CASCADE

Joint Cyber Sensor Architecture

[redacted]

Overview

- Project Overview
- Current Status
- Proposed Architecture
- Towards 2015

Project Overview

- Alignment of passive cyber sensor capabilities and architecture in the SIGINT and ITS missions
- Goals
  - Common sensor technology and architecture
  - Address scalability issues in sensor deployments
- Scope
  - Passive sensors and supporting infrastructure are in scope
  - Analytic tools are out of scope
  - Host based capability is out of scope (caveat: passive messaging is in scope)

Our Sensors

SIGINT / ITS

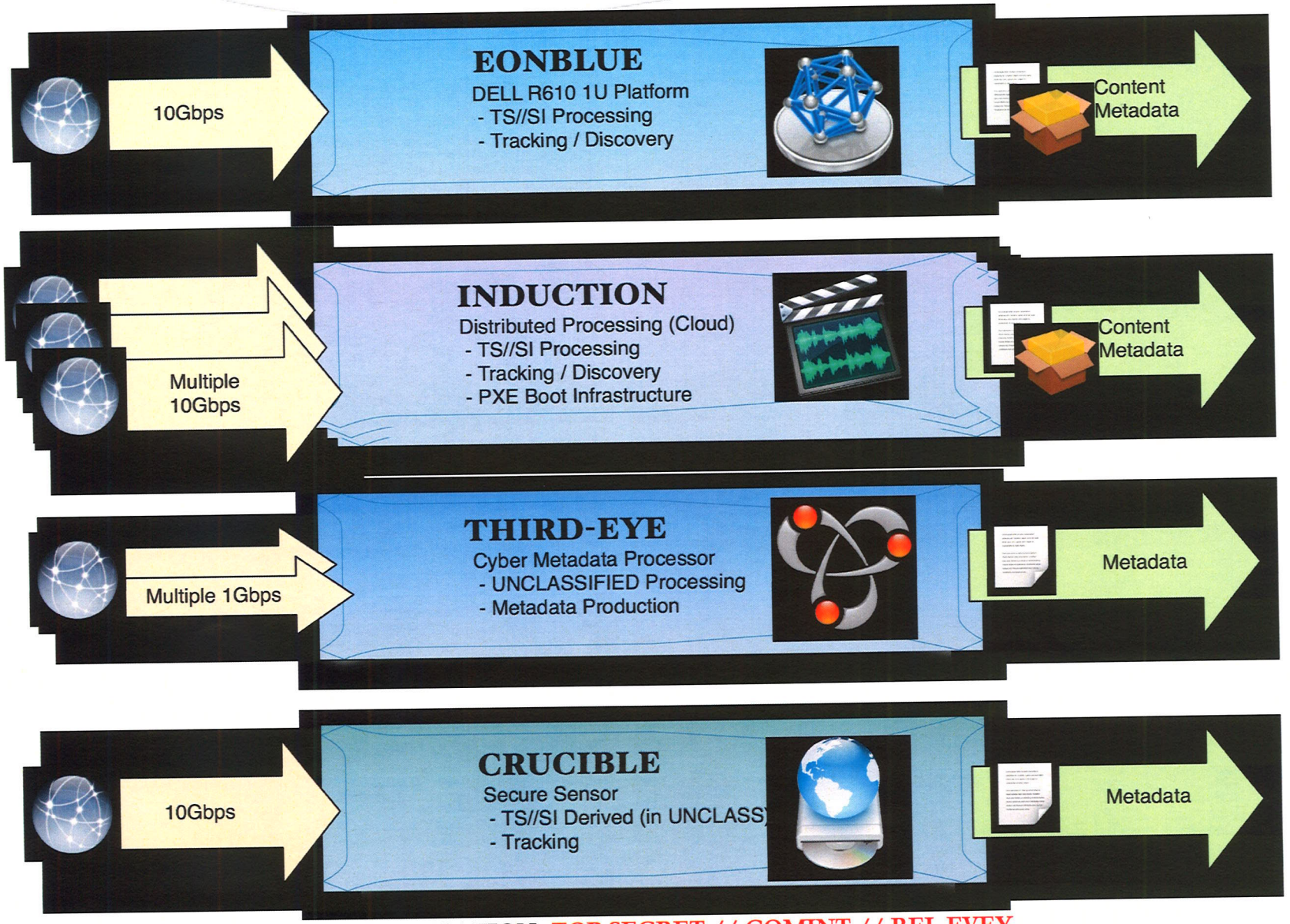
Photonic Prism

- Monitoring of GC Networks
- Includes:
  - Full-Take Packet Capture
  - Signature Based Detection
  - Anomaly Based Discovery
  - Analytic Environment
  - Oversight Compliance Tools

EONBLUE

- Monitoring in Passive SIGINT
- Includes:
  - Full-Take (on specific accesses)
  - Signature Based Detection
  - Anomaly Based Discovery
- Additional Functions are offloaded and exist further downstream:
  - Analytic Environment
  - Dataflow / Targeting
  - Oversight and Compliance Tools

Shades of Blue



Current Status – SIGINT Deployments

- Special Source
  - 100% INDUCTION coverage of main SSO sites + metadata production
  - THIRD-EYE metadata production at select new sites
  - CRUCIBLE deployments to newly emerging sites pre-SCIF environment (survey)
  - Increase in link speeds
- Warranted Collection
  - EONBLUE sensor deployment – full take collection
- FORNSAT
  - Recently upgraded to current EONBLUE code base, leveraging GCHQ CHOKEPOINT solution to integrate with environment (Virtualized)
- Working on SUNWHEEL / SMO
  - CHOKEPOINT system enroute to CASSIOPEIA
  - No SUNWHEEL presence as of yet, plans to leverage CHOKEPOINT capability

Current Status – IT Security Deployments

- Deployment at 3 edge gateway GC departments
  - Dynamic defence is enabled at two of these sites
- Deployment at the main government backbone
  - Dual 10Gbps links (~3Gbps loading)
  - Data volumes continue to increase due to Internet Access Point aggregation
- Currently performing full take and storage of all monitored traffic
  - System performance issues, overall analyst usability issues

Divergence – Sensor Deployments

- While both ITS/SIGINT currently leverage EONBLUE software:
  - The architectures are not aligned
  - Configuration differs greatly
  - Software versions are not standard across programs
  - The full capability of EONBLUE is not being leveraged equally across programs

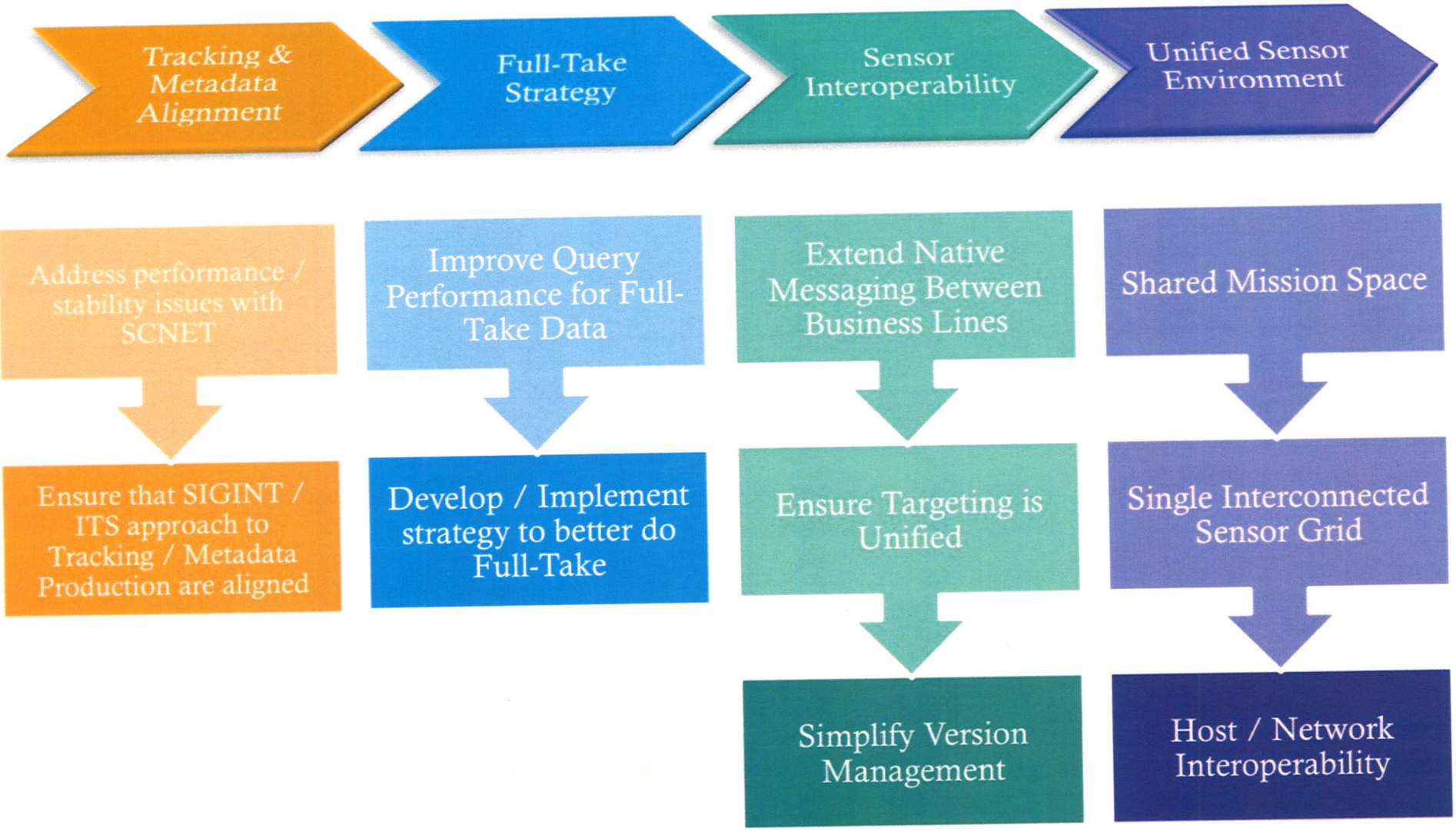
Proposal

CASCADE: A Way Forward

Problem Statement

- Divergence
  - Sensor architectures have diverged between ITS/SIGINT
  - Within each area, versions are not standardized
- Management and Scalability
  - Some configurations will not scale
  - Difficult to manage current sensor environment
  - High cost to grow existing solution (people, HW/SW costs)
- Duplication of Effort
  - Divergence creates duplication of effort
  - Limited resources are not focused on innovation and new challenges

A Phased Approach



Tracking and Metadata

Ensure EONBLUE is deployed in a standard fashion across all environments

- Upgrade SCNET to 10Gbps EONBLUE
- Update all SIGINT collection sites to latest code release

Produce Standard Metadata

- DNS Response Harvesting
- HTTP Client / Server Headers
- IP-to-IP Flow Summarizations

Full-Take Strategy

Address SCNET Scalability

Reconfiguration / Design of Storage Solution	Improved / Enforced data indexing and quering

Leverage Third-Eye Architecture

Distributed Collection Grid (at multiple clients)	Queries are Federated and Centrally Managed	Enables unique data ingest at client department (i.e. Firewall Logs)

Full-Take Strategy

- Benefits
  - Improve Performance
    - Better data indexing techniques
    - Federated queries across multiple systems
  - Reduced Cost (Storage local to client departments)
    - 10,000$ -> 25,000$ per client
    - Re-use of back-end Storage
  - Enable departmental security officers / operators
    - Capability of Third-Eye exceeds what is commercially available
- Cons
  - Requires network connections to each GC Department
  - Requires footprint within each departments datacenter
  - Complexity of distributed processing

Sensor Interoperability

EONBLUE sensors exchange messages to enable more robust selection and filtering

- Messages should be automatically exchanged between SIGINT and ITS/CTEC
- The sensor environment will be connected to enable seamless message flows

Targeting selectors for Cyber Threats will be unified

- When updates are made to SIGINT sensors the selectors will be automatically replicated for ITS
- JAZZFLUTE should support ITS analysts targeting SIGINT systems

Simplify Sensor Version Management

- Rapid deployment of new capability seamless across all programs / sites
- Distributed Induction (Across WAN)
- EBSH: Sensor has custom CLI like a switch and supports inline binary updates

Interoperability enables Synchronization

- ITS access to data collected by SIGINT sensors
  - Outputs should be common to enable a common analyst platform
  - Sensor environment should be seamlessly integrated
- Capability remains at cutting-edge
  - Single release for all collection programs in SIGINT, all points of presence, and across both missions
  - Management is simplified for operators, focusing on sensor expansions
  - Standardized OS Versions and Optimizations

Unified Sensor Environment

All Cyber Sensors form a complete eco-system

- Access point is Mandate / Authority Agnostic
- Sensors are Multi-Modal (Defence or Intelligence from any sensor, anytime)

Extend Messaging to Host Based Capabilities

- IT Security Host Based Agents
- CNE implants

Cyber Processing and analytic environments converge

Two-Tier Environment

- Automated / GUI rich environment for operators
- Command-Line Driven RAW access for Discovery

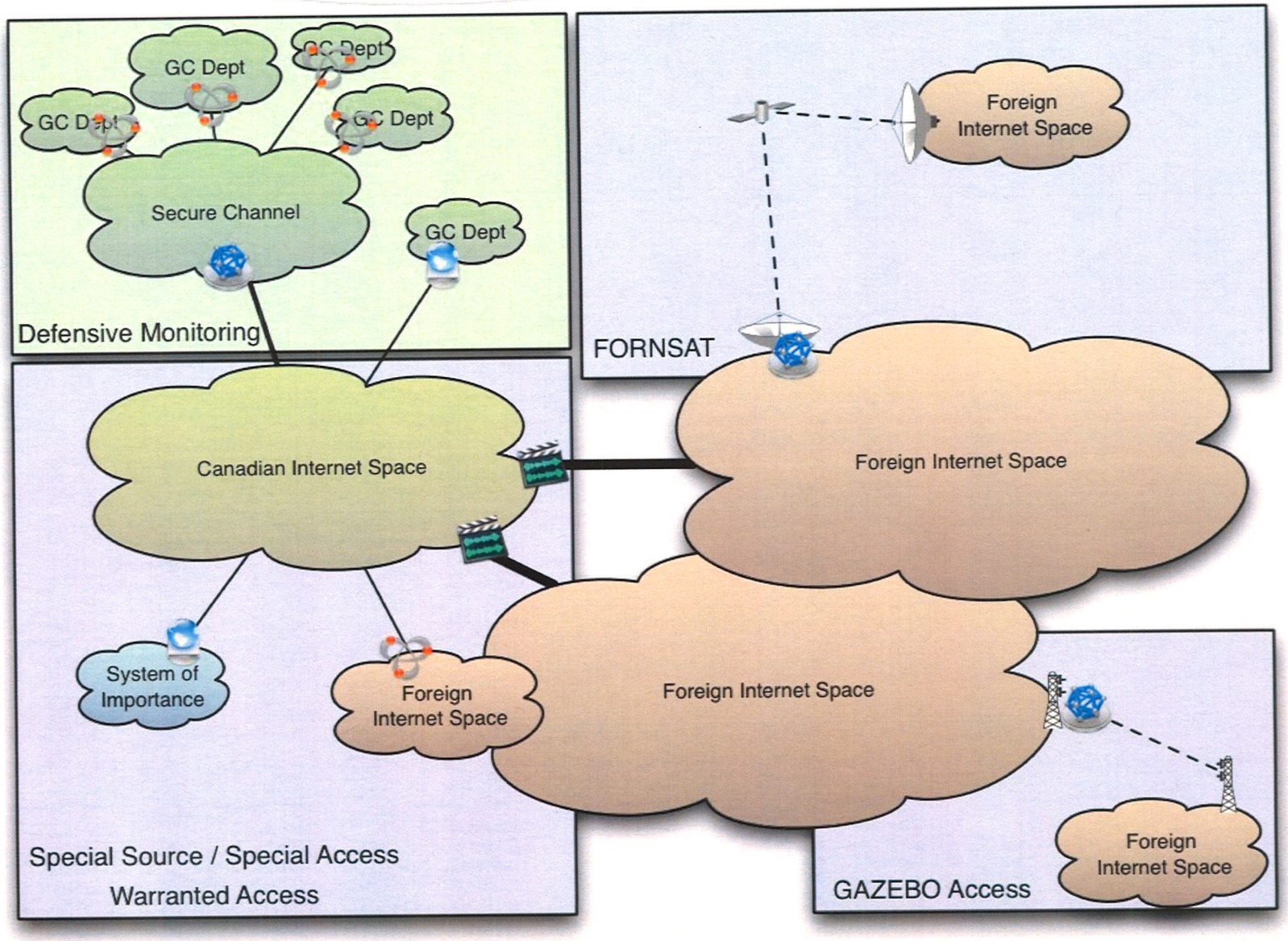
Shared Network Resources for Common Services

- Wiki / Blog / Chat
- NIS / NTP / DNS / Messaging / etc

Synchronized Deployment Strategy

- Where do you deploy sensors to maximize detection capabilities for Foreign Intelligence collection and Network Defence
- Coverage-based deployment considerations – what are the gaps?
  - [redacted]
  - [redacted]
  - [redacted]
- Threat-based deployment considerations – what are the gaps?
  - Based on EPRs
  - Threat trends and forecasting reports
  - Adversary TTPs

Canadian Cyber Sensor Grid



Towards 2015

Beyond sensor unification

CSEC 2015

- Strategic Priorities for CSEC
  - Strengthen "Team CSEC" and Prepare for Our New Facility
  - Adopt Innovative and Agile Business Solutions
  - **Expand Our Access Footprint**
  - **Improve Analytic Tradecraft**
  - Automate Manual Processes
  - **Synchronize the Cryptologic Enterprise for Cyber Security Mission**
  - **Enable "Effects" for Threat Mitigation**

Cyber Sensor in 2015

- **Expand Our Access Footprint**
  - We will increase SPECIAL SOURCE access to include all international gateways accessible from Canada.
  - We will deploy a sensor system that creates a protective grid at multiple layers over Government operations in Canada, and at all classification levels.
- **Improve Analytic Tradecraft**
  - We will equip SIGINT and cyber defence analysts with tools for flexible manipulation and customized analysis of large scale data sets.
  - We will build analytic tradecraft that understands, anticipates, and exploits the methodology of threat agents to provide comprehensive cyber- situational awareness based on multiple sources of cryptologic data.

Cyber Sensor in 2015

- **Synchronize the Cryptologic Enterprise for the Cyber Security Mission**
  - We will improve how we anticipate, identify, track and mitigate cyber threats on government systems through new concepts of joint operations.
  - We will design and develop joint SIGINT-ITS systems, including common data repositories, joint tasking and analytic systems.
  - We will increase operational capacity by ensuring SIGINT, ITS, and cryptologic partner sensors interoperate seamlessly.
  - We will synchronize and use ITS and SIGINT capabilities and complementary analyses to thwart cyber threats.

- **Enable "Effects" for Threat Mitigation**
  - We will seek the authority to conduct a wide spectrum of Effects operations in support of our mandates.
  - We will build the technical infrastructure, policy architecture and tradecraft necessary to conduct Effects operations.
  - We will further integrate ITS and SIGINT authorities and operations to leverage common sensors, systems and capabilities necessary for active and expanded dynamic cyber defence measures.

The Network Is The Sensor

Principles

- Security needs to be transparent to the user in order to be effective
- Security is a right for all Canadians
  - Federal Government
  - Municipal / Provincial Gov
  - Critical Infrastructure
  - Industry
  - The Citizen
- End-Users should incur little cost for security
- IT Assets should be distributed
- Access is mandate / authority agnostic

Goals

- Detect threats as they enter our national networks, not at the Gateway
- Identify Exfiltration, Command and Control, anywhere in our national networks
- The network is your defence for all infrastructure

Rationale

- We can't keep pace with our adversary
- Gateway / Device / End-Node protection is not sufficient (essential, yes)
- Rather than plugging one hole at a time, build better layered defence

Principles Explained

- Security is Transparent
  - If security inhibits functionality, or interferes with user experience it will be bypassed
- Security is a right
  - Attempting to protect everybody with end-node / gateway defenses is not feasible.
- IT Assets should be distributed
  - We run an open market, network providers will compete to provide access
  - Consolidated gateways creates single points of failure
  - Cost / Redundancy considerations

Goals

- Detection before attack hits target
  - If we wish to enable defence we must have intelligence to know when attacks enter our national infrastructure
- Identify Exfiltration / Command and Control
  - Some attacks will slip through or can't be seen (i.e. shaping)
  - Exploit our temporal advantage - aggressively pursue these implants as they will communicate 'home' for instruction
- The Network IS your Defence
  - In some cases, in cooperation with our partners we can affect change at the CORE of the Internet on detection:
    - Modify traffic routes
    - Silently discard malicious traffic (hygiene filtering)
    - Insert payload to disrupt adversaries

Rationale

- Keeping pace with the Adversary
  - From the time a malicious PDF is opened, till SEEDSPHERE has interactive control of a workstation is <3 minutes
  - There are countless malicious actors (state, crime, generic malware)
- Gateway / End-Node Defence by itself is insufficient
  - It is only one part of the problem
  - Over 600,000 Apps in the iTunes Appstore (How do you secure that?)
  - Defence in Depth includes network monitoring, and network interaction
- Build better Defence
  - Our current MO is to resolve one incident at a time
  - Automate the defence through a robust network capable of not only detection, but manipulation of malicious traffic

What does it Mean?

- EONBLUE will be integrated into the Network
  - Monitoring Government of Canada
  - Monitoring Core Infrastructure (Special Source) extending the reach to view national infrastructure
  - Monitoring foreign Internet Space
- EONBLUE will enable defensive operations
  - Through robust communication with host-based capabilities
  - Through direct manipulation of network communications
  - Through interaction with Teleco infrastructure to affect change

Food for Thought

Changing the way we think

Changing the way we think

- Tipping and Cueing
  - If the purpose is to enable defence of national infrastructure it becomes unnecessary in a 5-eyes context
    - We have full visibility of our national infrastructure
    - The chance of 'beating' the internet for latency of an attack is minimal
    - The network will perform the filtering
  - What if instead T&C enables intelligence collection (Cyber Session Collection)?

