evidence built over 2 years. Malicious traffic is costing Canadian's billions. There are also intangible risks associated with: brand reputation, litigation, privacy, customer experience, law-enforcement, regulation, standards, compliance, audit, SLAs and maturing customer expectations. The investment to clean the enterprise network of malicious traffic is a fraction of the cost of the current rate-of-loss.

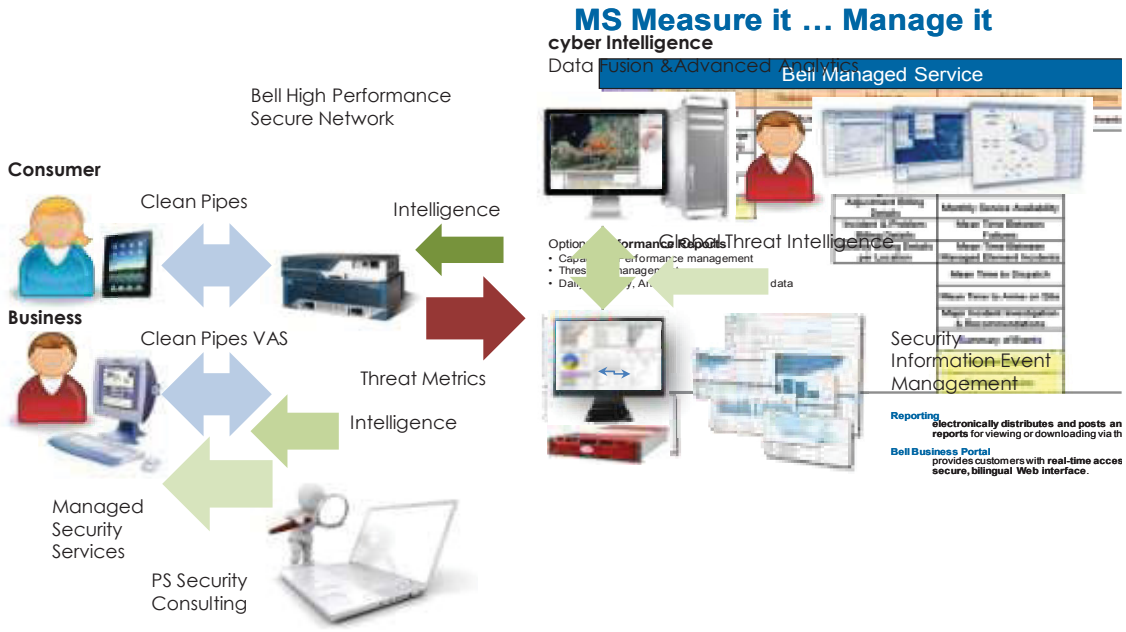
The clean pipe solution has been well understood and a low-risk migration plan could be fully implemented in months. A Clean Pipes program would involve: access to a spectrum of data sources; integrating these sources, applying central data fusion technology, and resourcing with advanced analytics capability. Real-time Security and business intelligence services could then be provided for C-level evidence based decision making.

DEFINITION

Clean Pipes generally consists of a number of necessary steps including: the Collection consolidation and collation of data sources, and the production of Business and Network Intelligence using advanced analytics and data fusion that can be used to mitigate business and network threats in the core while at the same time providing for intelligence-led business operations.

"Security is the heart of internetworking's future." - **Service Provider Solutions DDoS Protection Solution Enabling "Clean Pipes" Capabilities**, June CISCO 2005

'Clean pipes' are meant to filter 'toxic' content from the Internet before delivering it to clients.



The process consists of detecting malicious traffic in the carrier cloud, fusing the threat data with global sources, and using advanced analytics to produce and disseminate cyber threat intelligence as a value added service to businesses and for mitigation within the cloud as upstream security services. The industry calls this Security Intelligence Services (SIS) and is a multi-Billion dollar business. [Yankee Group]

"Network security is a reactive process of identifying policies, procedures, vulnerabilities, and threats, then designing and implementing systems and continuously managing them to ensure a secure operating environment. This process is iterative and takes hours or days, frequently months, to implement. The emergence of security intelligence service (SIS) providers is flipping this paradigm on its head by claiming to make adaptive network security management a proactive process, allowing users to get out in front of the hackers trying to infiltrate IT systems." - **Security Intelligence Services: The Competitive Landscape Security Solutions & Services**, REPORT Vol. 2, No. 1—January 2002 *the Yankee Group*

The allegory for the clean Internet pipes business case already exists. The city treats and monitors the water supply for much the same reasons including: public expectations, legal obligations, downstream health repercussions, and revenue generating opportunities. For more discerning clients there is always a market for bottled water. Canadians take clean tap water for granted and then bought over $500 million in bottled water last year, even though they had perfectly good potable tap water. The case is in cyberspace, Canadian's are drinking partially filtered water.

Clean pipes does NOT inhibit security services it empowers it.

The prime business, drivers for 'clean pipes' are mitigating direct losses/brand risk, and creating new and robust opportunities/services.

Cleaning Internet Pipes is a complex mix of technical and non-technical variables. An in-depth discussion of implementing a national cyber security strategy in the context of universal complex systems theory is provided in the reference research literature herein.

MAIN MESSAGE –SUMMARY

The threat, risks and opportunities

EVIDENCE OF THREAT RISK

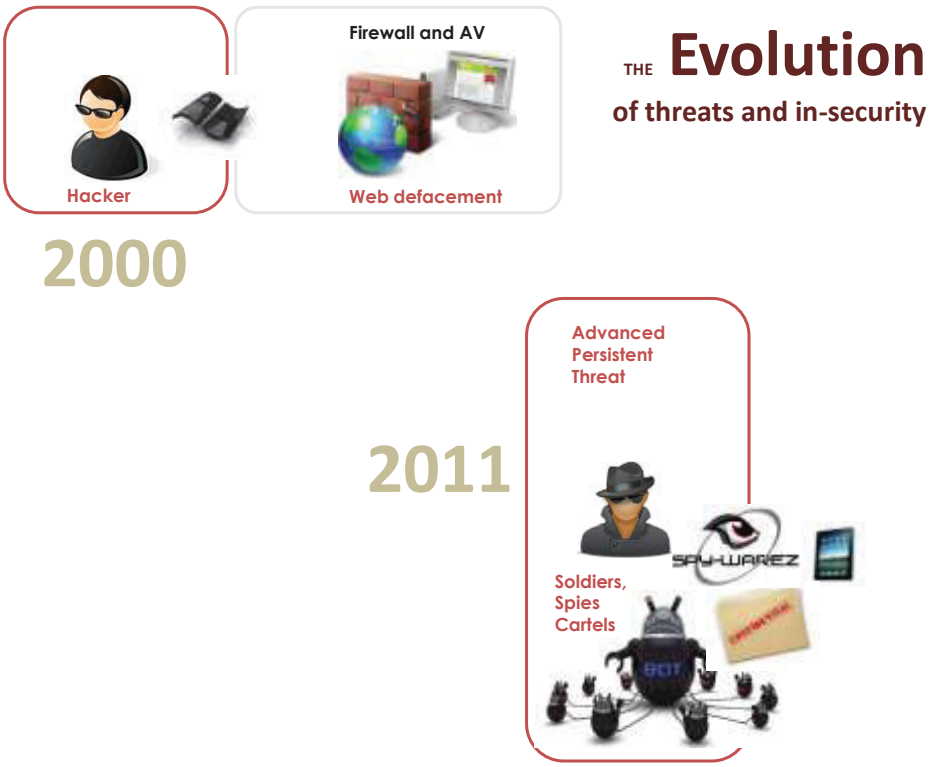
There is incontrovertible documented evidence of a clear aggressive and sophisticated threat, widespread attacks and measurable losses affecting all critical sectors[112] and organizations including Fortune 100 companies, financial institutions, government and telecommunications carriers, and the necessity for clean pipes.

"an overwhelming quantity of empirical evidence from network sensors that would suggest a high degree of penetration, compromise and loss in all the organizations we investigated. None had the necessary multi-source data-fusion systems, cyber-intelligence analysis capabilities to either process or share data, nor the autonomous command and control security infrastructure to mitigate risks beyond current levels

The business case for 'clean pipes' is substantiated by a compelling body-of-evidence built over 2 years of research.[113] Historical evidence dating back to 2005, Comprehensive threat intelligence assessment, Investigation finding which uncovering systemic cyber breaches and compromises; a complete engineering solution for clean pipes; and a future vision of cyber security, and the business thereof. The studies were subject to full academic peer review.