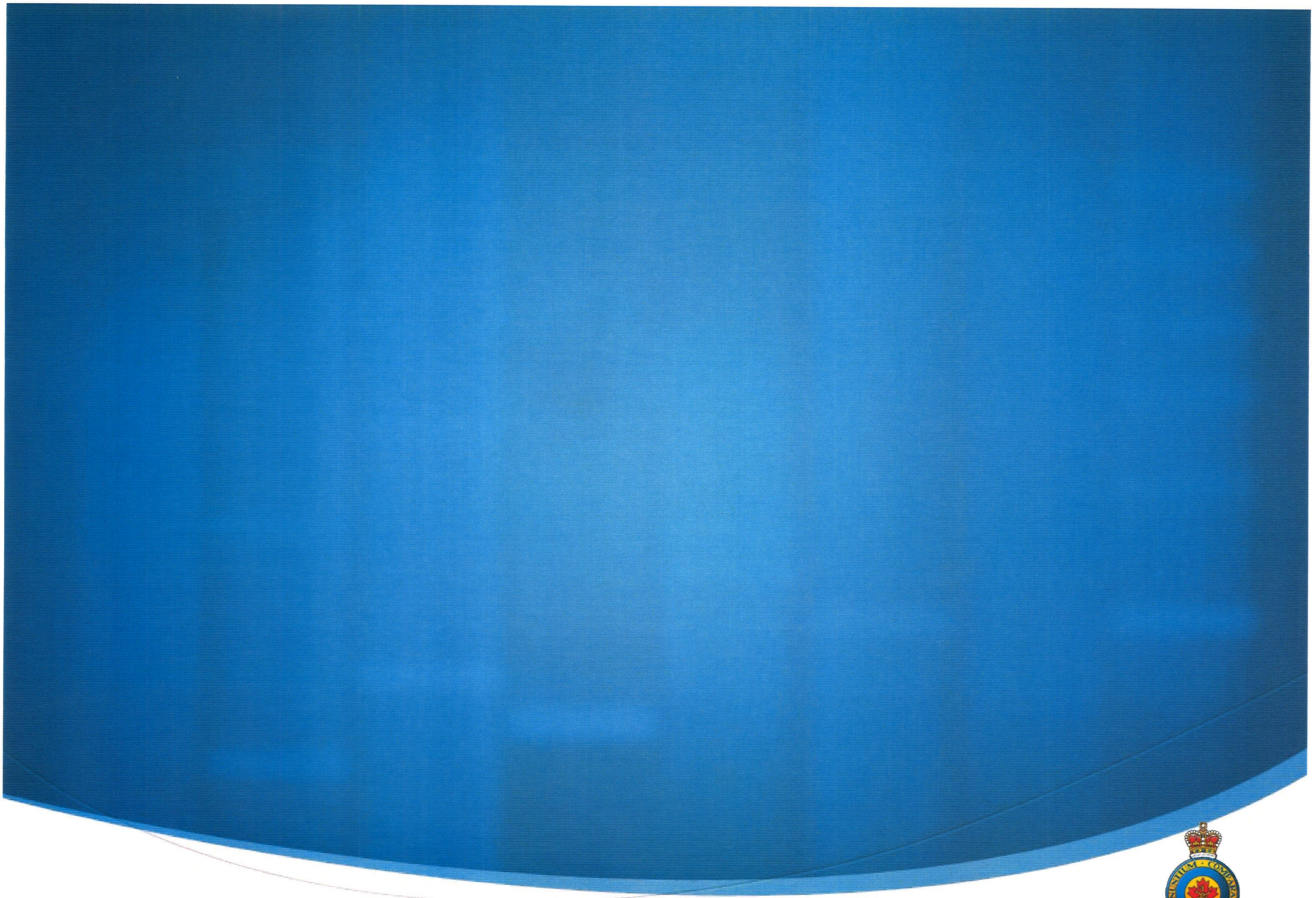
- Targeting and Tasking
  - We all share common targets and we will all target using our national capability the cyber threats we know about
  - No need for 2nd party tasking / targeting requests. Instead expose cyber information across the community
  - What if instead we focus on analytic collaboration and knowledge transfer
    - TEXPRO information, federated repositories (malware/traffic), etc

Changing the way we think

- Foreign SIGINT Intercept
  - Becomes the 'hunting ground' for discovery of new threats
  - Enables attribution and counter-intelligence reporting
  - Defence is taken care of by 'The Network'
  - Mobile Platforms are the next frontier, what is their implication on Cyber?
- Domestic Defence
  - We will exhaust the treasury deploying network appliances to perform dynamic defence
  - The same capabilities will be integrated into the CORE of the Internet
  - Defence in Depth through complimentary capabilities on end-nodes, at the gateway, and in the core of the Internet.

Conclusion

- CASCADE
  - The harmonization of ITS/SIGINT Sensor capabilities
  - Lays the foundation for long-term integration of Cyber within the Cryptologic Enterprise
- Towards 2015
  - The Network is the Sensor
    - Defence, Mitigation, Intelligence all formed from a single comprehensive network creating a perimeter around Canada
    - Extending our reach through 5-eyes partnerships to ensure mutual defence of national assets.



CASCADE

Joint Cyber Sensor Architecture

[redacted]

Overview

- Project Overview
- Current Status
- Proposed Architecture
- Towards 2015

Project Overview

- Alignment of passive cyber sensor capabilities and architecture in the SIGINT and ITS missions
- Goals
  - Common sensor technology and architecture
  - Address scalability issues in sensor deployments
- Scope
  - Passive sensors and supporting infrastructure are in scope
  - Analytic tools are out of scope
  - Host based capability is out of scope (caveat: passive messaging is in scope)

What is the project about?
Define the goal of this project
Is it similar to projects in the past or is it a new effort?
Define the scope of this project
Is it an independent project or is it related to other projects?

* Note that this slide is not necessary for weekly status meetings

Our Sensors

SIGINT / ITS

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Photonic Prism

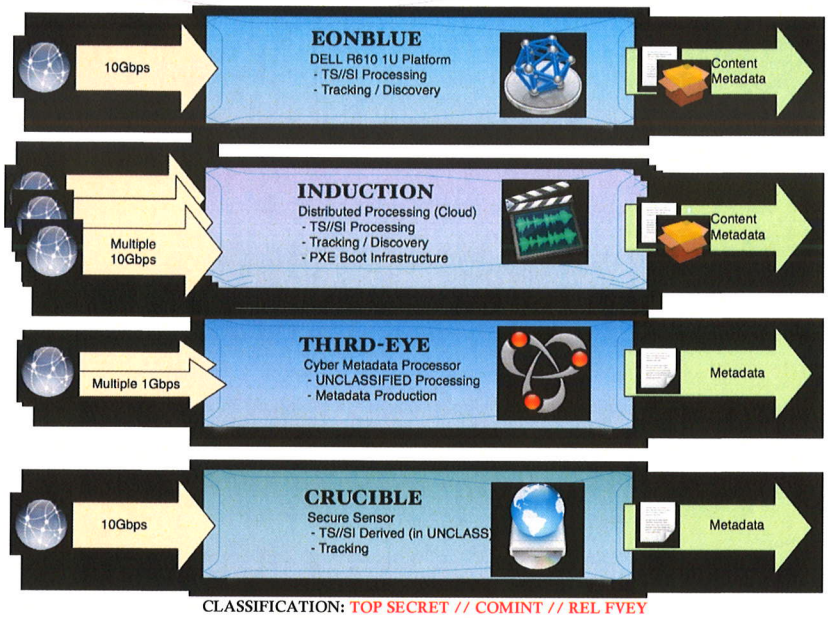
- Monitoring of GC Networks
- Includes:
  - Full-Take Packet Capture
  - Signature Based Detection
  - Anomaly Based Discovery
  - Analytic Environment
  - Oversight Compliance Tools

EONBLUE

- Monitoring in Passive SIGINT
- Includes:
  - Full-Take (on specific accesses)
  - Signature Based Detection
  - Anomaly Based Discovery
- Additional Functions are offloaded and exist further downstream:
  - Analytic Environment
  - Dataflow / Targeting
  - Oversight and Compliance Tools

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Shades of Blue



CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Current Status – SIGINT Deployments

- Special Source
  - 100% INDUCTION coverage of main SSO sites + metadata production
  - THIRD-EYE metadata production at select new sites
  - CRUCIBLE deployments to newly emerging sites pre-SCIF environment (survey)
  - Increase in link speeds
- Warranted Collection
  - EONBLUE sensor deployment – full take collection
- FORNSAT
  - Recently upgraded to current EONBLUE code base, leveraging GCHQ CHOKEPOINT solution to integrate with environment (Virtualized)
- Working on SUNWHEEL / SMO
  - CHOKEPOINT system enroute to CASSIOPEIA
  - No SUNWHEEL presence as of yet, plans to leverage CHOKEPOINT capability

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

* If any of these issues caused a schedule delay or need to be discussed further, include details in next slide.

Current Status – IT Security Deployments

- Deployment at 3 edge gateway GC departments
  - Dynamic defence is enabled at two of these sites
- Deployment at the main government backbone
  - Dual 10Gbps links (~3Gbps loading)
  - Data volumes continue to increase due to Internet Access Point aggregation
- Currently performing full take and storage of all monitored traffic
  - System performance issues, overall analyst usability issues

Divergence – Sensor Deployments

- While both ITS/SIGINT currently leverage EONBLUE software:
  - The architectures are not aligned
  - Configuration differs greatly
  - Software versions are not standard across programs
  - The full capability of EONBLUE is not being leveraged equally across programs

Proposal

CASCADE: A Way Forward

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

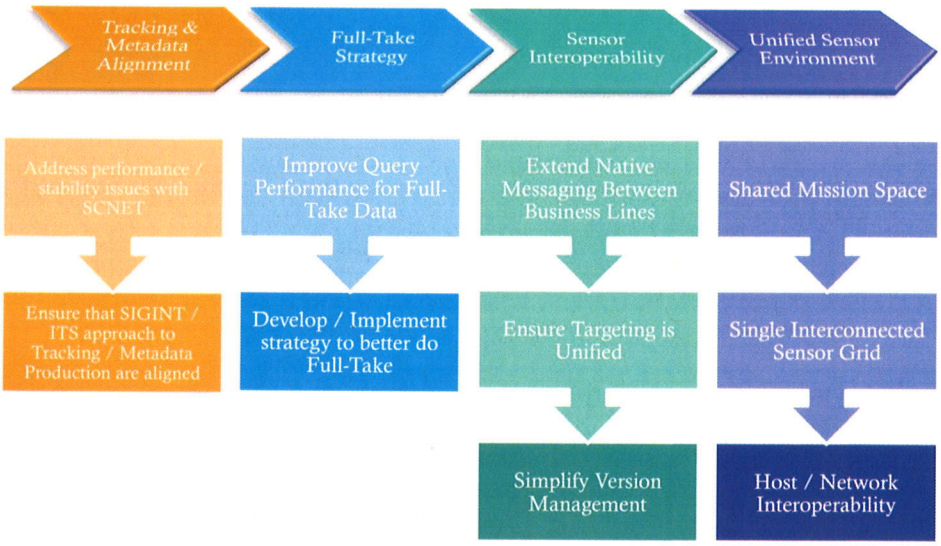
Problem Statement

- Divergence
  - Sensor architectures have diverged between ITS/SIGINT
  - Within each area, versions are not standardized
- Management and Scalability
  - Some configurations will not scale
  - Difficult to manage current sensor environment
  - High cost to grow existing solution (people, HW/SW costs)
- Duplication of Effort
  - Divergence creates duplication of effort
  - Limited resources are not focused on innovation and new challenges

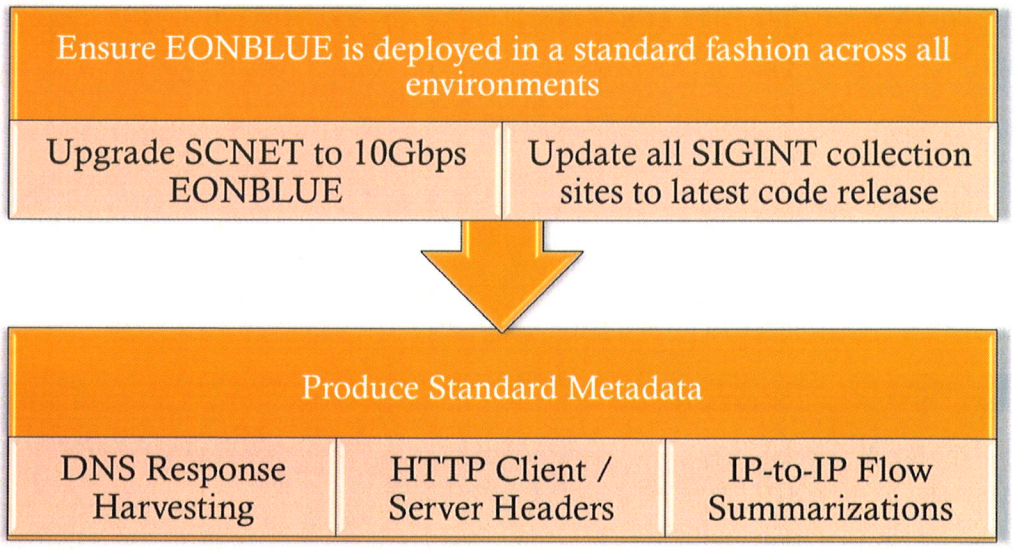
CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Duplicate this slide as necessary if there is more than one issue.
This and related slides can be moved to the appendix or hidden if necessary.

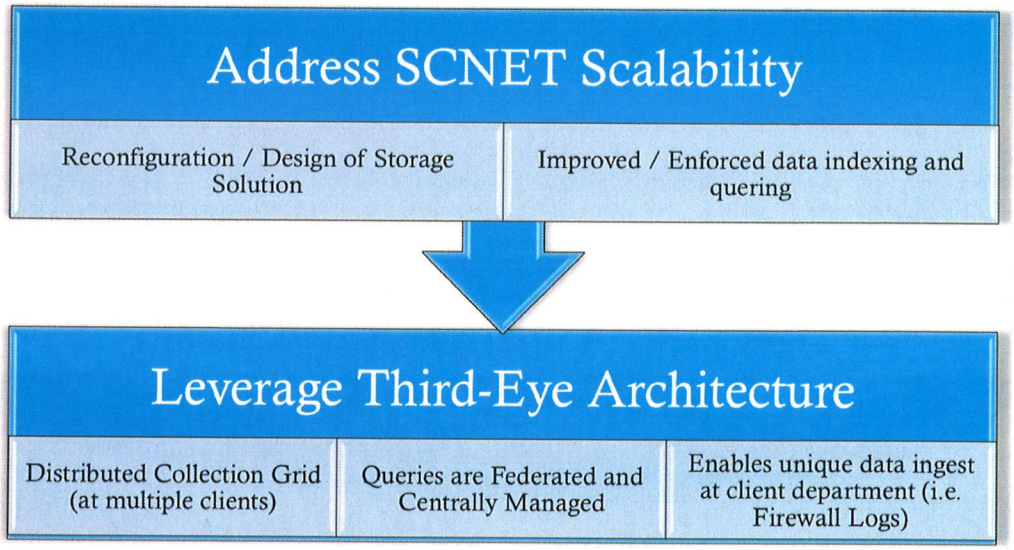
A Phased Approach



Tracking and Metadata



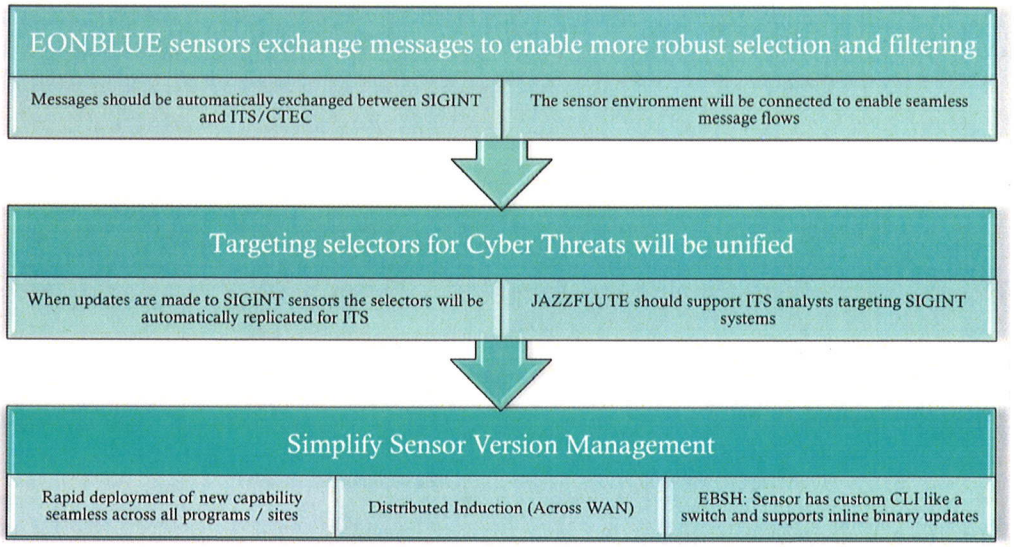
Full-Take Strategy



Full-Take Strategy

- Benefits
  - Improve Performance
    - Better data indexing techniques
    - Federated queries across multiple systems
  - Reduced Cost (Storage local to client departments)
    - 10,000$ -> 25,000$ per client
    - Re-use of back-end Storage
  - Enable departmental security officers / operators
    - Capability of Third-Eye exceeds what is commercially available
- Cons
  - Requires network connections to each GC Department
  - Requires footprint within each departments datacenter
  - Complexity of distributed processing

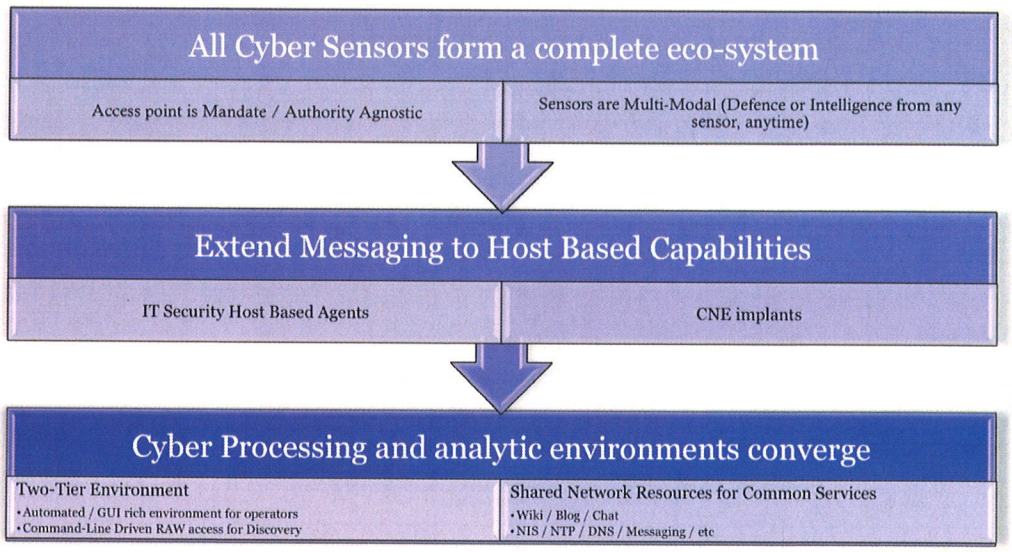
Sensor Interoperability



Interoperability enables Synchronization

- ITS access to data collected by SIGINT sensors
  - Outputs should be common to enable a common analyst platform
  - Sensor environment should be seamlessly integrated
- Capability remains at cutting-edge
  - Single release for all collection programs in SIGINT, all points of presence, and across both missions
  - Management is simplified for operators, focusing on sensor expansions
  - Standardized OS Versions and Optimizations

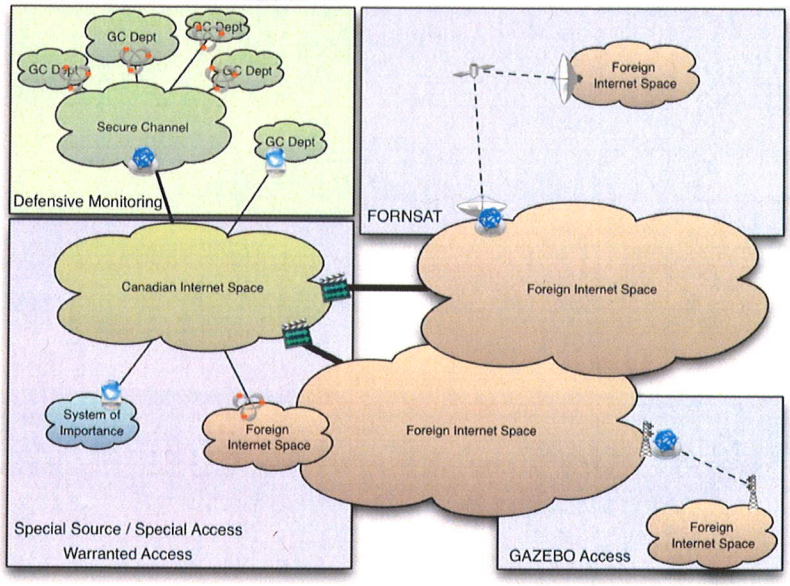
Unified Sensor Environment



Synchronized Deployment Strategy

- Where do you deploy sensors to maximize detection capabilities for Foreign Intelligence collection and Network Defence
- Coverage-based deployment considerations – what are the gaps?
  - [redacted]
  - [redacted]
  - [redacted]
- Threat-based deployment considerations – what are the gaps?
  - Based on EPRs
  - Threat trends and forecasting reports
  - Adversary TTPs

Canadian Cyber Sensor Grid



Towards 2015

Beyond sensor unification

CSEC 2015

- Strategic Priorities for CSEC
  - Strengthen "Team CSEC" and Prepare for Our New Facility
  - Adopt Innovative and Agile Business Solutions
  - **Expand Our Access Footprint**
  - **Improve Analytic Tradecraft**
  - Automate Manual Processes
  - **Synchronize the Cryptologic Enterprise for Cyber Security Mission**
  - **Enable "Effects" for Threat Mitigation**

Cyber Sensor in 2015

- **Expand Our Access Footprint**
  - We will increase SPECIAL SOURCE access to include all international gateways accessible from Canada.
  - We will deploy a sensor system that creates a protective grid at multiple layers over Government operations in Canada, and at all classification levels.
- **Improve Analytic Tradecraft**
  - We will equip SIGINT and cyber defence analysts with tools for flexible manipulation and customized analysis of large scale data sets.
  - We will build analytic tradecraft that understands, anticipates, and exploits the methodology of threat agents to provide comprehensive cyber- situational awareness based on multiple sources of cryptologic data.