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

[113] Bell Canada led a team consisted of resources and sponsorship from the Centre for Security Science, Research Establishment, Communications Security Establishment of Canada (CSEC), Royal Canadian Mounted Police (RCMP), Department of National Defence (DND), Canada Revenue Agency (CRA), and Industry Canada (IC). We had major contributions from top researchers from The Munk Centre, SecDev Group and the Canada Center for Global Security, The Citizen Lab, University of Toronto, Concordia, the RAND Corporation with consultation with Berkman Center for Internet and Society at Harvard Law School and the Advanced Network Research Group at Cambridge University, together with the engineering teams from Bell's industry partners McAfee, Cisco, Arcsight, Niksun,.



Cyber threats have evolved from hackers, script kiddies and web defacements to expansive crime cartels operating sophisticated robot network in tandem with hostile foreign intelligence services (HoIS).

Investigative analysis would indicate that 5-12 % of consumer space is compromised and have been turned into zombie machines, controlled, for the most part, by off-shore organized crime syndicates. These figures are consistent with those released by the security industry.

"We found accelerating threats and vulnerabilities. For the second year in a row, IT executives in the critical infrastructure sector told us that they perceive a real and growing cyberthreat. Extortion attempts were also more frequent in the CIP sectors. And 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.

Extortion is "*becoming more commonplace*," says Dr. Ed Amoroso, chief information security officer at AT&T. "*It's happening enough that it doesn't even raise an eyebrow anymore. If you don't enable upstream security services, then you are negligent.*"

"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**, June CISCO 2005

Research has exposed and verified compromise and direct losses (consumption of network resources) to enterprises owing to deliberate cyber-threats from targeted state-sponsored espionage, organized crime and telecoms fraud. Subsequent investigations[114] saw infiltration of organized crime elements, executive spear phishing, piracy, supply-chain shaping, autonomous robot spy networks and terrorist activity. Espionage and organized crime are by far the most damaging, where as piracy and spam consume the most bandwidth.

"Foreign governments preparing sophisticated exploits like Stuxnet, cyberattackers have targeted critical infrastructure." - **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.

During the course of the investigation, pervasive attacks on the Olympics were monitored, public and private Sectors sustained heavy damage from foreign based cyber attacks, attributed to Chinese controlled servers.

"The Government's role is still unclear. How are governments responding to the vulnerability of their core civilian infrastructures? In general, they continue to play an ambiguous role in cybersecurity. Globally, industries fear attacks by governments, and more than half of respondents say that they have already suffered from government attacks. Governments also play another, more notorious role in cybersecurity. One of the more startling results of our research is the discovery of the constant probing and assault. Our survey data lend support to anecdotal reporting that militaries in several countries have done reconnaissance and planning for cyberattacks, mapping the underlying network infrastructure and locating vulnerabilities for future attack. Their intelligence and military arms infiltrate and prepare to attack the networks of other countries. During the interviews conducted for this report, the cyberthreat that was cited most often was government-sponsored sabotage and espionage."- **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.

On any given day 98% of e-mail is malicious[115], 60% of all DNS activity is threat related and 30% of overall bandwidth is consumed by illicit activity.

"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

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

security intelligence [clean pipes] are deployed to substantial benefit, recovering up to 30% of the core network bandwidth. Significant asset recovery was the reason Upstream Intelligence was developed and deployed in the first place, but this need only be the starting point of this capability." - **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 Defence (DoD) managed by the Defence Technical Information Center (DTIC), and Director, Defence Research and Engineering (DDR&E), Co-authors Tyson Macaulay (Bell Canada), Dave McMahon (Bell Canada) and Chris Mac-Stoker (Niksun Corporation).