Cyber Sensor in 2015

- **Synchronize the Cryptologic Enterprise for the Cyber Security Mission**
  - We will improve how we anticipate, identify, track and mitigate cyber threats on government systems through new concepts of joint operations.
  - We will design and develop joint SIGINT-ITS systems, including common data repositories, joint tasking and analytic systems.
  - We will increase operational capacity by ensuring SIGINT, ITS, and cryptologic partner sensors interoperate seamlessly.
  - We will synchronize and use ITS and SIGINT capabilities and complementary analyses to thwart cyber threats.

- **Enable "Effects" for Threat Mitigation**
  - We will seek the authority to conduct a wide spectrum of Effects operations in support of our mandates.
  - We will build the technical infrastructure, policy architecture and tradecraft necessary to conduct Effects operations.
  - We will further integrate ITS and SIGINT authorities and operations to leverage common sensors, systems and capabilities necessary for active and expanded dynamic cyber defence measures.

The Network Is The Sensor

Principles

- Security needs to be transparent to the user in order to be effective
- Security is a right for all Canadians
  - Federal Government
  - Municipal / Provincial Gov
  - Critical Infrastructure
  - Industry
  - The Citizen
- End-Users should incur little cost for security
- IT Assets should be distributed
- Access is mandate / authority agnostic

Goals

- Detect threats as they enter our national networks, not at the Gateway
- Identify Exfiltration, Command and Control, anywhere in our national networks
- The network is your defence for all infrastructure

Rationale

- We can't keep pace with our adversary
- Gateway / Device / End-Node protection is not sufficient (essential, yes)
- Rather than plugging one hole at a time, build better layered defence

Principles Explained

- Security is Transparent
  - If security inhibits functionality, or interferes with user experience it will be bypassed
- Security is a right
  - Attempting to protect everybody with end-node / gateway defenses is not feasible.
- IT Assets should be distributed
  - We run an open market, network providers will compete to provide access
  - Consolidated gateways creates single points of failure
  - Cost / Redundancy considerations

Goals

- Detection before attack hits target
  - If we wish to enable defence we must have intelligence to know when attacks enter our national infrastructure
- Identify Exfiltration / Command and Control
  - Some attacks will slip through or can't be seen (i.e. shaping)
  - Exploit our temporal advantage - aggressively pursue these implants as they will communicate 'home' for instruction
- The Network IS your Defence
  - In some cases, in cooperation with our partners we can affect change at the CORE of the Internet on detection:
    - Modify traffic routes
    - Silently discard malicious traffic (hygiene filtering)
    - Insert payload to disrupt adversaries

Rationale

- Keeping pace with the Adversary
  - From the time a malicious PDF is opened, till SEEDSPHERE has interactive control of a workstation is <3 minutes
  - There are countless malicious actors (state, crime, generic malware)
- Gateway / End-Node Defence by itself is insufficient
  - It is only one part of the problem
  - Over 600,000 Apps in the iTunes Appstore (How do you secure that?)
  - Defence in Depth includes network monitoring, and network interaction
- Build better Defence
  - Our current MO is to resolve one incident at a time
  - Automate the defence through a robust network capable of not only detection, but manipulation of malicious traffic

What does it Mean?

- EONBLUE will be integrated into the Network
  - Monitoring Government of Canada
  - Monitoring Core Infrastructure (Special Source) extending the reach to view national infrastructure
  - Monitoring foreign Internet Space
- EONBLUE will enable defensive operations
  - Through robust communication with host-based capabilities
  - Through direct manipulation of network communications
  - Through interaction with Teleco infrastructure to affect change

Food for Thought

Changing the way we think

Changing the way we think

- Tipping and Cueing
  - If the purpose is to enable defence of national infrastructure it becomes unnecessary in a 5-eyes context
    - We have full visibility of our national infrastructure
    - The chance of 'beating' the internet for latency of an attack is minimal
    - The network will perform the filtering
  - What if instead T&C enables intelligence collection (Cyber Session Collection)?

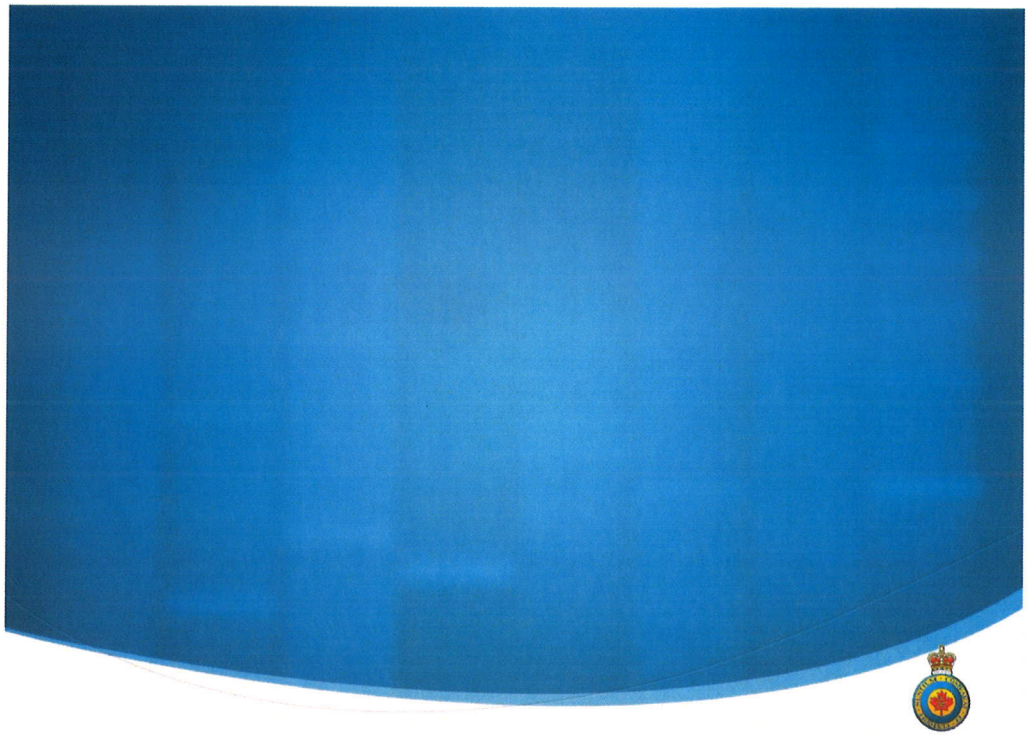
- Targeting and Tasking
  - We all share common targets and we will all target using our national capability the cyber threats we know about
  - No need for 2nd party tasking / targeting requests. Instead expose cyber information across the community
  - What if instead we focus on analytic collaboration and knowledge transfer
    - TEXPRO information, federated repositories (malware/traffic), etc

Changing the way we think

- Foreign SIGINT Intercept
  - Becomes the 'hunting ground' for discovery of new threats
  - Enables attribution and counter-intelligence reporting
  - Defence is taken care of by 'The Network'
  - Mobile Platforms are the next frontier, what is their implication on Cyber?
- Domestic Defence
  - We will exhaust the treasury deploying network appliances to perform dynamic defence
  - The same capabilities will be integrated into the CORE of the Internet
  - Defence in Depth through complimentary capabilities on end-nodes, at the gateway, and in the core of the Internet.

Conclusion

- CASCADE
  - The harmonization of ITS/SIGINT Sensor capabilities
  - Lays the foundation for long-term integration of Cyber within the Cryptologic Enterprise
- Towards 2015
  - The Network is the Sensor
    - Defence, Mitigation, Intelligence all formed from a single comprehensive network creating a perimeter around Canada
    - Extending our reach through 5-eyes partnerships to ensure mutual defence of national assets.



CSEC SIGINT Cyber Discovery: Summary of the current effort

[redacted]

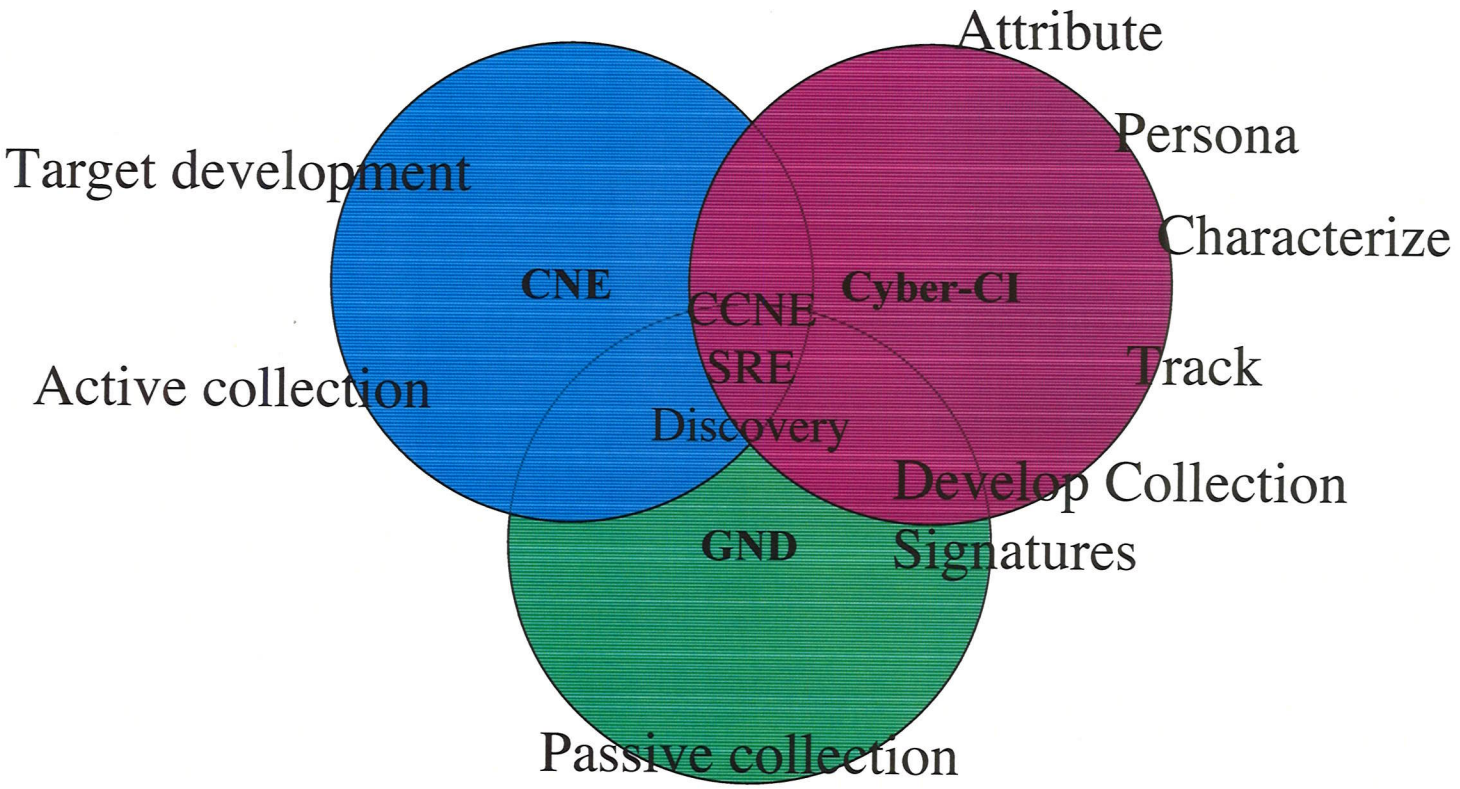
Communications Security Establishment Canada
Covert Network Threats
Cyber-Counterintelligence

Discovery Conference
GCHQ – November 2010

Outline

- CSEC SIGINT Cyber
  - K0G (CCNE)
  - GA4 (GND)
  - CNT1 (CCI)
- CSEC SIGINT Cyber – Operational Discovery
  - Network Based Anomaly Detection
  - Host Based Anomaly Detection
- Contacts

CSEC Cyber Counterintelligence

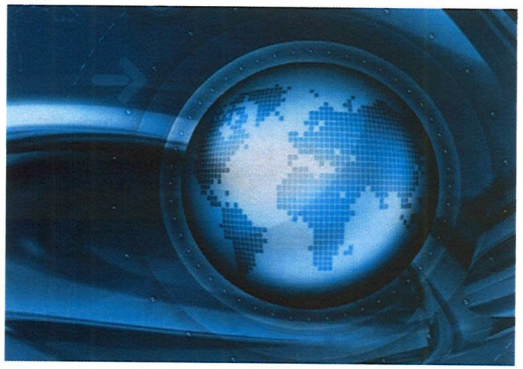


Counter CNE (K0G)

- Part of CSEC CNE operations (K0)
- Recently formed matrix team
- Analysts and operators from CNE Operations, Cyber-Counterintelligence and Global Network Detection
- Mandate:
  - Provide situational awareness to CNE operators
  - Discover unknown actors on existing CNE targets
  - Detect known actors on covert infrastructure
  - Pursue known actors through CNE
  - Review OPSEC of CNE operations

Global Network Detection (GND)

- Develop capabilities to improve the ability of the SIGINT collection system to detect Computer Network Exploitation and Computer Network Attack



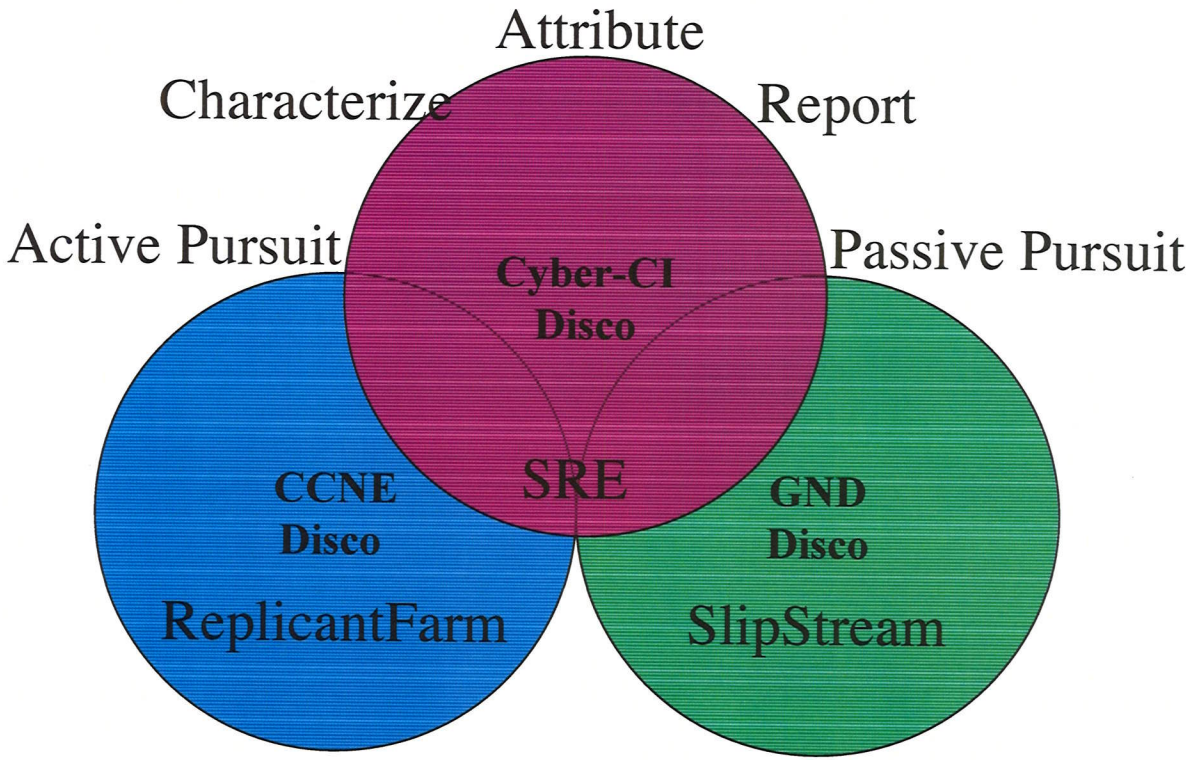
- Help enable CSEC's CNE program through timely identification of vulnerable computer systems and foreign CNE methodologies/activities

- Act as technical liaison between IT Security and SIGINT for CNO issues

Cyber Counterintelligence (CNT1)

- Covert Network Threats (New Directorate within CSEC)
  - CNT1 (Cyber Counterintelligence)
  - CNT2 (Traditional Counterintelligence)
- CNT1 Mission
  - To produce intelligence on the capabilities, intentions and activities of Hostile Intelligence Services to support Counterintelligence activities at home and abroad.
- Fusion of Cyber Analytic Skills with Traditional Counterintelligence Analytic Skills
  - All Cyber-Counterintelligence Investigations *should* lead to Traditional Counterintelligence investigations.

CSEC SIGINT CCI Discovery



CSEC CNE (K) - WARRIORPRIDE

- WARRIORPRIDE (WP):
  - Scalable, Flexible, Portable CNE platform
  - Unified framework within CSEC and across the 5 eyes
  - WARRIORPRIDE@CSE/etc. == DAREDEVIL@GCHQ
  - xml command output to operators
- Several plugins used for machine recon / OPSEC assessment
  Several WP plugins are useful for CCNE:
  - Slipstream : machine reconnaissance
  - ImplantDetector : implant detection
  - RootkitDetector : rootkit detection
  - Chordflier/U_ftp : file identification / retrieval
  - NameDropper : DNS
  - WormWood : network sniffing and characterization

K0G – ReplicantFarm

- Created to leverage the WP XML output in a meaningful way
- Module based parser/alert system running on real-time CNE operational data
- Custom/module based analysis:
  - Actors
  - Implant technology
  - Host based signatures
  - Network based signatures

REPLICANTFARM generic modules

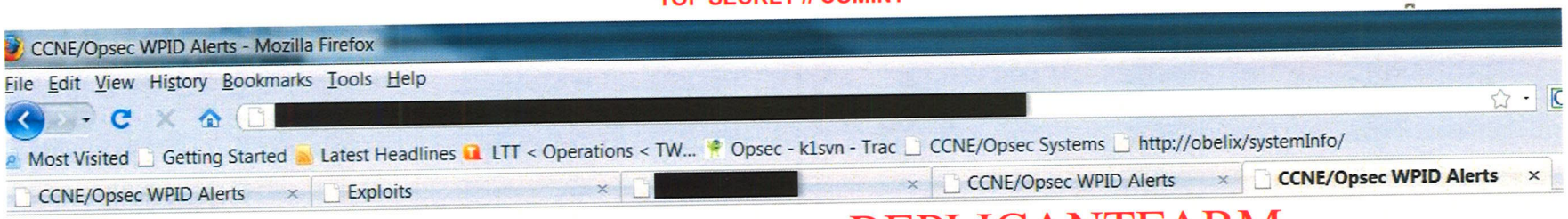
- Cloaked
- Recycler
- Rar password
- Tmp executable
- Packed
- Peb modification
- Privileges
- MS pretender
- System32 “variables”
- Strange DLL extensions
- Kernel cloaking
- Schedule at
- Ntuninstall execution
- hidden

Other ideas….

Generic modules : example

```
my @runningProcs = xml_isProcessRunning( $xml, 'svchost.{1,3}\\.exe',
                                               'winlogon.{1,3}\\.exe',
                                               'services.{1,3}\\.exe',
                                               'lsass.{1,3}\\.exe',
                                               'spoolsv.{1,3}\\.exe',
                                               'autochk.{1,3}\\.exe',
                                               'logon.{1,3}\\.scr',
                                               'rundll32.{1,3}\\.exe',
                                               'chkdsk.{1,3}\\.exe',
                                               'chkntfs.{1,3}\\.exe' ,
                                               'logonui.{1,3}\\.exe',
                                               'ntoskrnl.{1,3}\\.exe',
                                               'ntvdm.{1,3}\\.exe',
                                               'rdpclip.{1,3}\\.exe',
                                               'taskmgr.{1,3}\\.exe',
                                               'userinit.{1,3}\\.exe',
                                               'wscntfy.{1,3}\\.exe',
                                               'tcpmon.{1,3}\\.dll' );

   foreach my $runningProc (@runningProcs)
   {
      $alertText .= "Suspicious process detected, legitimate exe named appended with string: " .
     $runningProc . ".\n";
   }
```



CCNE/Opsec WPID Alerts

REPLICANTFARM

Note that the search is done with the fields as perl regular expressions...

Examples:	Current Modules:							
• Dots (.) are single-character wildcards • Dot-Star (.*) means any number of characters • Single WPID: 51\.8\.1\.13 • Class C WPID: 51\.8\.1\. • Infrastructure: ^50\.	mod_1000_WH_Implant.pl mod_100_MM_SHEPHERD.pl mod_101_MM_CARBON.pl mod_102_MM_REGBACKUP.pl mod_103_MM_DOGHOUSE.pl mod_104_MM_WALKER.pl	mod_1100_VO_Implant.pl mod_11_cloaked.pl mod_1200_AF_ALOOFNESS.pl mod_12_system32var.pl mod_13_rarpassword.pl mod_14_strangedllextensions.pl	mod_15_procParents.pl mod_16_recyclerexec.pl mod_17_tmpexec.pl mod_18_passwordfilters.pl mod_19_kernelcloaking.pl mod_1_packed.pl	mod_200_SD_MI20.pl mod_201_SD_MI25FTP.pl mod_20_pebmodification.pl mod_21_scheduleat.pl mod_22_ntuninstallexec.pl mod_23_hidden.pl	mod_24_expectedArguments.pl mod_25_privileges.pl mod_300_UNK_TCPSRV32.pl mod_301_UNK_BLAZINGANGEL.pl mod_302_TINYWEB.pl mod_303_UNK_CYDLL.pl	mod_304_UNK_WINPACP.pl mod_305_UNK_IASEX.pl mod_306_UNK_WINUPDATE.pl mod_307_UNK_QUIVERINGSQUAB.pl mod_308_UNK_WINDO.pl mod_309_UNK_DIESELRATTLE.pl	mod_310_UNK_WIDOWKEY.pl mod_311_UNK_CIVETCAT.pl mod_3_mspretender.pl mod_400_SS_WINBEE.pl mod_401_SS_SSLINST.pl mod_402_SS_SharpR.pl	mo mo mo mo mo mo

WPID Regexp:	Module Regexp: MM	Type: Historic: Live:

Submit Query

ALERTS

[redacted]	Module: mod_103_MM_DOGHOUSE.pl	Date: 2010-01-21T15:36:39.968	Tag: MM	File name: ../datastore/archive/2010/01/21/15/TXID0000272485_18_Y2010M01D21_H15M28S59_MS642MU500NS0_RXID050_000_0

Details:
Possible MM DOGHOUSE driver file: C:\WINNT\$NtUninstallQ244598$.
Possible MM DOGHOUSE driver file: C:\WINNT\$NtUninstallQ244598$\afd.sys.
Possible MM DOGHOUSE driver file: C:\WINNT\$NtUninstallQ244598$\netbt.sys.
Possible MM DOGHOUSE driver file: C:\WINNT\$NtUninstallQ244598$\tcpip.sys.
Possible MM DOGHOUSE driver file: C:\WINNT\$NtUninstallQ244598$\hotfix.inf.