The investigation accounted for over 200 Petabytes of malicious traffic[116] that passes through the network every a year, causing an estimated billions[117] in damage to the Canadian economy. There are varying opinions as the degree of culpability organizations have in delivering malware, and the responsibility to 'clean the pipes,' but several things are for certain:

- It costs money to route and manage bad traffic.
- Handling toxic content raised the exposure corporate networks to compromise/infection
- Risk is conducted through critical interdependencies and has multi-order cascading consequences that are hard to predict.[118]
- Permits serious damage downstream
- Decreases customer satisfaction and precipitates increase help desk calls at a measurable cost to the enterprise
- There is a growing perception that it is bad business and a corresponding movement to regulate, legislate, litigate and contractually compel government and business to improve the situation
- It can't be good for one's reputation

"The rapid technological change and the need to permit flexibility in implementing security measures militate against codifying requirements by regulation... legal or regulatory action is necessary to force ISPs to better protect their customers from Botnet attacks...ISPs could be

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

held liable for their role in hosting partly or entirely a Botnet attack….ISPs could have a proactive role by monitoring their end-users' computers and quarantine any infected machines before they cause any harm." - **Liability for Botnet attacks: using tort to improve cybersecurity**, Jennifer Chandler, Canadian Journal of Technology Law, March 2006

The total revenue-at-risk to any organization is much greater that the cost to clean the pipes.

And there are intangible risks to the brand.

"Legal driven standards of care such as COBIT, SOX, PIPEDA, GLB are also used to frame this review in context of professional practices such as ITIL, SEI-CMMI and other related ISO (project management and Information Security Management) bodies of knowledge that are considered certifiable best practices." - Dr. Robert Garigue, Vice President for Information Integrity and Chief Security Executive, Bell Canada , March 27, 2006

In brief, some of the less quantifiable, but very real, risks list: Compliance (SOX, PCI, PIPEDA), Laws, ethics, Human Rights, Workplace health and safety, Liability, Privacy, Corporate Responsibility, Brand Protection and goodwill, Regulation, Insurance, Credit Rating, Stock Performance after a breach, Peer Pressure, Market Confidence and baseline standards of due care as percentage of security investment.

"Jennifer Stoddart, Canada's privacy commissioner, just last week called for increased powers for her office to levy fines against companies that allow data security breaches." - Financial Times, 10 May 2011

"Twenty-five percent of critical infrastructure companies do not interact with the government on cybersecurity and network defence matters. Government can encourage security by collaborating with industry — and by adopting regulations that demand better security than the market does. China's government seems to play an aggressive role in demanding security from its critical infrastructure." - **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.

The lack of clean pipes drives organizations in unpredictable directions, and in so doing, increase risk owing to uncertainty.

Clean Pipes Investment Curve

Average consumers are not likely to pay for clean pipes. Something they expect anyway from their private or public sector provider. However, there are a number of strong drivers for cleaning Internet services further; not the least of which are cost/fraud reduction, network performance, brand reputation, regulatory/legislative compliance and corporate responsibility.

"*Better Bandwidth Utilization with Network-based Defence - By removing attack traffic within the IP backbone, the Internet Clean Pipe solution rapidly clears threats in the cloud before they hit the customer network. The solution also provides users with multiple bandwidth speeds and ensures optimal bandwidth usage. Proactive, Real-time Mitigation [are] built into a global IP backbone for full transparency to users once mitigation begins. The service scrutinizes network traffic in real-time to identify anomalies and quarantine attack packets. Only malicious traffic is blocked — legitimate traffic continues to flow through so network and applications remain available to users.*" - **Internet Clean Pipe - DDoS Protection Global Tier-1 network with built-in DDoS Detection and Mitigation services,** TATA Communications, Aug 2009

At a certain point, these drivers lose momentum to a cost-benefit balance and net-neutrality arguments. Businesses are willing to pay for cleaner pipes past this point. The business driver for business clients is ROI as measured by cost for clean megabyte. Costs begin to climb somewhere around 98% clean (TBD) and sophisticated tradecraft, tools and advanced analytic resources are required to get to 99%+ clean. This is a point, beyond which all practical security measures have been put in place and it makes no more sense to invest in security. Malicious activity is driven down to the cost of doing business.

"*Sophisticated Detection Capabilities - In addition to built-in attack profiles, the Dedicated Internet Access/DDoS Detection and Mitigation service uses statistical and behavioural analysis methods to identify attacks in progress, leveraging state-of-the-art Arbor Peakflow DDoS analysis technology*." - **Internet Clean Pipe - DDoS Protection Global Tier-1 network with built-in DDoS Detection and Mitigation services,** TATA Communications, Aug 2009

Organizations who have implemented clean pipe solutions have recorded a 10:1 ROI in cost savings (fraud reduction, resource recovery).

Cloud, Aurora, Mobility, Zeus, APT, Wikileaks, Stuxnet, Anonymous. If a word cloud were created using infosec headlines from 2010, these would certainly be rendered big and bold. It's an interesting juxtaposition of themes. While the Cloud and mobile devices increasingly allow us to do anything from anywhere with anyone at any time, Aurora, Zeus, Advanced Persistent Threats (APTs), Wikileaks, and Stuxnet remind us of the difficulty of protecting our information assets in a usability-driven World. Zeus sprouted up within our 2009 caseload, but came to full bloom in 2010. Between the USSS and ourselves, Zeus and its evil business partners, account takeover and transfer fraud, were rampant among consumers and businesses alike… If Zeus shows us that criminals have their minds on our money, Aurora, APTs, Stuxnet, and Anonymous remind us that some threat agents have more than money on their minds. These gave information risk a more sinister, targeted, and personal feel for us all in 2010.The numbers of public sector victims hit an all-time high in 2010. We studied more incidents involving theft of classified information, intellectual property, and other sensitive organizational data than ever before." - **2011 Data Breach Investigations Report (DBIR)**, Verizon and the United States Secret Service (USSS), and the Dutch National High Tech Crime Unit (NHTCU), 15 April 2011

"A significant portion of these threats can be averted by network services providers. There are some categories where a network service provider is best suited to provide security services. There are numerous reasons for this:

a) The network generates data that can be profiled and analyzed for anomalies that may be leading indicators of threats that are developing on the Internet. A large network service provider has a good vantage point to identify new threats and incorporate mechanisms to counteract them well before most network users can see them.

b) Providers of private enterprise services can analyze the same types of data for both and external threats. Their customers can minimize their need to implement separate network protections to supplement Internet gateway solutions.

c) Many providers control huge amounts of bandwidth in the core network where flooding attacks can be routed away from smaller bandwidth customer access links,

d)The network represents a huge processing infrastructure that can be used to help provide the security services needed.

Network service providers like AT&T are increasing these security services. The effectiveness and supplemental security services offerings provided by an ISP are an important differentiator in a highly competitive market. Among network based security service offerings that are available through leading providers include:

– Direct Denial of Service Defence, which can detect and filter flooding attacks in the network, where significant amounts of bandwidth are available to steer attacks way from target victims.

– Network-based Firewall services, which provide filtering of network packet activity before reaching customer boundaries based on ports, protocols, IP addresses, and even web URLs.

– Email scanning services, which screen email content for malware attachments, malicious Internet links, and spam.

– Various network flow analysis services can analyze Internet and private enterprise network activity for security threats without customers having to deploy services on their premise.

– Security analysis and operations services provide 24x7 network security monitoring, analytical support, and incident response capabilities. This service bring to customers the advantages their network providers' security expertise and merges it with their network operations disciplines. Network-based security services provide an opportunity for network service providers to offer more than competitive pricing as selection criteria for customers. protect other assets. And since major network service providers are an important part of critical national security infrastructure, it is only natural to consider network service providers as a trusted resource to help protect other assets.

Incentives for an international public-industry cooperative for real-time information and response will help to thwart globally diverse botnet threats before they are able to conduct other malicious acts.

We hope that owners and operators of other critical infrastructure will do their part to employ well prepared service providers to help protect their services. That is our challenge and our destiny in cybersecurity". - **Interview by General Clive Addy FrontLine Security Magazine Spring 2010** Brian Rexrod, Principal Network Security Architect at AT&T Chief Security Office

"As long as major governments desire unimpeded operational freedom in cyberspace, it will continue to be the Wild West. In the meantime, the owners and operators of the critical infrastructure which makes up this new battleground will continue to get caught in the cross-fire. Executives said that, apart from operational failures, the consequence they most feared from a cyberattack was reputational damage. The risk that mandatory disclosure of security incidents—for example the compromise of personal data—can drive policy and resources in counter-productive directions. Executives were also doubtful about the ability of their own critical infrastructure providers to offer reliable service in the event of a major cyberattack, 31 percent had the same doubts about their telecom provider." - **In the Crossfire Critical Infrastructure in the Age of Cyber War**, A global report on the threats facing key industries, McAfee Dec 2009

YOUR CORPORATE STRATEGY

AS SEEN AS PART OF A LARGER STRATEGIC INITIATIVE

The clean pipes strategy must be seen as an integral part of larger strategic initiatives. Conversely, the clean pipes imperative must also be considered within all product development/introduction. It is no longer acceptable to role out insecure products and services and retrofit security as a feature. Properties of confidentiality, integrity, availability, and privacy must be intrinsic to new systems.