--==PULLEDPORK==--

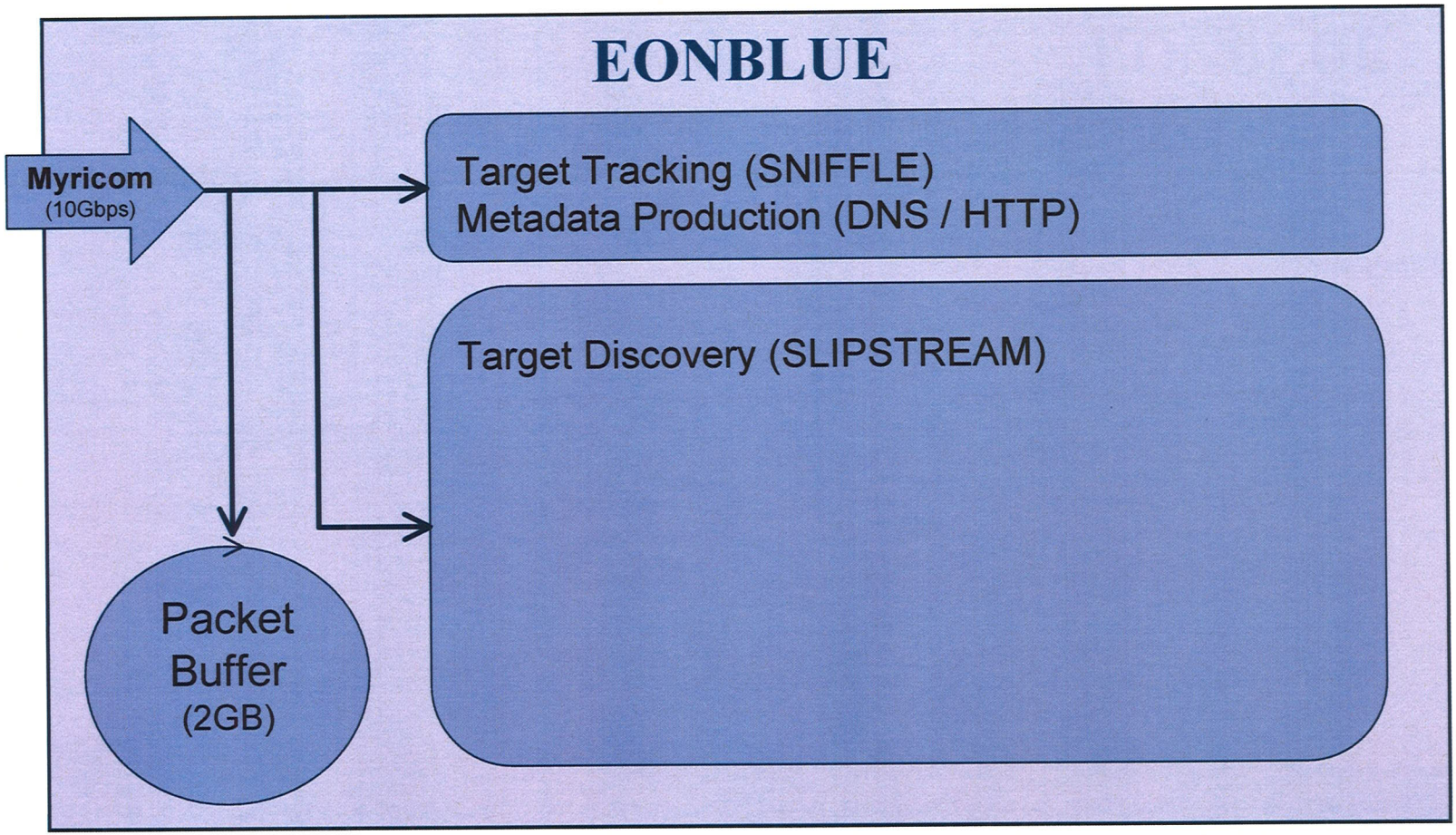
EONBLUE

- CSEC cyber threat detection platform
- Over 8 years of development effort
- Scales to backbone internet speeds
- Over 200 sensors deployed across the globe

Track Known Threats

Discover Unknown Threats

Defence at the core of the Internet


EONBLUE
Myricom
(10Gbps)
Target Tracking (SNIFFLE)
Metadata Production (DNS / HTTP)
Target Discovery (SLIPSTREAM)
Packet
Buffer
(2GB)

Anomaly Detection Tools

- There are currently over 50 modules in Slipstream
  - RFC Validation
  - Heuristic Checks
  - Periodicity
  - Simple Encryption
  - Streaming Attack Detection
  - Analyst Utilities

- Not all of these tools are 'YES/NO', some will require some work.

Heuristic Example

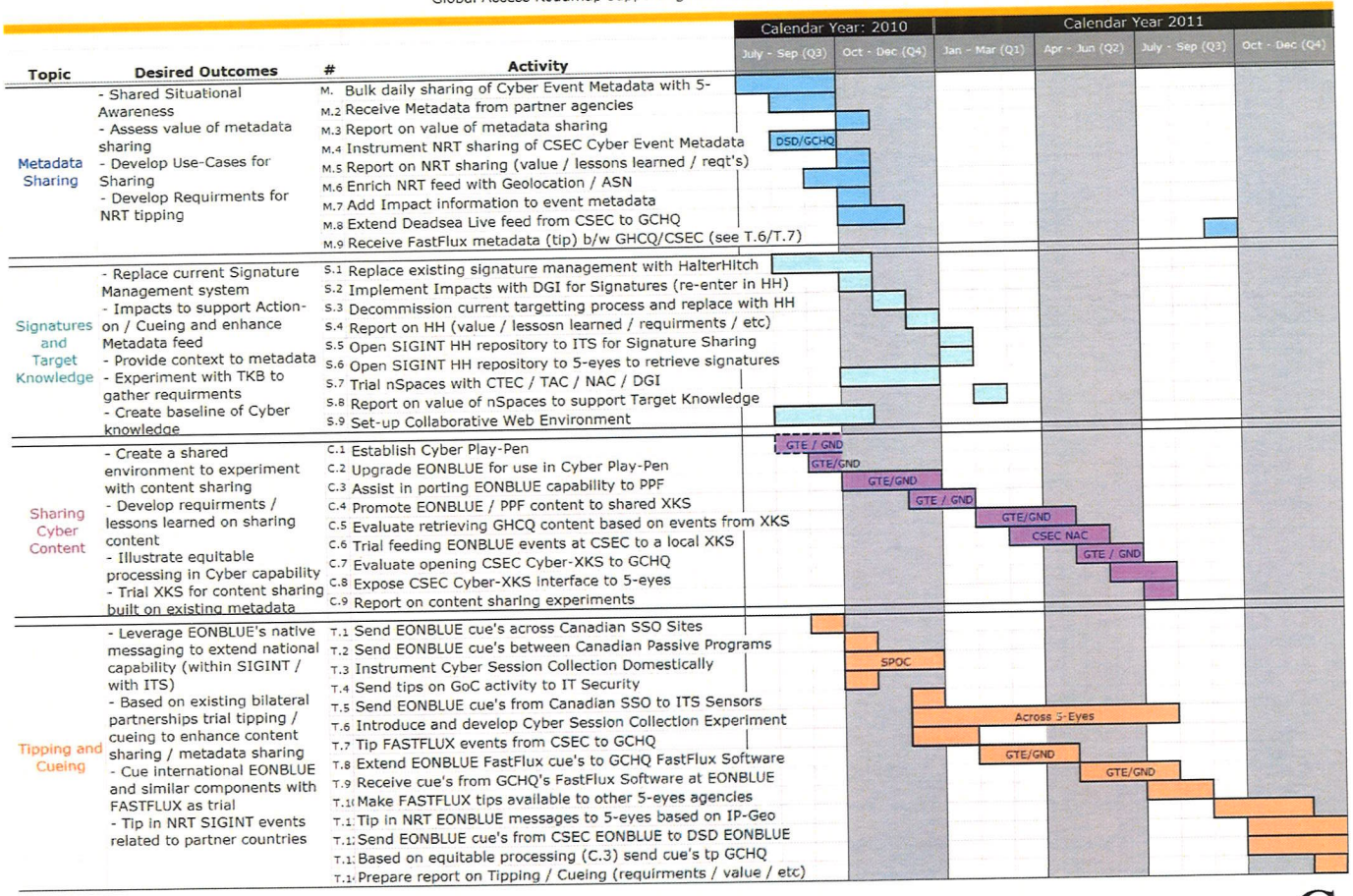
- QUANTUM
  - It's no lie, quantum is cool.
    - But its easy to find
  - Analyze first content carrying packet
    - Check for sequence number duplication, but different data size
    - If content differs within the first 10% of the pkt payload, alert.

What's Next?

- Anomaly Discovery at scale
  - Multi-10G anomaly detection
- Cross Agency communication of anomalies
  - Sometimes signatures aren't enough
- DONUTS!
  - Everyone likes them:
    - [redacted]
  - 5-eyes accessible DONUTS
    - Discovery of New Unidentified Threats
    - CSEC / GCHQ right now

CLASSIFICATION: TOP SECRET // COMINT // REL TO FVEY

Global Access Roadmap supporting SRSG and WISDEN Scenarios



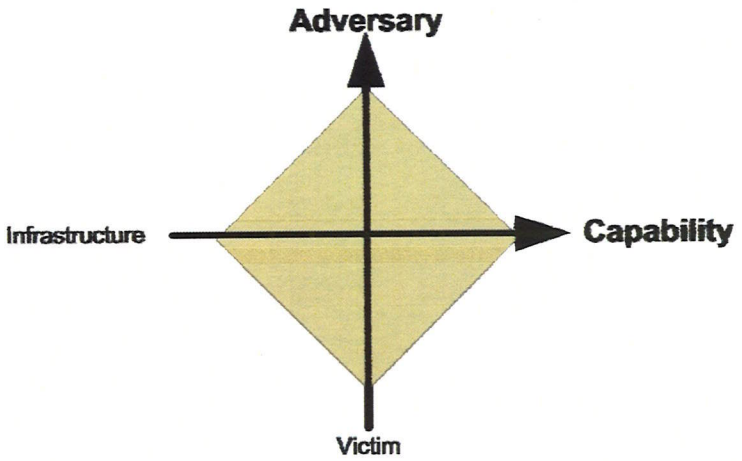
Topic	Desired Outcomes	#	Activity
Metadata Sharing	- Shared Situational Awareness - Assess value of metadata sharing - Develop Use-Cases for Sharing - Develop Requirments for NRT tipping	M.	Bulk daily sharing of Cyber Event Metadata with 5-
		M.2	Receive Metadata from partner agencies
		M.3	Report on value of metadata sharing
		M.4	Instrument NRT sharing of CSEC Cyber Event Metadata
		M.5	Report on NRT sharing (value / lessons learned / reqt's)
		M.6	Enrich NRT feed with Geolocation / ASN
		M.7	Add Impact information to event metadata
		M.8	Extend Deadsea Live feed from CSEC to GCHQ
		M.9	Receive FastFlux metadata (tip) b/w GHCQ/CSEC (see T.6/T.7)
Signatures and Target Knowledge	- Replace current Signature Management system - Impacts to support Action-on / Cueing and enhance Metadata feed - Provide context to metadata - Experiment with TKB to gather requirments - Create baseline of Cyber knowledge	S.1	Replace existing signature management with HalterHitch
		S.2	Implement Impacts with DGI for Signatures (re-enter in HH)
		S.3	Decommission current targetting process and replace with HH
		S.4	Report on HH (value / lessosn learned / requirments / etc)
		S.5	Open SIGINT HH repository to ITS for Signature Sharing
		S.6	Open SIGINT HH repository to 5-eyes to retrieve signatures
		S.7	Trial nSpaces with CTEC / TAC / NAC / DGI
		S.8	Report on value of nSpaces to support Target Knowledge
		S.9	Set-up Collaborative Web Environment
Sharing Cyber Content	- Create a shared environment to experiment with content sharing - Develop requirments / lessons learned on sharing content - Illustrate equitable processing in Cyber capability - Trial XKS for content sharing built on existing metadata	C.1	Establish Cyber Play-Pen
		C.2	Upgrade EONBLUE for use in Cyber Play-Pen
		C.3	Assist in porting EONBLUE capability to PPF
		C.4	Promote EONBLUE / PPF content to shared XKS
		C.5	Evaluate retrieving GHCQ content based on events from XKS
		C.6	Trial feeding EONBLUE events at CSEC to a local XKS
		C.7	Evaluate opening CSEC Cyber-XKS to GCHQ
		C.8	Expose CSEC Cyber-XKS Interface to 5-eyes
		C.9	Report on content sharing experiments
Tipping and Cueing	- Leverage EONBLUE's native messaging to extend national capability (within SIGINT / with ITS) - Based on existing bilateral partnerships trial tipping / cueing to enhance content sharing / metadata sharing - Cue international EONBLUE and similar components with FASTFLUX as trial - Tip in NRT SIGINT events related to partner countries	T.1	Send EONBLUE cue's across Canadian SSO Sites
		T.2	Send EONBLUE cue's between Canadian Passive Programs
		T.3	Instrument Cyber Session Collection Domestically
		T.4	Send tips on GoC activity to IT Security
		T.5	Send EONBLUE cue's from Canadian SSO to ITS Sensors
		T.6	Introduce and develop Cyber Session Collection Experiment
		T.7	Tip FASTFLUX events from CSEC to GCHQ
		T.8	Extend EONBLUE FastFlux cue's to GCHQ FastFlux Software
		T.9	Receive cue's from GCHQ's FastFlux Software at EONBLUE
		T.10	Make FASTFLUX tips available to other 5-eyes agencies
		T.11	Tip in NRT EONBLUE messages to 5-eyes based on IP-Geo
		T.12	Send EONBLUE cue's from CSEC EONBLUE to DSD EONBLUE
		T.13	Based on equitable processing (C.3) send cue's tp GCHQ
		T.14	Prepare report on Tipping / Cueing (requirments / value / etc)

CNT1 - Analysis

- Triage leads from K0G and GA4
  - Links to existing intrusion sets?
- Pursue interesting leads
  - Passive SIGINT collection
  - Technical analysis
- Produce reporting
- Attribute

Analytic Approach

1. Begin with lead
2. Apply to SIGINT
3. Apply to CCNE
4. Track, research and report
5. Generate persona lead
6. Coordinate with traditional CI



Cyber-Specifics of the Analytic Approach

Network Traffic Analysis

- We have access to Special Source, Warranted and 2nd Party collection in raw, unprocessed form
- Work very closely with protocol and crypt analysts

Malware Analysis and Reverse Engineering

- Samples are received through passive collection and human sources

Forensic Analysis

- Assist traditional CI investigations and others

CSEC Contacts

CCI (CNT1)

[redacted]@cse
[redacted]@cse
[redacted]@cse

ioops@cse-cst.gc.ca

CCNE (K0G)

[redacted]@cse
[redacted]@cse
[redacted]@cse

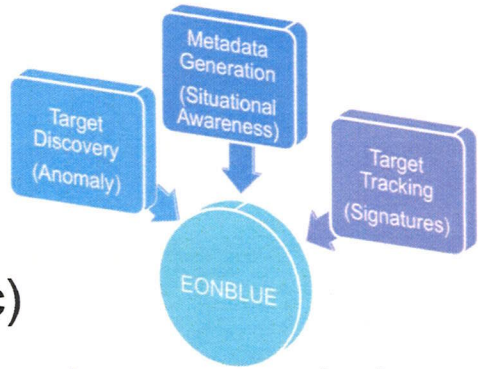
k0-ccne-dl@po.cse

GND (GA4)

[redacted]@cse
[redacted]@cse

ga4-staff@cse-cst.gc.ca

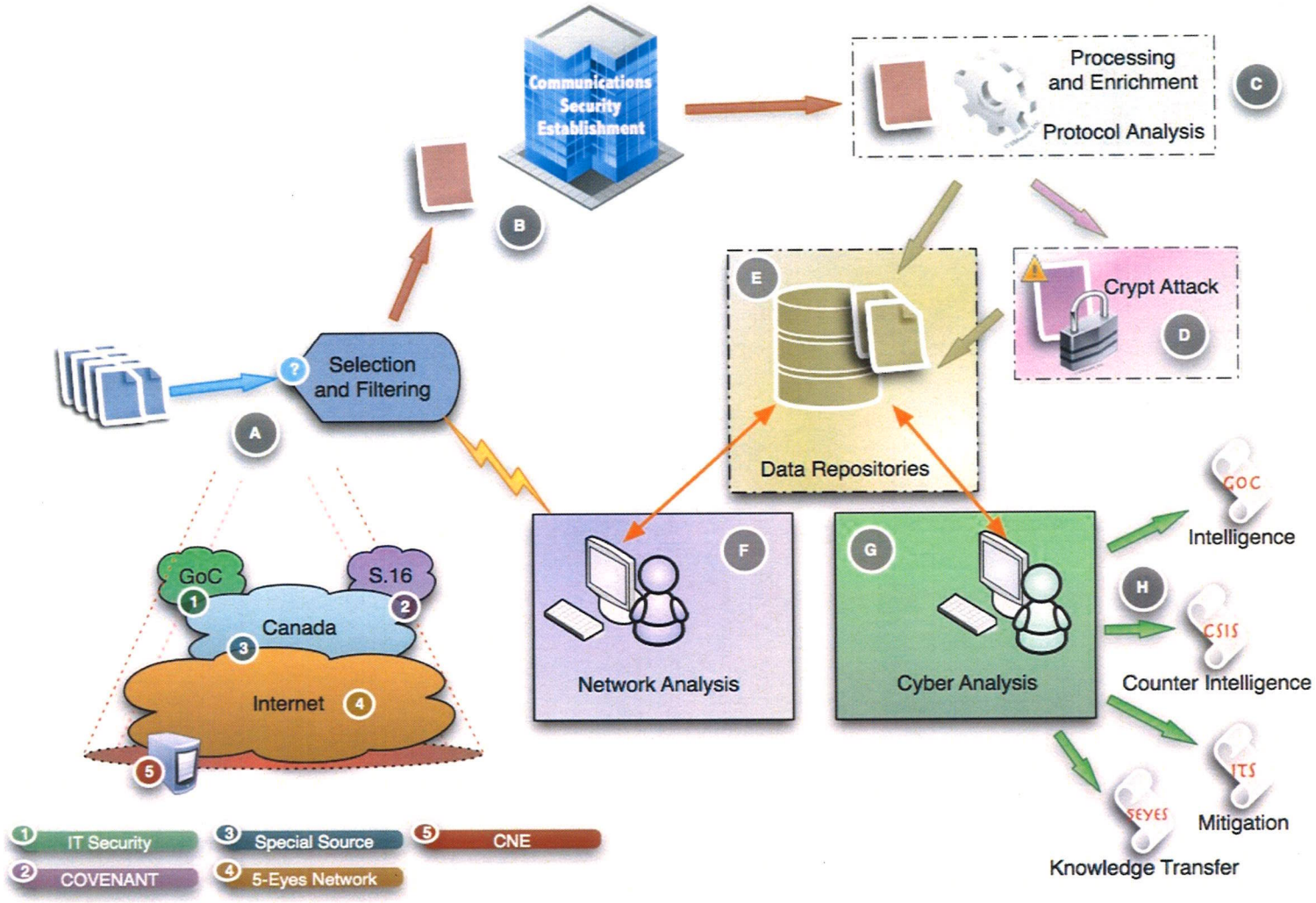
Cyber Threat Detection



- Passive Cyber Threat Detection Platform - EONBLUE
  - Currently deployed alongside traditional DNI Collection (SPECIALSOURCE, Warranted Access, FORNSAT, etc)
  - Packet Processing capability tailored to Cyber built over a 6+ year period
  - Cyber Threat Tracking (Deep Packet Inspection signatures for 'known' intrusions)
  - Cyber Threat Discovery (Anomaly Detection for discovering unknown intrusions)
- In 2009 an average of 115,000 Traffic Items collected daily from Canadian and Allied Sources
  - Collection from allies is crucial to success, but based on IP Address collection (causes over collect, sessionization corrupts data, difficult to analyze with Cyber toolkit)
- POC: [redacted] Global Network Detection [redacted]@cse-cst.gc.ca)

Canada

Holistic Cyber Threat Capability



Canada

Communications Security Establishment | Centre de la sécurité des télécommunications

CSEC – SIGINT Supporting CND

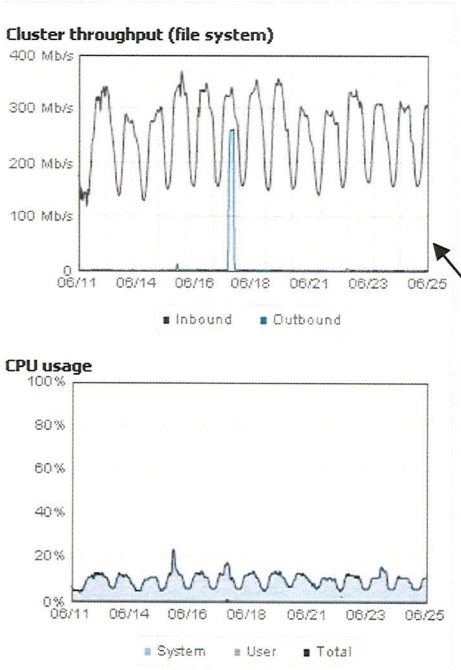
- Globally pervasive threat
  - Covered by 5-Eyes network
- Utilizing encryption
  - Subject to CSEC cryptographic attack
- Abusing telecommunications protocols
  - Understood and reverse engineered at CSEC
- Communicate using foreign languages
  - Access to CSEC and partner linguistic community
- Constantly changing modus operandi
  - Advanced signal processing analytics and anomaly detection
- Exfiltrate valuable intelligence
  - That we can collect and use to enhance our repositories
- These operations are also directed against GoC networks
  - Which we can detect and mitigate using both SIGINT and domestic sensors