Billion's will be invested into new networks in 2012, and this investment needs to be future-proofed. Clean pipes (security) must be native to IPv6, Mobility 4G+, Cloud and Datacentre consolidation strategies. The cost of implementing clean pipes in this manner is 'in the noise.' However, retrofitting clean pipes and the security necessary to sell IPv6, Mobility 4G+, Cloud and Datacentre products will be extremely expensive.

The clean pipe imperative for your Mobility strategy

The evolving mobility market is far more significant than people had first conceived. Convergence, IPV6, cloud and consumerization are powerful forces driving the infostructure value to the mobile edge-device. These wireless devices are as powerful as yesterdays computers and can access the cloud faster than many home wired connections.

Corporate networks, given consumerization, are getting drawn out into the mobile space. Traditional enterprise networks could theoretically be lost overnight.

COMMAND AND CONTROL INFRASTRUCTURE - Mitigation

Client-side mitigation requires that the customer build-out a reference architecture (ie., high performance secure network) with a command and control infrastructure capable of receiving real-time cyber threat intelligence (signatures, blacklists, reputational ratings, packet staining, policies etc), integrating the intelligence with in-house metrics and then apply modified policies to mitigate threats. The system must be automatic, dynamic and real-time.

"A secure infrastructure forms the foundation for service delivery."- **Service Provider Solutions DDoS Protection Solution Enabling "Clean Pipes" Capabilities**, June CISCO 2005

CLEANING CENTRE

Upstream intelligence can be delivered to perimeter cleaning/scrubbing centres for organizational specific solutions. These solutions are neither fully in-the-cloud clean pipes or client-side solutions. Rather, they fall more in line with traditional MSS offerings, but rely on upstream intelligence to function properly.

INTRINSIC MOTIVATORS FOR CLEAN PIPE INITIATIVES

MUST DO - CLEAN PIPE OBLIGATIONS

There is a mix of evolving standards, regulation and laws, which will, in their modern interpretation, require a degree of clean pipes that can be validated Type 1 evidence through continuous compliance audit.

"Internet Service Providers are in an excellent position to identify infections. ISPs should be given appropriate incentives for bearing the costs of Botnet Detection, Measurement, Disinfection & Defence. Government incentives or regulations may be created to integrate ISPs more fully in the mitigation process." - **Botnet Detection, Measurement, Disinfection & Defence**, European Network and Information Security Agency (ENISA), 09 March 2011

ISO recently adopted 27010 – Information Security Management for Inter-Sector Communications talks directly to 'clean pipes' delivery and reporting standards for ISPs.

Reports that need to be produced and delivered to governance bodies:

- *Enterprise wide scan of the infrastructure (none have never been produced)*
- *Quarterly and monthly status reports on all security processes,*
- *Incidents that affect the enterprise security posture or the information integrity such as Trojans, attacks, virus outbreaks, new technical vulnerabilities and business models that change their security mechanisms.*
- *Projects that have significant risks or do not comply to the information security architecture*

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.* Verifiable compliance and quantitative metrics is required as evidence for real time auditing. - **Technology Supply Chain Guidelines (TSCG) contracting clauses for telecommunications equipment and services,** Communications Security Establishment of Canada, TSCG-01\G October 2010

Lawful Access, Child Safety and anti-SPAM/Fraud laws require mandatory disclosure of certain crimes and support to Law Enforcement with and without a warrant for cyber threat intelligence data that can only be derived through a detection, processing and analysis infrastructure.

SHOULD DO

There are things that an organization ought to do as a matter of good corporate responsibility.

CUSTOMER EXPERIENCE

The customer experience directly manifests itself in sales revenue and consumed resources in Help Desk calls. There is an immense load (and cost) to when a significant portion of one's client based is compromised by malware they downloaded through the Internet and are now calling tech support because their 'Internet Service' is slow.