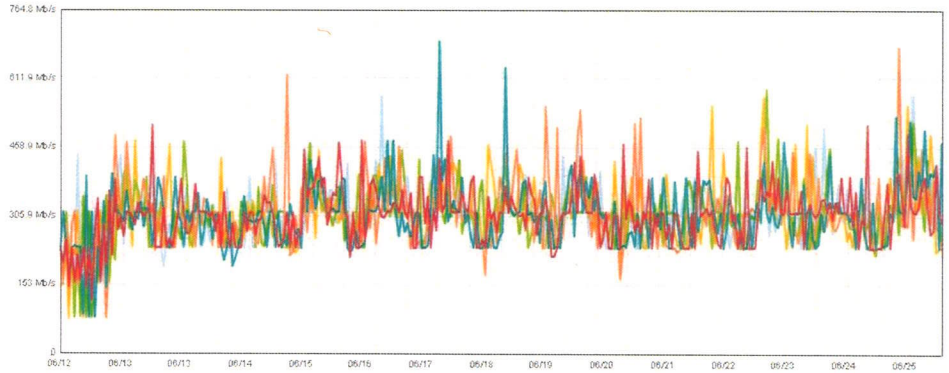
CSEC elements working as one … provides unparalleled situational awareness of the threat … monitors health and status of government networks … coupled with the ability to stop or mitigate attacks and intrusions directed against networks of importance to the GoC

Canada

Front-end Cyber Tradecraft

- Deployed high-speed clustered storage to our collection sites
  - Enables extraction / storing and processing of all HTTP metadata to identify Cyber Threat Anomalies
  - Leveraged by CSEC's network knowledge engine to facilitate DNS Response harvesting and de-duplication





Black Line: Total data into the Cluster
Blue Line: Data Outbound from SAN

Data deduplication at sight results in much better use of limited bandwidth

Data into the cluster is balanced across multiple nodes. Each color denotes a separate node, automatically dividing the load amongst all systems

Joint Capability Development

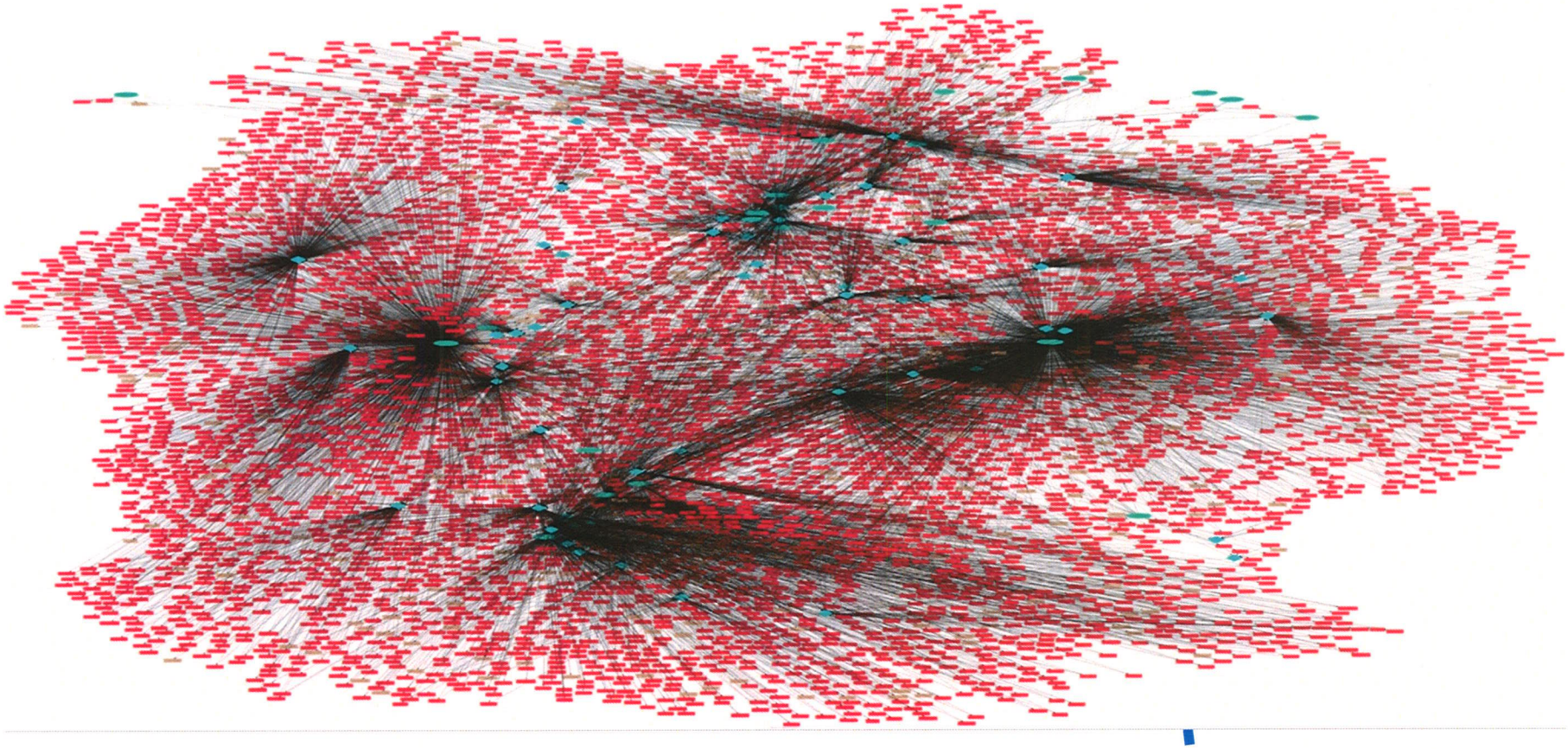
SIGINT / ITS – Cyber Threat Detection

- Fast Flux Botnet Detection – CROSSBOW
  - A target-discovery algorithm deployed at CSEC SSO sites (currently operational)
  - Detects botnets that use the DNS protocol for command and control (i.e. the technique runs exclusively on metadata)
  - Initial planning phase Tipping/Cueing trials between SIGINT/ITS and the 5Eyes (stand-alone source code has been shared with 5Eyes, i.e. through T3IO)
- "Throw-away" Cyber Threat Detection Sensor – CRUCIBLE
  - A low-cost, rapidly-deployed passive cyber threat detection sensor designed for use with TS//SI signatures in a non-SCIF environment (cyber target-tracking capability)
  - Strength of the sensor is derived primarily by the logical countermeasures (i.e. cryptographic hashes and bloom filters)
- POC: [redacted] DG ITS Operations ([redacted]@cse-cst.gc.ca)

Canada

Sample of Fast Flux Activity Detected

Square nodes: contacted by fast flux "bots"
Diamond nodes: fast flux "bots"
Oval nodes: suspected fast flux domain



1 week of detected fast flux activity for a particular fast flux domain at a CSEC access

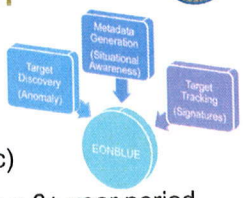
Joint Capability Development

SIGINT / ITS – Cyber Threat Detection

- Scanning Detection - LODESTONE
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

Communications Security Establishment | Centre de la sécurité des télécommunications

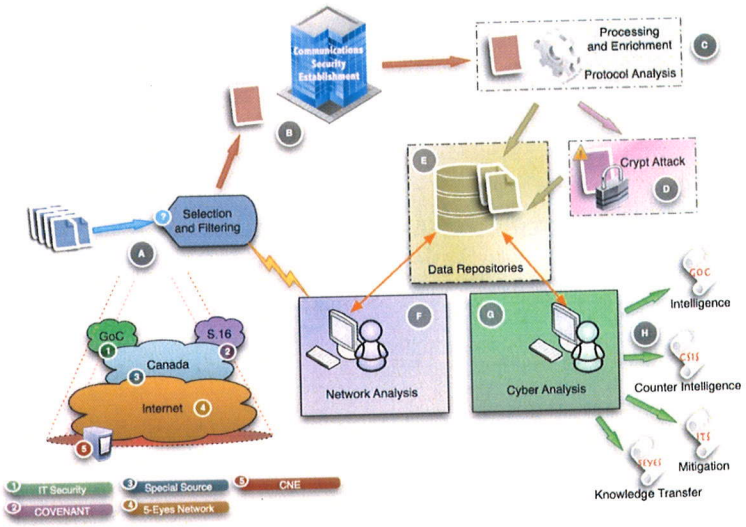
Cyber Threat Detection



- Passive Cyber Threat Detection Platform - EONBLUE
  - Currently deployed alongside traditional DNI Collection (SPECIALSOURCE, Warranted Access, FORNSAT, etc)
  - Packet Processing capability tailored to Cyber built over a 6+ year period
  - Cyber Threat Tracking (Deep Packet Inspection signatures for 'known' intrusions)
  - Cyber Threat Discovery (Anomaly Detection for discovering unknown intrusions)
- In 2009 an average of 115,000 Traffic Items collected daily from Canadian and Allied Sources
  - Collection from allies is crucial to success, but based on IP Address collection (causes over collect, sessionization corrupts data, difficult to analyze with Cyber toolkit)
- POC: [redacted] Global Network Detection ([redacted]@cse-cst.gc.ca)

Canada

Holistic Cyber Threat Capability



Canada

TOP SECRET//COMINT

Communications Security Establishment | Centre de la sécurité des télécommunications

CSEC – SIGINT Supporting CND

- Globally pervasive threat
  - Covered by 5-Eyes network
- Utilizing encryption
  - Subject to CSEC cryptographic attack
- Abusing telecommunications protocols
  - Understood and reverse engineered at CSEC
- Communicate using foreign languages
  - Access to CSEC and partner linguistic community
- Constantly changing modus operandi
  - Access to CSEC analytics and anomaly detection
- Exfiltrate valuable intelligence
  - That we can collect and use to enhance our repositories
- These operations are also directed against GoC networks
  - Which we can detect and mitigate using both SIGINT and domestic sensors

•CSEC elements working as one …

• provides unparalleled situational awareness of the threat

• monitors health and status of government networks

• coupled with the ability to stop or mitigate attacks and intrusions

directed against networks of importance to the GoC

Canada

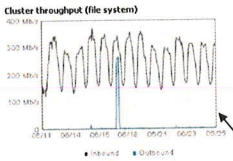
Speaker: [redacted]

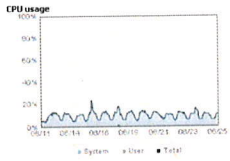
-Added the health and status of Government network bullet

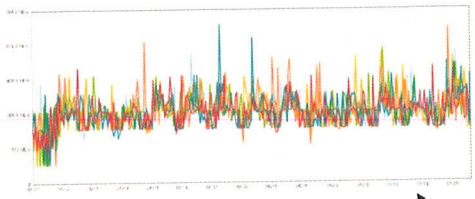
-Removed '4th party' and instead mention how it enhances our repositories (will introduce 4th party here)

Front-end Cyber Tradecraft

- Deployed high-speed clustered storage to our collection sites
  - Enables extraction / storing and processing of all HTTP metadata to identify Cyber Threat Anomalies
  - Leveraged by CSEC's network knowledge engine to facilitate DNS Response harvesting and de-duplication







Black Line: Total data into the Cluster
Blue Line: Data Outbound from SAN

Data deduplication at sight results in much better use of limited bandwidth

Data into the cluster is balanced across multiple nodes. Each color denotes a separate node, automatically dividing the load amongst all systems

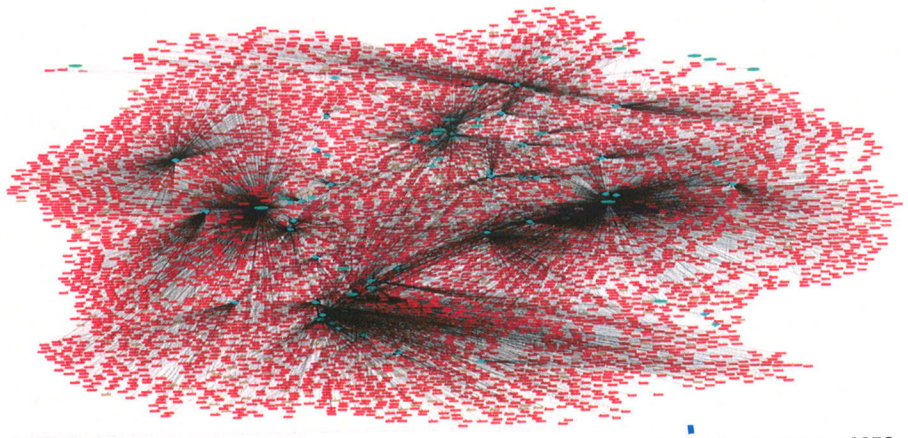
Joint Capability Development

SIGINT / ITS – Cyber Threat Detection

- Fast Flux Botnet Detection – CROSSBOW
  - A target-discovery algorithm deployed at CSEC SSO sites (currently operational)
  - Detects botnets that use the DNS protocol for command and control (i.e. the technique runs exclusively on metadata)
  - Initial planning phase Tipping/Cueing trials between SIGINT/ITS and the 5Eyes (stand-alone source code has been shared with 5Eyes, i.e. through T3IO)
- "Throw-away" Cyber Threat Detection Sensor – CRUCIBLE
  - A low-cost, rapidly-deployed passive cyber threat detection sensor designed for use with TS//SI signatures in a non-SCIF environment (cyber target-tracking capability)
  - Strength of the sensor is derived primarily by the logical countermeasures (i.e. cryptographic hashes and bloom filters)
- POC: [redacted] DG ITS Operations [redacted]@cse-cst.gc.ca)

Sample of Fast Flux Activity Detected

Square nodes: contacted by fast flux "bots"
Diamond nodes: fast flux "bots"
Oval nodes: suspected fast flux domain



1 week of detected fast flux activity for a particular fast flux domain at a CSEC access

Joint Capability Development

SIGINT / ITS – Cyber Threat Detection

- Scanning Detection - LODESTONE
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

CSEC Cyber Threat Capabilities

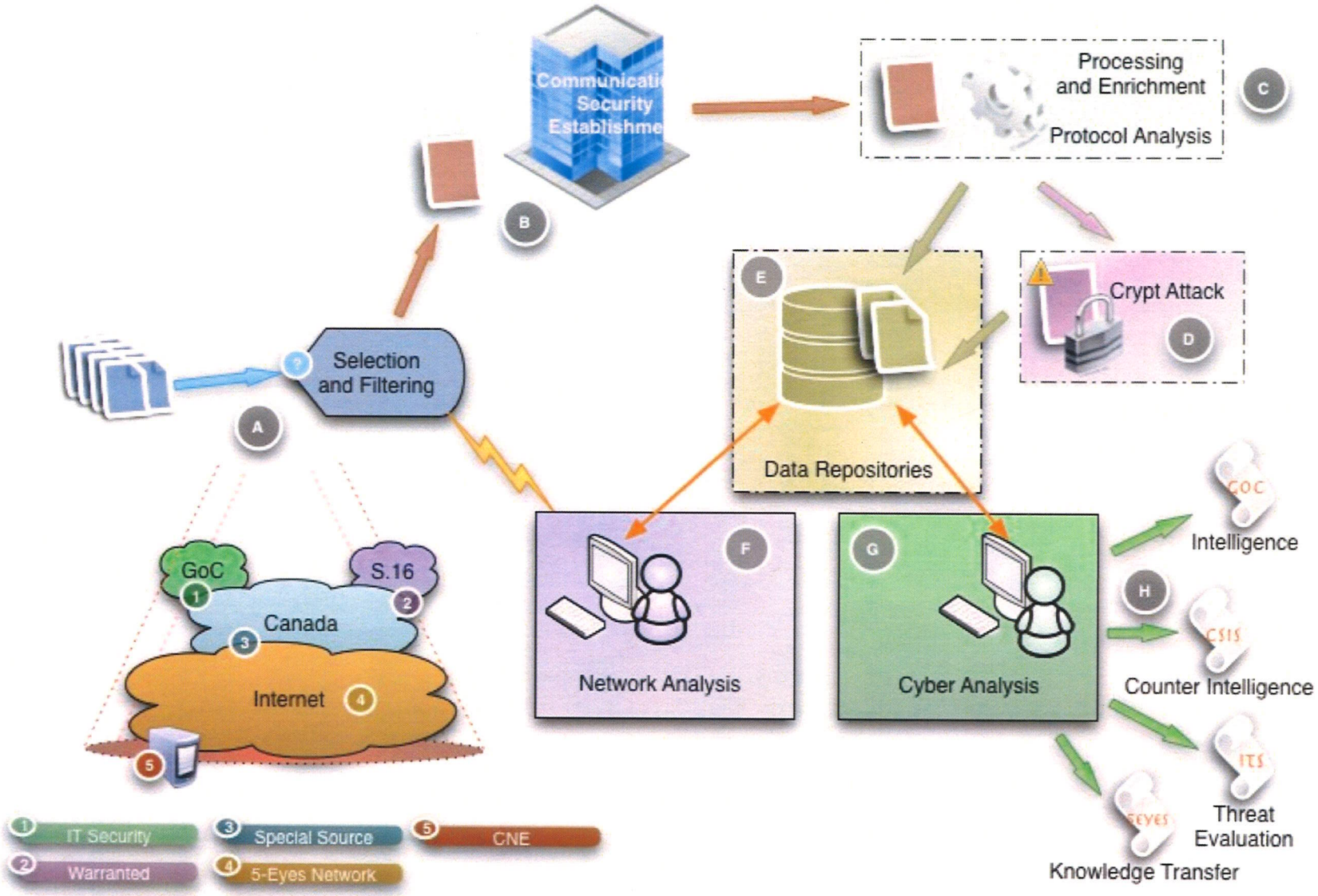
SIGINT and ITS: an end-to-end approach

Cyber Security

- What do we mean by Cyber?
  - Detection / Discovery and Tracking of State-Sponsored Hacking
  - Counter-Intelligence Reporting / Mitigation Advice and Defence against Cyber Threats

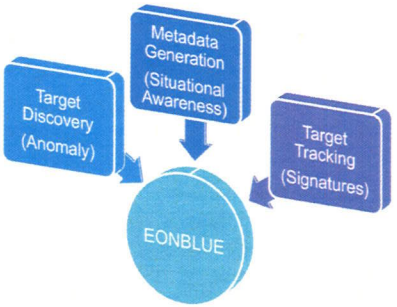
- SIGINT Detects Cyber Activity
  - Access Canadian and Allied collection to discover and track covert networks (counter-intelligence)
- IT Security Defends against Cyber Activity
  - Sensors Government of Canada networks to identify malicious activity and enhance defences

Comprehensive Cyber Capabilities



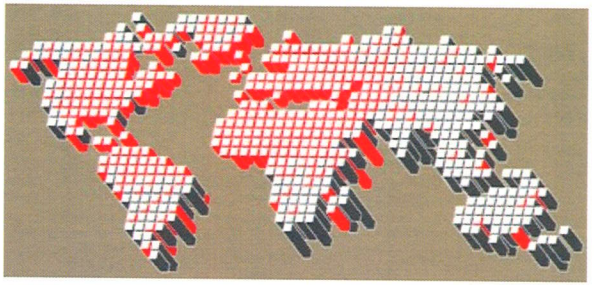
The Grand Challenge – Detection

- EONBLUE is the cyber threat detection sensor developed and deployed in SIGINT and ITS
  - Cyber threat tracking (signature-based detection)
  - Cyber threat discovery (anomaly-based detection)



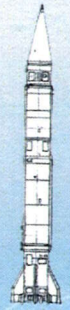
- A 6+ year effort that incorporates the best of breed detection algorithms/technology in collaboration with our 5-eyes partners
  - Based on classified knowledge
  - Scales to major ISP network speeds (10G)
  - Enables rapid prototyping to adapt to ever changing threats

The Cyber Landscape



- Adversaries and Targets
  - Operate globally
  - Varying degrees of sophistication
  - Constantly changing tools and techniques
- Detection / Discovery
  - Tools must operate at all network speeds
  - Deep Packet Inspection at scale
  - Targeting tradecraft / protocols vs. individuals
  - We must 'live' in cyber space

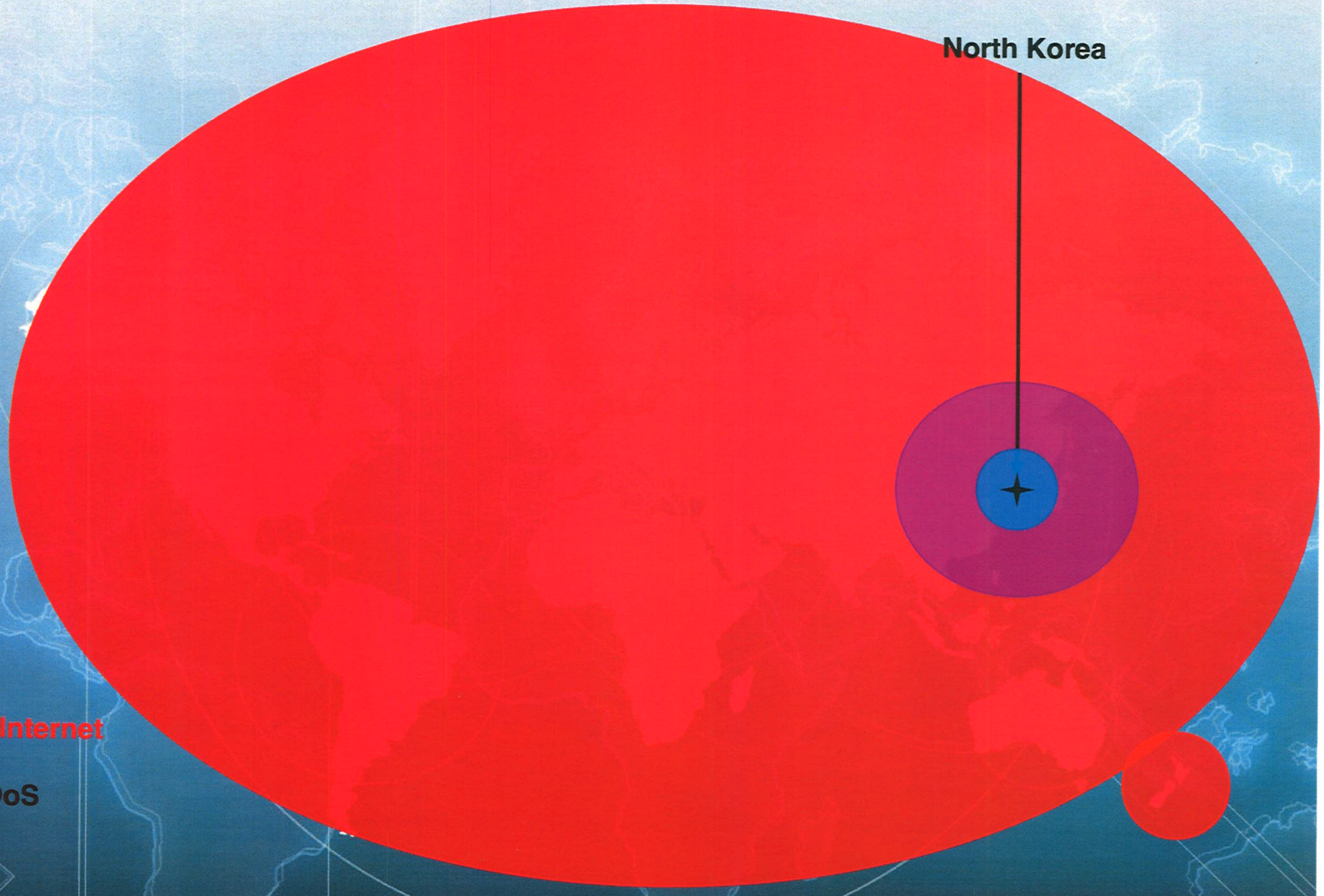
Why is Cyber Critical?



Nodong Missile
Range: 1300km
Type: Ballistic

Taepodong Missile
Range: 2900km
Type: Multistage
Payload: Nuclear

Desktop PC
Range: The Internet
Type: IBM
Payload: DDoS
Cost: 500$



Working in Cyber Space

- Tools must adapt constantly / quickly
  - Signature based targeting
  - Metadata analytics
  - Custom tradecraft for discovery

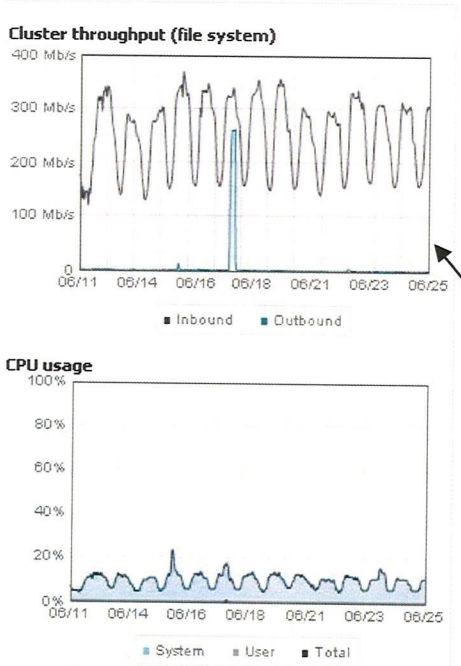
- Would I do a better job from my PC at home?
  - Enhance / Enable collaboration
  - Adopt Internet technologies on our Classified networks
    - SKYPE / Web 2.0 / Video Chat / Google Apps / etc
  - Centralize our 'cyber' analytics
    - CyberDMZ

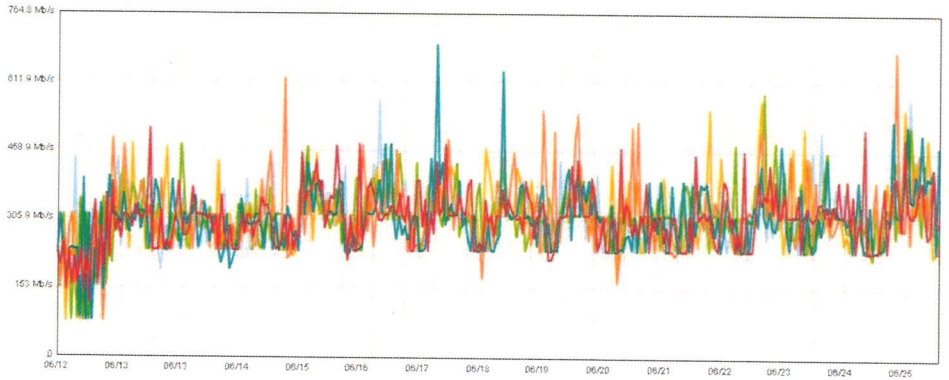
SEEDSPHERE - Discovery

- EONBLUE anomaly detection utilities isolate network anomalies
  - Discover network beacons in Warranted full-take collection
- Knowledge developed is shared with CNE
  - During CNE activities, implant is found to be cohabitating
  - Implant is copied to CSEC HQ for reverse engineering
- IT Security detects SEEDSPHERE attacks against Government of Canada weekly

Repositories – At Collection Site

- Global Access is pushing tradecraft to the front-end of access
  - 50 terabytes of high speed storage
  - Processing over 125GB/hour of HTTP metadata





Black Line: Total data into the Cluster
Blue Line: Data Outbound from SAN

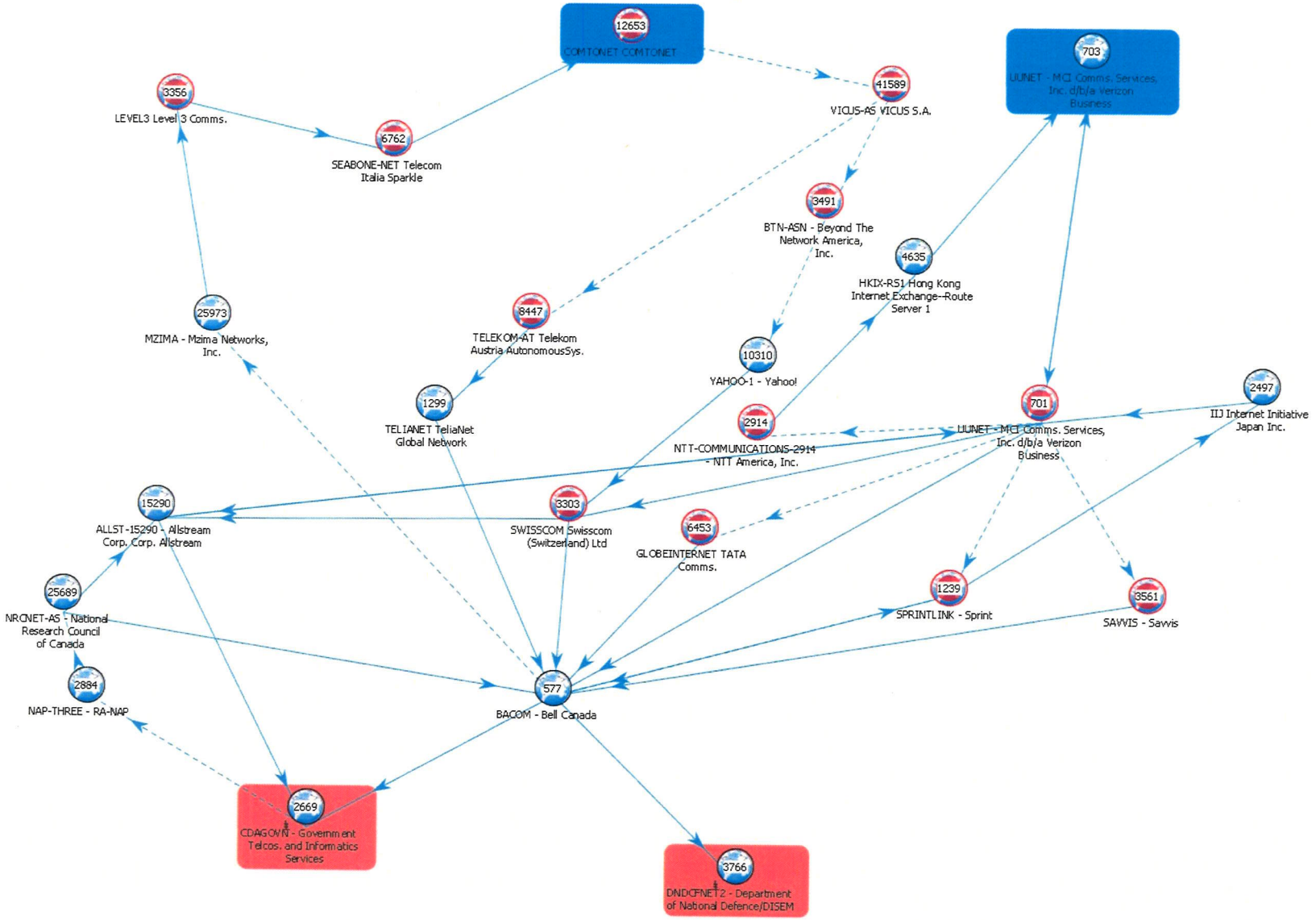
Data deduplication at sight results in much better use of limited bandwidth

Data into the cluster is balanced across multiple nodes. Each color denotes a separate node, automatically dividing the load amongst all systems

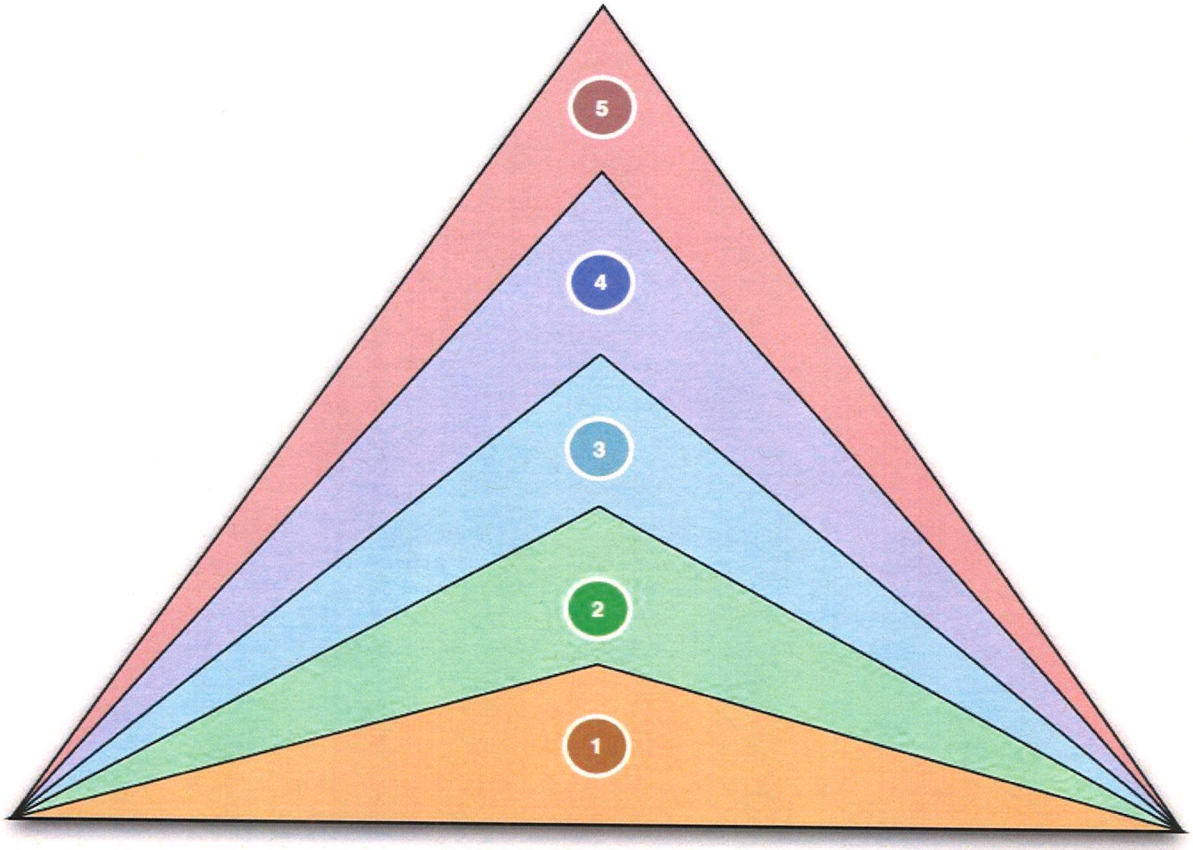
Cyber Repositories

- In 2009 an average of 112,794 IP traffic items related to cyber threat collected each day from Canadian and Allied sources
- Traditional SIGINT sources prove invaluable in cyber threat analysis
  - Travel Tracking Databases used to attribute CNE activity along with SMS collection
- IT Security domestic sensors store 300TB of full-take
  - Equivalent to 'months' of traffic
  - Enables historical analysis and anomaly detection
- In 2009 IT Security domestic sensors enable 95 mitigation actions

F: Network Analysis



Cyber Analysis



5 Cyber Report

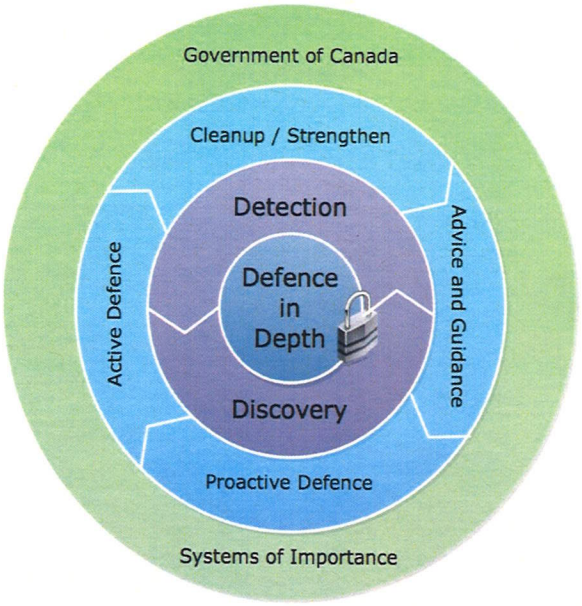
4 Network Analysis

3 Malware Reverse Engineering

2 Traffic Analysis

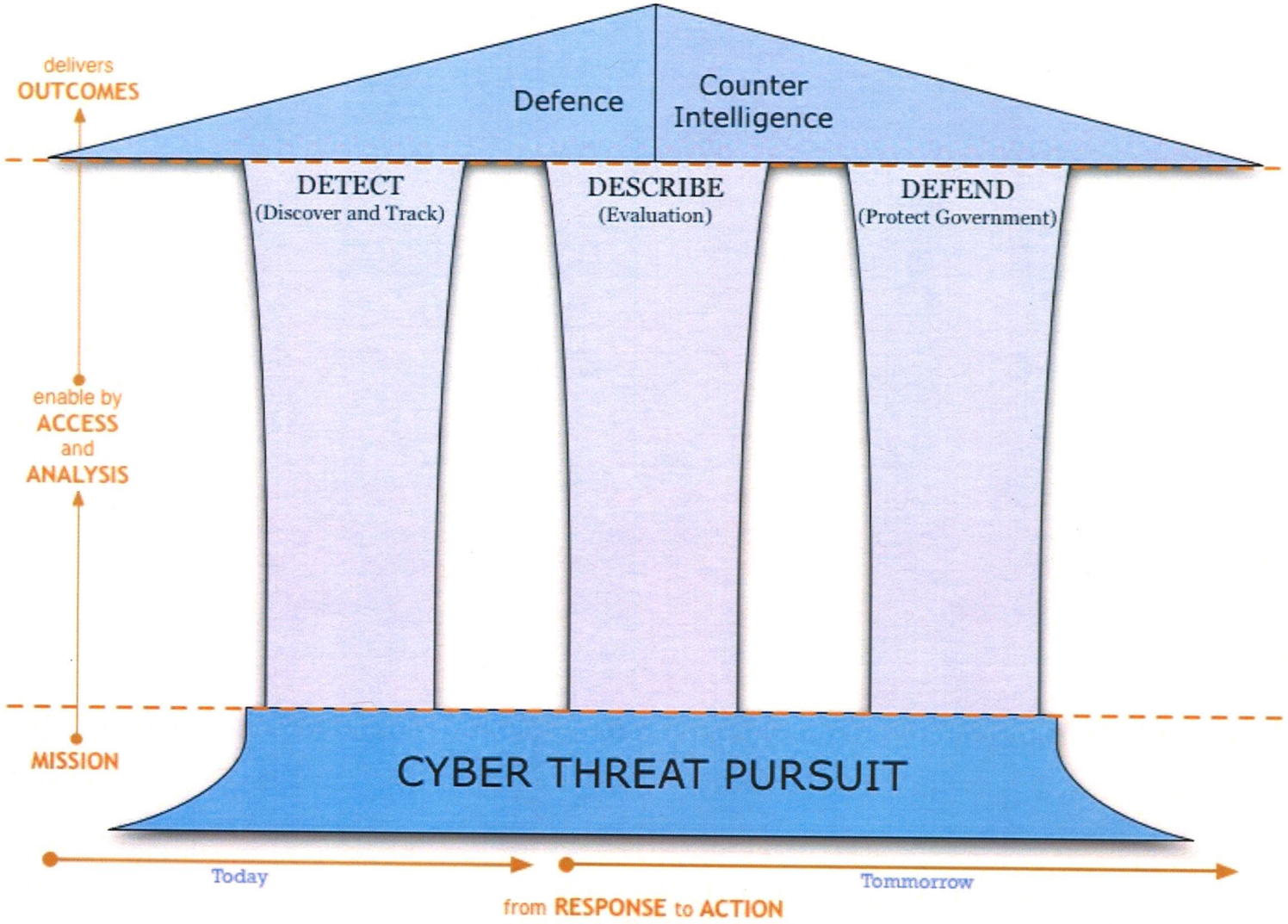
1 Tasking and Collection

Mitigation



- Direct protection of GC systems and information
  - Prevention and response activity
  - Leverage SIGINT and 5 Eyes intelligence, complemented by our own GC domestic sensor capabilities
  - Report:
    - Actionable technical mitigation reports provided to client's IPC
    - Cyber threat situational awareness reports provided to departments
  - CSEC review of incidents against systems of importance
  - CSEC analysts deployed to capture technical evidence to develop/support mitigation activity
  - CSEC information is merged with all-source cyber threat activities to create complete picture of cyber threats

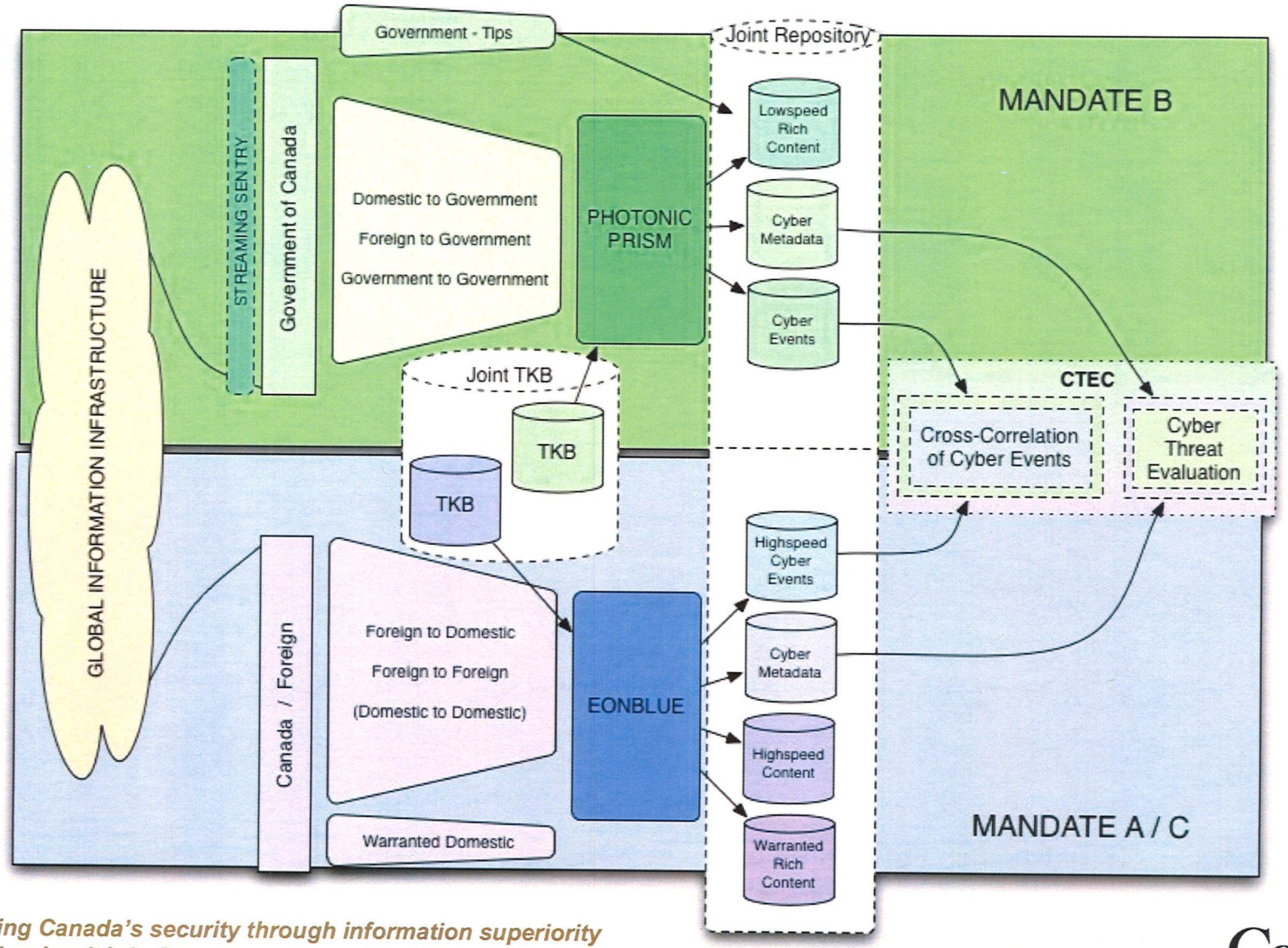
Positioning for the future



Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Synchronized SIGINT / ITS Mission Space



Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

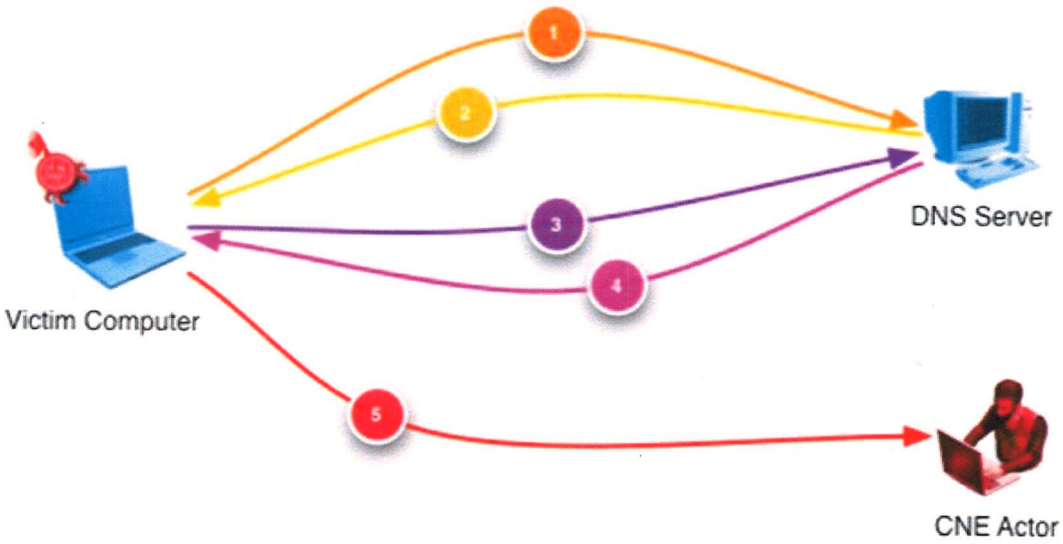
Canada

Situational Awareness

- SA is:
  - The perception of environmental elements within a volume of space and time
    - The comprehension of their meaning
    - Projection of their status in the near future
    - Insight – the capacity to understand hidden truths

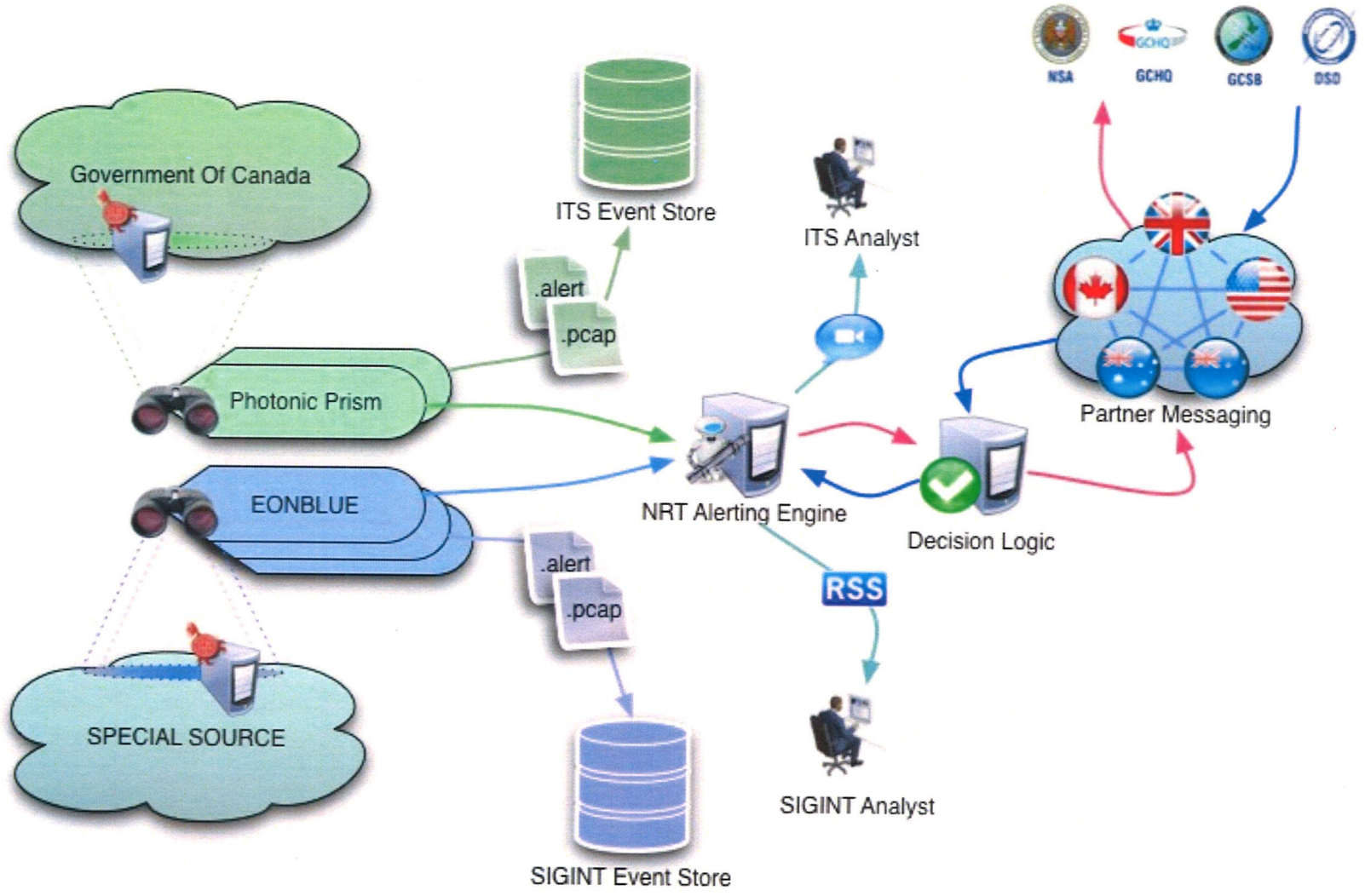
- In the Cyber Context:
  - Gathering and enabling access to cyber information
    - Event Metadata / Event Content / Near Real-Time Exchange
  - Data mining of cyber information to create understanding in broader context
  - Predict our adversaries actions based on this knowledge

Cyber Session Collection



1. Implant performs DNS Lookup for 'evilDomain.org'
2. DNS Server returns the value '127.0.0.1'; Implant remains idle
3. Implant performs DNS Lookup for 'evilDomain.org'
4. DNS Server returns the IP of CNE Actor Infrastructure
5. Implant connects to the CNE Actor infrastructure at IP returned in step 4

Enabled by Sydney Resolution



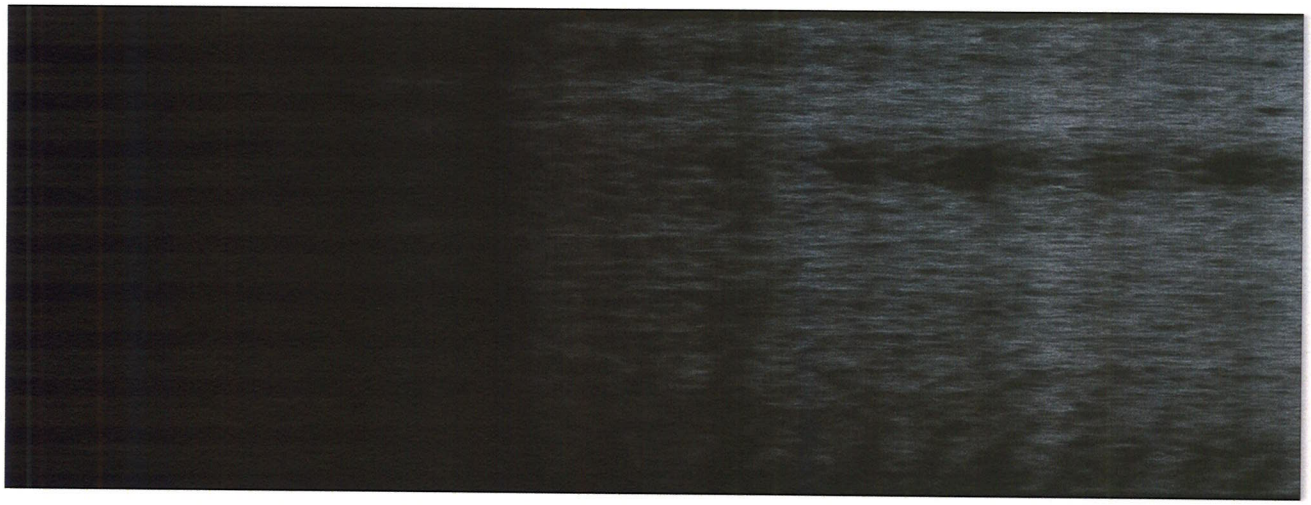
Tipping and Cueing (Why)

- SIGINT – data volumes/network speeds impose severe temporal restrictions on collection (use it or lose it)
  - ability to extend cyber target tracking across all 5-Eyes accesses and/or analytic event stores instead of just domestic – global aperture
  - ability to uncover covert overlay networks
  - cyber session collection? Uncover tradecraft/binaries/exploit vectors…
- CND - network edge vs. network core (microscope vs. telescope)
  - enable mitigation of cyber exploitation and/or attack (dynamic defence)
  - facilitate indications and warning – can SIGINT provide me with the true threat picture in NRT? Could we detect "test firing" of new tools/techniques?
  - collaborative defence – can my partners see malicious activity in SIGINT against networks I need to protect? Can they tell me in NRT?

SIGINT -> ITS Tipping

Sample of CNO tips provided to ITS from SIGINT SSO on May 05, 2010.

DS800| **SEEDSPHERE** -
DS800| **SEEDSPHERE** -
DS800| **SEEDSPHERE** -
DS800| **SEEDSPHERE** -
DS800| **SEEDSPHERE** -
DS800| **SEEDSPHERE** -
DS800| **SUPERDRAKE** -
DS800| **SEEDSPHERE** -
DS800| **SUPERDRAKE** -
DS800| **SEEDSPHERE** -



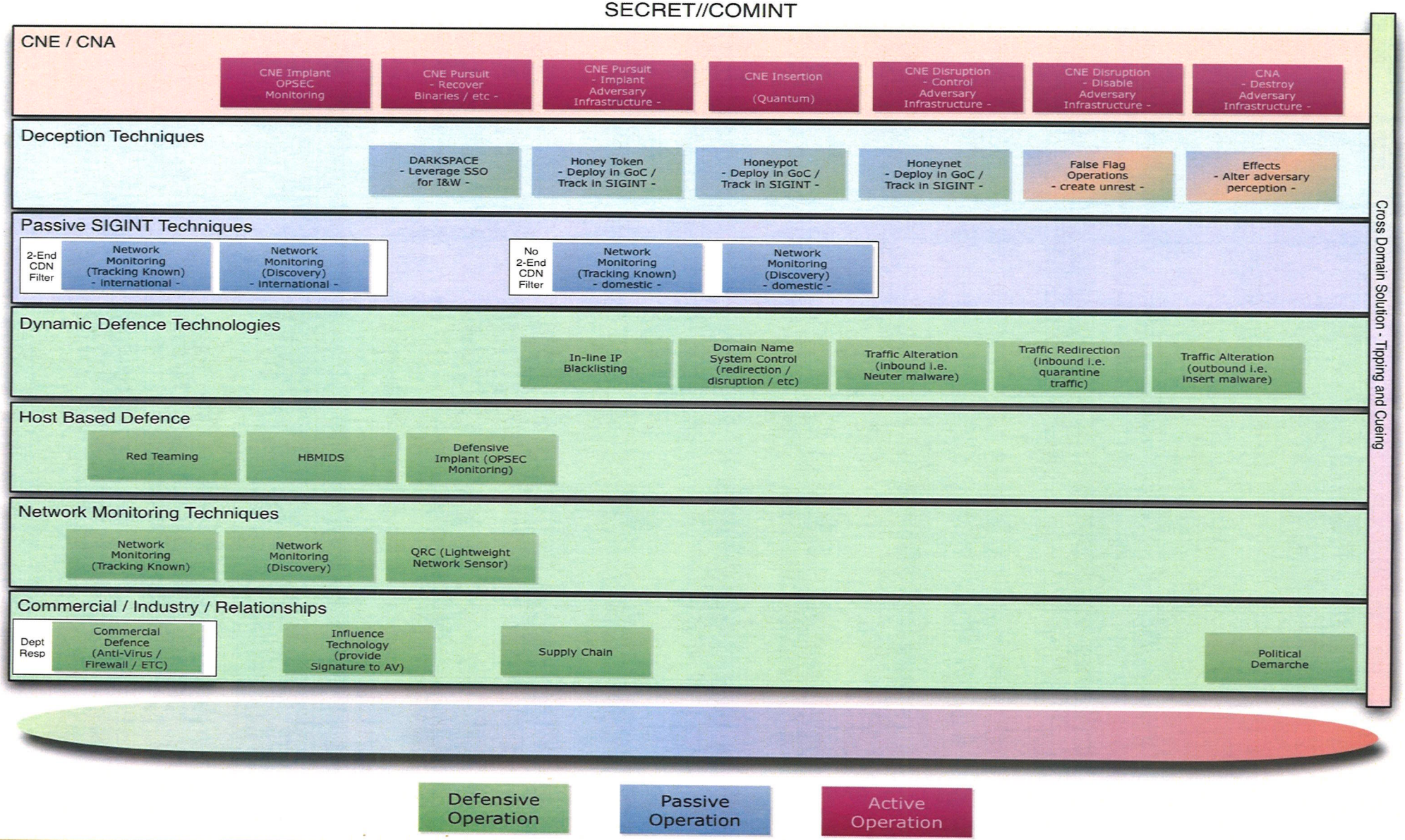
The Network Name is: canadian house of commons
The Network Name is: environment canada
The Network Name is: federal office of regional development (quebec)
The Network Name is: forestry canada
The Network Name is: public works and government services canada

Dynamic Defense

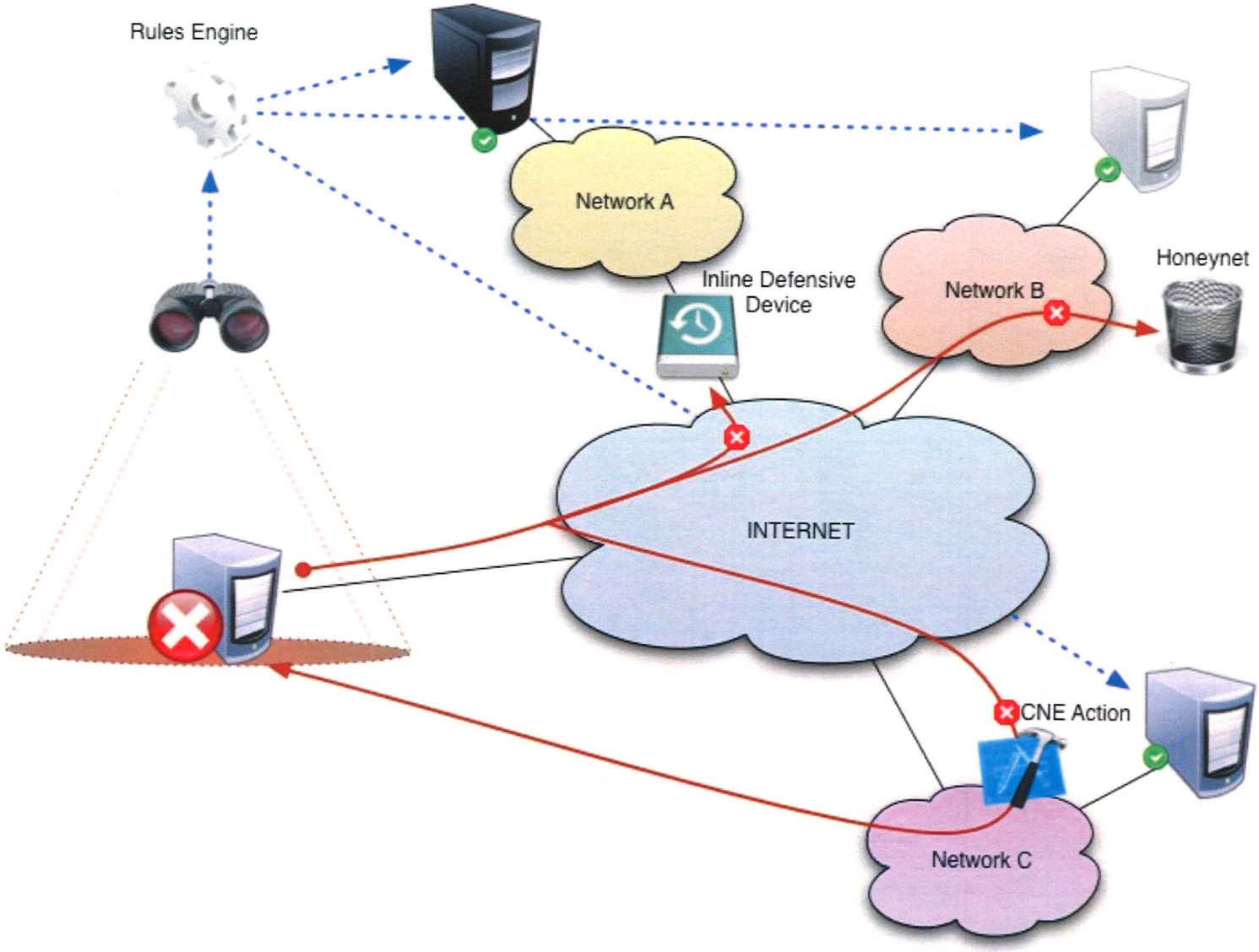
- All elements acting as one
- Defence at:
  - Network Edge (ITS)
    - Localized/tailored mitigation (e.g. blocking, binary neutering, redirection)
    - Focused response to ongoing and potential threats
  - Network Core (SIGINT)
    - Global mitigation possible (e.g. redirection, null routing, filtering)
    - Large scale (but still focused!) response to ongoing and potential threats
  - Adversary Space (CNE)
    - Reconnaissance – probe/explore/learn adversarial network space
    - Co-habitate covert network infrastructure for info gathering, tool extraction, etc

Cyber Activity Spectrum

SECRET//COMINT



Dynamic Defense Scenarios



Next Steps

Domestic

- Synchronize SIGINT and ITS Mission
- Alignment with Cyber Strategy
- Funding
- Joint Approach for Domestic Partners
- Recruitment and Staffing for Growth
- Joint Capabilities Development (Sensors and Analytics)

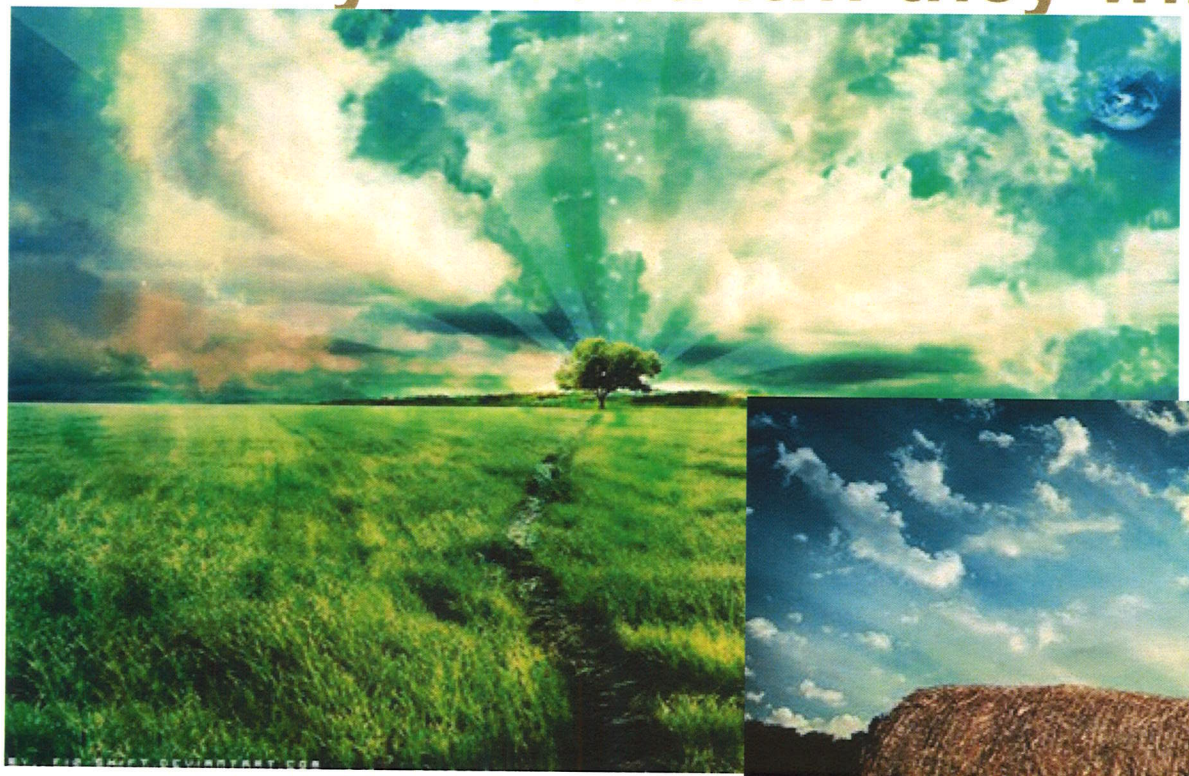
Consider

- Legislative Amendments
- Develop Career Framework

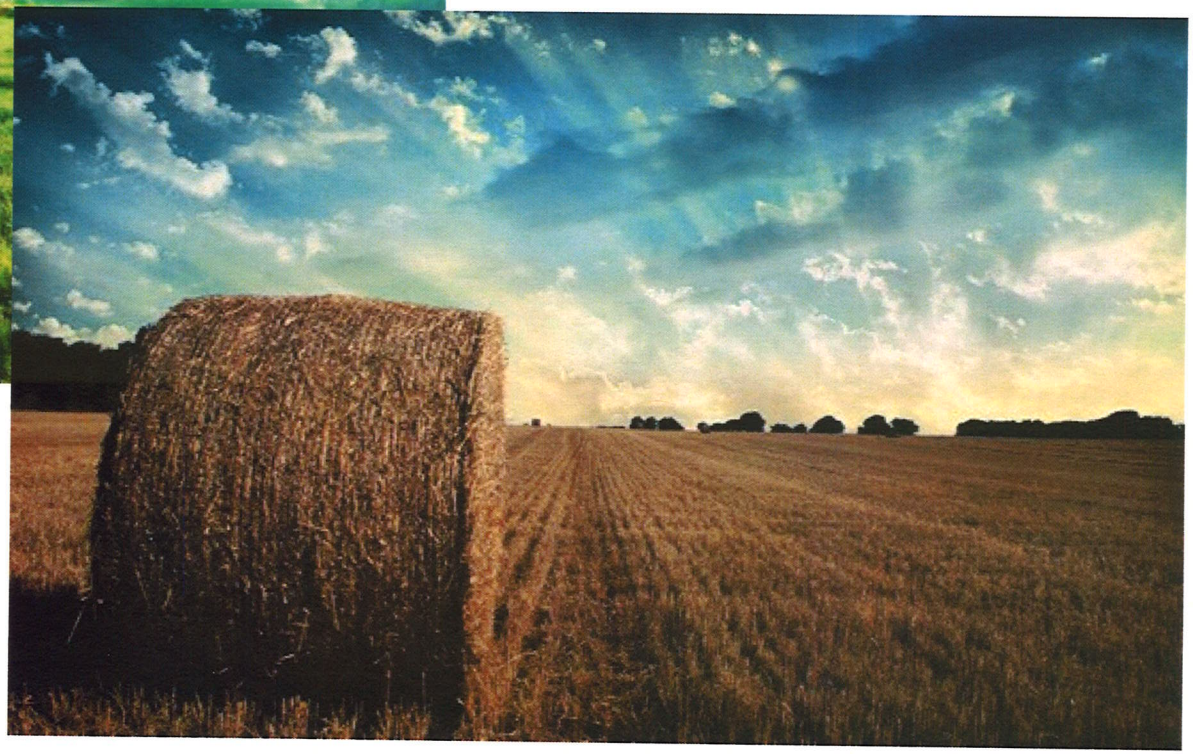
International

- Tipping and Cueing
- Interoperability
- Policy Coordination
- 5-Eyes Interoperability and Policy