BRAND RISK

All organizations, and domains have reputational ratings based upon malicious activity monitoring. The way and priority in which traffic is routed/handled of shaped/throttled[119] across the Internet will be based upon these 'credit-like' ratings. Failure to implement clean pipes may adversely affect an organization's ability to route traffic quickly.

[119] *"In this decision, the Commission sets out its determinations in the proceeding initiated by Telecom Public Notice 2008-19 regarding the use of Internet traffic management practices (ITMPs) by Internet service providers (ISPs). The Commission establishes a principled approach that appropriately balances the freedom of Canadians to use the Internet for various purposes with the legitimate interests of ISPs to manage the traffic thus generated on their networks, consistent with legislation, including privacy legislation. "* - **Review of the Internet traffic management practices of Internet service providers,** Telecom Regulatory Policy CRTC 2009-657

CONCLUSION

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. There is no network perimeter and the entire supply chain is under some degree of global risk.

Our investigation uncovered high-confidence targeted threats over 24 hours period, from within a gargantuan data set, that had previously gone undetected by traditional (standard) security safeguards. This finding represents a manageable target set which would permit eventual attribution to an actor and a risk profile for the organization, should the research efforts been extended past the two month window permitted.

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 volume of malicious activity measured on a given network.

Proactive cyber defence is the only effective strategy within a real-time risk integrated risk framework. Next-generation reference architectures for high-performance secure networking© paves 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.

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

Every network component has three purposes:

- a primary function like routing,
- an ability to product 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 or measure effectiveness.

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 consolidate available 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 darknets, recursive DNS, honeynets, 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.

If you really want to know what is going on in your organization, then you have to invest smartly in the right solution for the given threat.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – CSS
22 Nepean St
Ottawa, Ontario K1A 0K2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
(NON-CONTROLLED GOODS)
DMC-A
REVIEW: GCEC JUNE 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

The Dark Space Project

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

McMahon, D. ; Rohozinski, R.

5. DATE OF PUBLICATION (Month and year of publication of document.)

July 2013

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

259

6b. NO. OF REFS (Total cited in document.)

119

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – CSS
22 Nepean St
Ottawa, Ontario K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

PSTP 02-359eSEc

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

DRDC CSS CR 2013-007

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unclassified/Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT

Cyberspace is best understood as a complex global ecosystem subject to technical and social drivers.

The research carried out by this study suggests that current approaches to cyber security are ill suited to detecting or anticipating threats, which increasingly rely on hybrid socio-technical vectors.

Securing national cyberspace requires a paradigm shift toward a common operating picture

(COP) of cyberspace. The project undertook research and experimental work along several axes critical to establishing a common operating picture of cyberspace. The principal outputs are grouped under the following three categories: i) research into the practical and ethical dimensions of a behaviour based model of detecting and anticipating cyber threats; ii) a reference architecture for implementing the objectives of the national cyber security strategy; and, iii) testing and validating methodological approaches to detecting advanced cyber threats on the basis of “live” data obtained from operational sources that had been stripped of Personal Identifiable Information.

Le concept de cyberespace est plus facile à comprendre lorsqu’on le décrit comme un écosystème complexe soumis à des facteurs techniques et sociaux. La recherche effectuée dans le cadre de la présente étude semble indiquer que les démarches actuelles en matière de cybersécurité sont inadéquates lorsque l'on tente de détecter ou d'anticiper des menaces, qui sont de plus en plus fondées sur des vecteurs hybrides socio-techniques. La protection du cyberespace national nécessite un changement de paradigme pour adopter une conception commune de la situation opérationnelle (ICSO) du cyberespace. Dans le cadre du projet, on a entrepris une étude et un travail expérimental sur plusieurs axes essentiels à l’établissement d’une conception commune de la situation opérationnelle du cyberespace. Les principaux résultats sont regroupés dans les trois catégories suivantes : i) recherches sur les aspects pratiques et éthiques d'un modèle fondé sur le comportement pour la détection et l'anticipation de cybermenaces; ii) une architecture de référence pour la mise en œuvre des objectifs de la Stratégie nationale de cybersécurité; iii) la mise à l'essai et la validation des démarches méthodologiques concernant la détection de cybermenaces avancées en fonction de données « réelles » provenant de sources opérationnelles et desquelles on a retiré tous les renseignements personnels identifiables (RPI).

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be
helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a
published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Cyber Security; Dark Space; Personal Identifiable Information