If you build it… they will come



Rather
Than



CSEC Cyber Threat Capabilities

SIGINT and ITS: an end-to-end approach

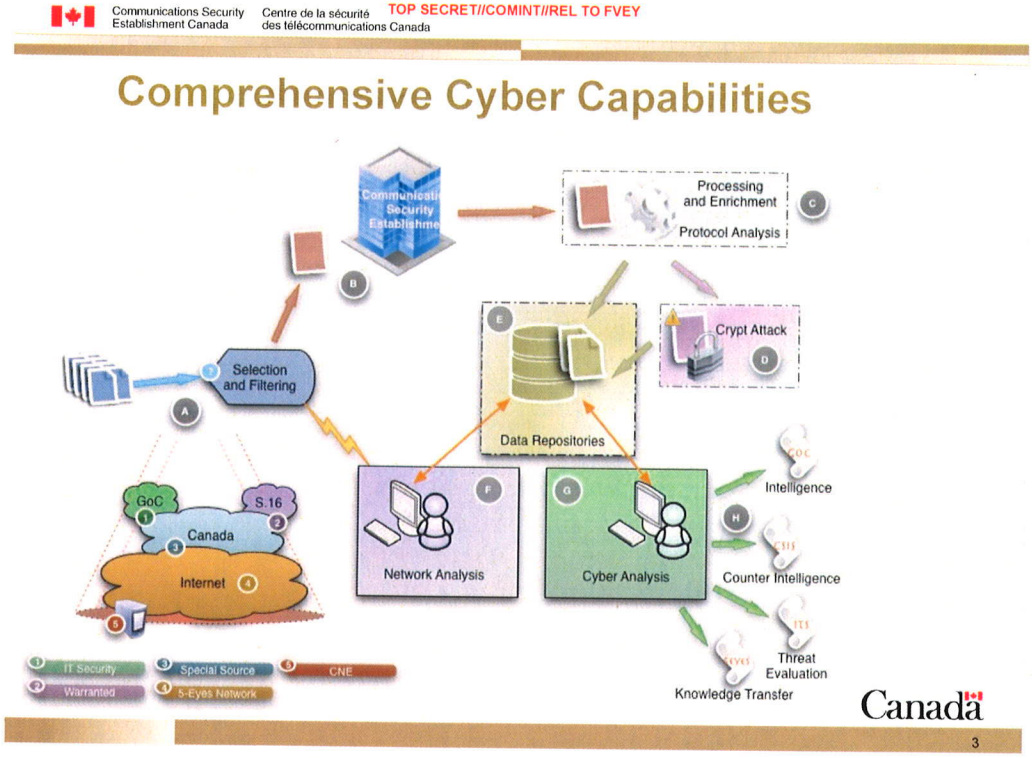
Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Cyber Security

- What do we mean by Cyber?
  - Detection / Discovery and Tracking of State-Sponsored Hacking
  - Counter-Intelligence Reporting / Mitigation Advice and Defence against Cyber Threats

- SIGINT Detects Cyber Activity
  - Access Canadian and Allied collection to discover and track covert networks (counter-intelligence)
- IT Security Defends against Cyber Activity
  - Sensors Government of Canada networks to identify malicious activity and enhance defences

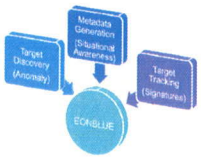


Speak: [redacted] (GA4)

- Added output to the 5-Eyes which is labelled as Knowledge Transfer (mention the sharing of tradecraft / techniques / tools / etc)
- Mention how analytic work load is split among parnters

The Grand Challenge – Detection

- EONBLUE is the cyber threat detection sensor developed and deployed in SIGINT and ITS
  - Cyber threat tracking (signature-based detection)
  - Cyber threat discovery (anomaly-based detection)



- A 6+ year effort that incorporates the best of breed detection algorithms/technology in collaboration with our 5-eyes partners
  - Based on classified knowledge
  - Scales to major ISP network speeds (10G)
  - Enables rapid prototyping to adapt to ever changing threats

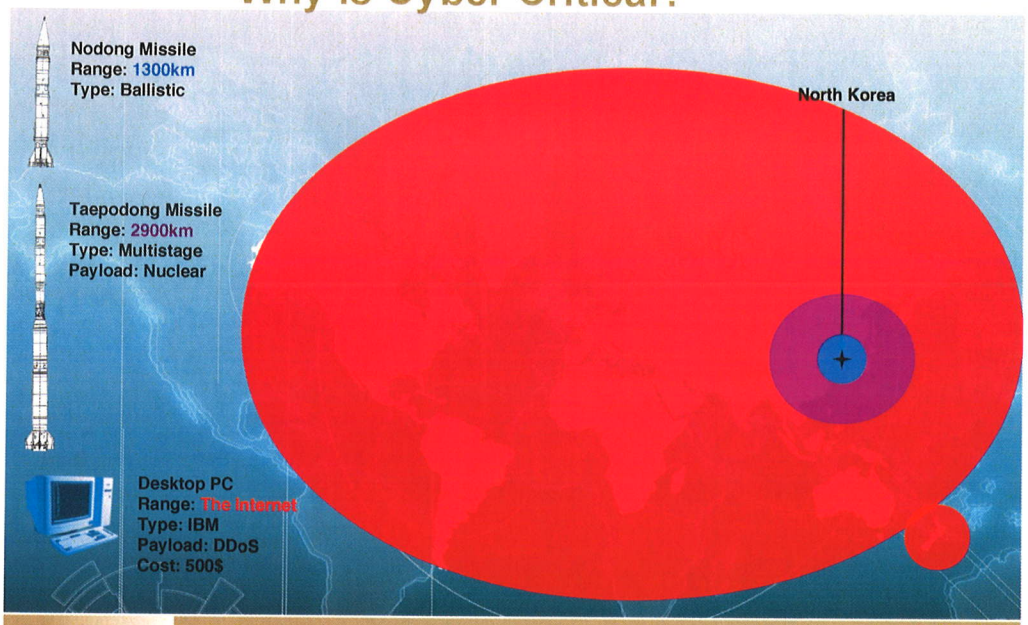
Speaker: [redacted] (ITS)

- Message is commercial is not enough

The Cyber Landscape

- Adversaries and Targets
  - Operate globally
  - Varying degrees of sophistication
  - Constantly changing tools and techniques
- Detection / Discovery
  - Tools must operate at all network speeds
  - Deep Packet Inspection at scale
  - Targeting tradecraft / protocols vs. individuals
  - We must 'live' in cyber space

Why is Cyber Critical?



Working in Cyber Space

- Tools must adapt constantly / quickly
  - Signature based targeting
  - Metadata analytics
  - Custom tradecraft for discovery

- Would I do a better job from my PC at home?
  - Enhance / Enable collaboration
  - Adopt Internet technologies on our Classified networks
    - SKYPE / Web 2.0 / Video Chat / Google Apps / etc
  - Centralize our 'cyber' analytics
    - CyberDMZ

SEEDSPHERE - Discovery

- EONBLUE anomaly detection utilities isolate network anomalies
  - Discover network beacons in Warranted full-take collection
- Knowledge developed is shared with CNE
  - During CNE activities, implant is found to be cohabitating
  - Implant is copied to CSEC HQ for reverse engineering
- IT Security detects SEEDSPHERE attacks against Government of Canada weekly

Speaker: [redacted]

-Major point: How it is an all-source collection effort to get the data

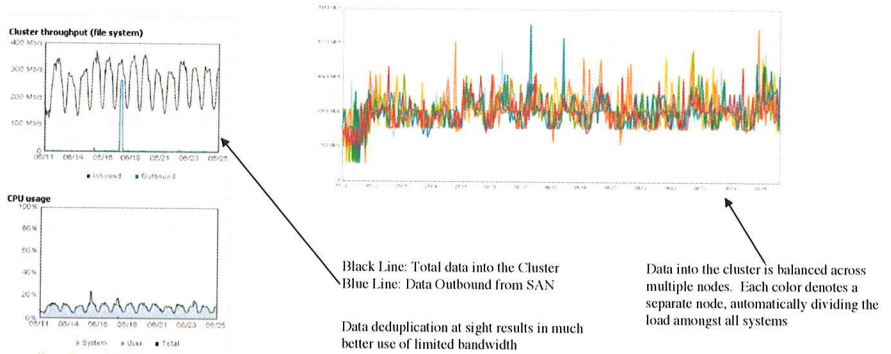
-Explain the value of COVENANT to seed new discovery

-How CNE is now seeding new discovery

-How ITS detects attacks into GC

Repositories – At Collection Site

- Global Access is pushing tradecraft to the front-end of access
  - 50 terabytes of high speed storage
  - Processing over 125GB/hour of HTTP metadata



Speaker: [redacted]

We are talking about the massive volumes (Reference to earlier SSO brief ng). There is so much traff c we keep it at the front-end and do advanced datamining / new tradecraft development

50TB = Library of Congress 3 times over

125GB of data = 14 Hours of High Def nition Video

SIGINT 2010 – Keep stuff online

Cyber Repositories

- In 2009 an average of 112,794 IP traffic items related to cyber threat collected each day from Canadian and Allied sources
- Traditional SIGINT sources prove invaluable in cyber threat analysis
  - Travel Tracking Databases used to attribute CNE activity along with SMS collection
- IT Security domestic sensors store 300TB of full-take
  - Equivalent to 'months' of traffic
  - Enables historical analysis and anomaly detection
- In 2009 IT Security domestic sensors enable 95 mitigation actions

Speaker: [redacted]

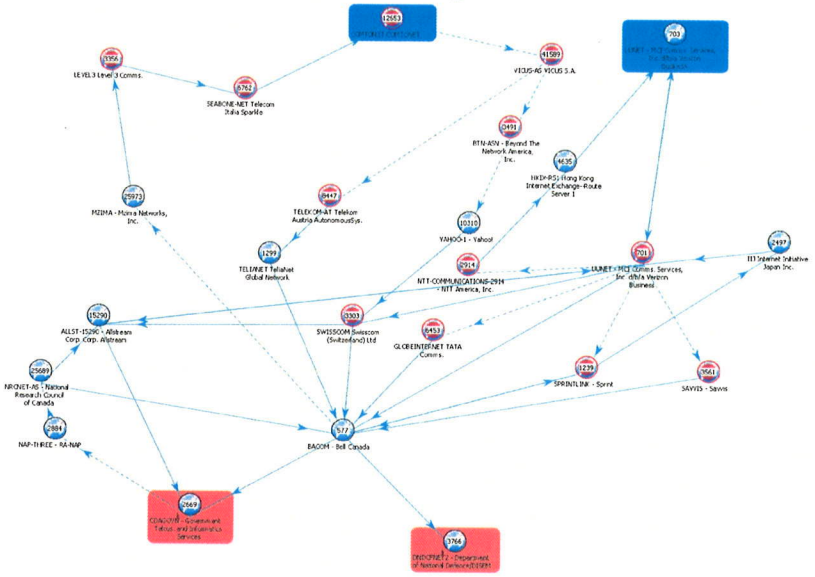
Major Point (Traffic breakdown is 70/30 for SIGINT)

Canadian Collect is almost all actionable

Canadian Collect is more precise because of EONBLUE

IT Security generates Mass quantity of valuable information on attacks (Linked to their fulltake capability)

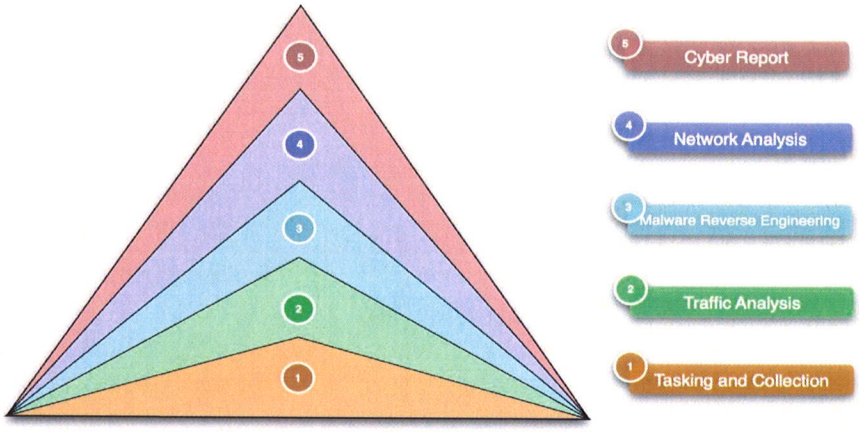
F: Network Analysis



Speaker: [redacted]

- Expand on how ANT provides best point of access (TBD)

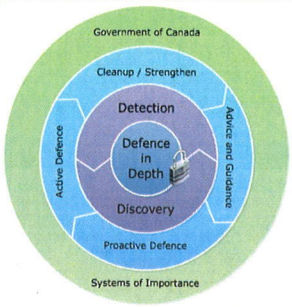
Cyber Analysis



Speaker: [redacted]

Major Points – A lot goes into a Cyber Threat Report We must stay on top of Tasking, Traffic Analysis / Reverse Engineering, Network Analysis all feed into a Cyber Report. We do this quickly because of tradecraft

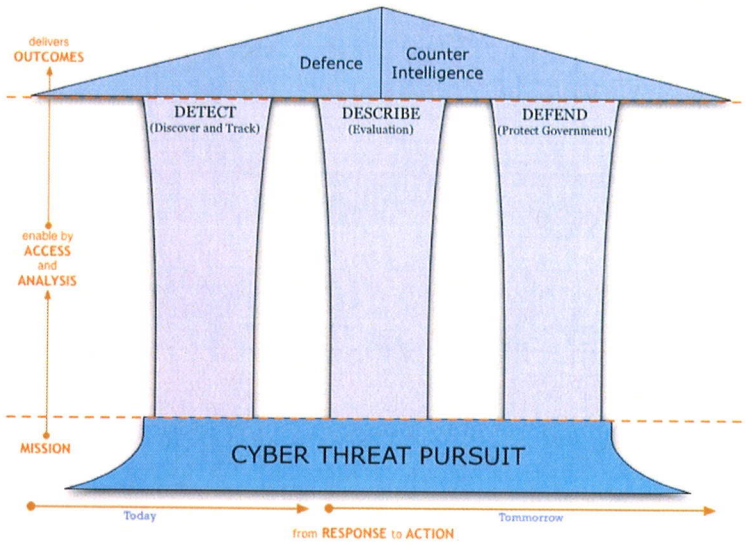
Mitigation



- Direct protection of GC systems and information
  - Prevention and response activity
  - Leverage SIGINT and 5 Eyes intelligence, complemented by our own GC domestic sensor capabilities
  - Report:
    - Actionable technical mitigation reports provided to client's IPC
    - Cyber threat situational awareness reports provided to departments
  - CSEC review of incidents against systems of importance
  - CSEC analysts deployed to capture technical evidence to develop/support mitigation activity
  - CSEC information is merged with all-source cyber threat activities to create complete picture of cyber threats

Speaker: [redacted]

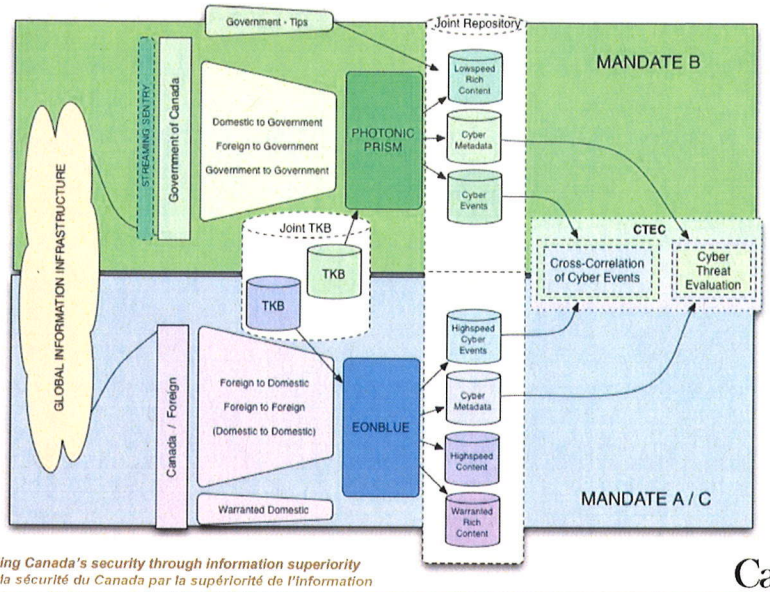
Positioning for the future



Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Synchronized SIGINT / ITS Mission Space



Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

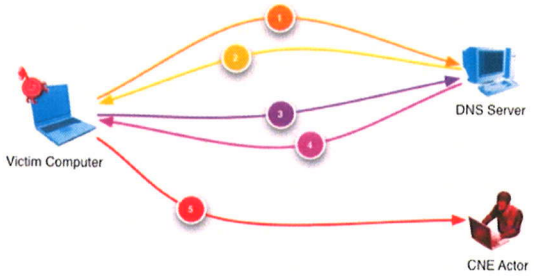
Canada

Situational Awareness

- SA is:
  - The perception of environmental elements within a volume of space and time
    - The comprehension of their meaning
    - Projection of their status in the near future
    - Insight – the capacity to understand hidden truths

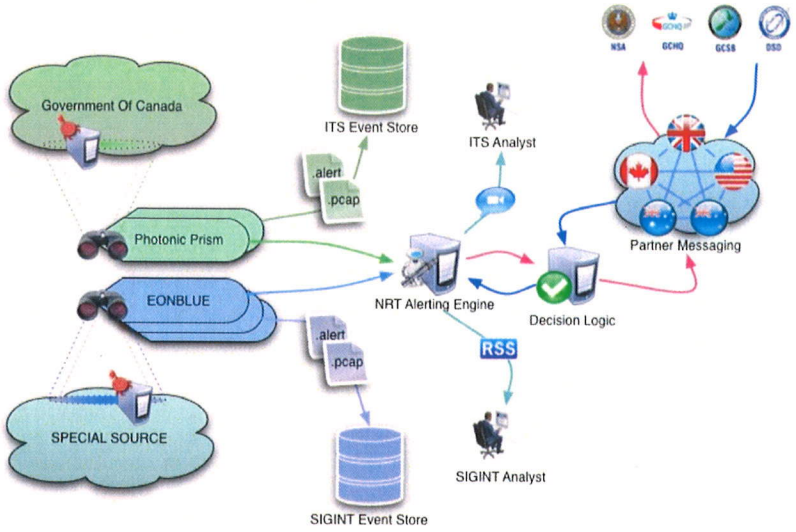
- In the Cyber Context:
  - Gathering and enabling access to cyber information
    - Event Metadata / Event Content / Near Real-Time Exchange
  - Data mining of cyber information to create understanding in broader context
  - Predict our adversaries actions based on this knowledge

Cyber Session Collection



1. Implant performs DNS Lookup for 'evilDomain.org'
2. DNS Server returns the value '127.0.0.1'; Implant remains idle
3. Implant performs DNS Lookup for 'evilDomain.org'
4. DNS Server returns the IP of CNE Actor Infrastructure
5. Implant connects to the CNE Actor infrastructure at IP returned in step 4

Enabled by Sydney Resolution



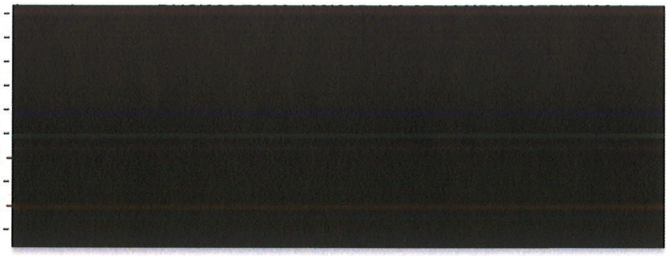
Tipping and Cueing (Why)

- SIGINT – data volumes/network speeds impose severe temporal restrictions on collection (use it or lose it)
  - ability to extend cyber target tracking across all 5-Eyes accesses and/or analytic event stores instead of just domestic – global aperture
  - ability to uncover covert overlay networks
  - cyber session collection? Uncover tradecraft/binaries/exploit vectors…
- CND - network edge vs. network core (microscope vs. telescope)
  - enable mitigation of cyber exploitation and/or attack (dynamic defence)
  - facilitate indications and warning – can SIGINT provide me with the true threat picture in NRT? Could we detect "test firing" of new tools/techniques?
  - collaborative defence – can my partners see malicious activity in SIGINT against networks I need to protect? Can they tell me in NRT?

SIGINT -> ITS Tipping

Sample of CNO tips provided to ITS from SIGINT SSO on May 05, 2010.

DS800| **SEEDSPHERE** -
DS800| **SEEDSPHERE** -
DS800| **SEEDSPHERE** -
DS800| **SEEDSPHERE** -
DS800| **SEEDSPHERE** -
DS800| **SEEDSPHERE** -
DS800| **SUPERDRAKE** -
DS800| **SEEDSPHERE** -
DS800| **SUPERDRAKE** -
DS800| **SEEDSPHERE** -



The Network Name is:	**canadian house of commons**
The Network Name is:	**environment canada**
The Network Name is:	**federal office of regional development (quebec)**
The Network Name is:	**forestry canada**
The Network Name is:	**public works and government services canada**

Dynamic Defense

- All elements acting as one
- Defence at:
  - Network Edge (ITS)
    - Localized/tailored mitigation (e.g. blocking, binary neutering, redirection)
    - Focused response to ongoing and potential threats
  - Network Core (SIGINT)
    - Global mitigation possible (e.g. redirection, null routing, filtering)
    - Large scale (but still focused!) response to ongoing and potential threats
  - Adversary Space (CNE)
    - Reconnaissance – probe/explore/learn adversarial network space
    - Co-habitate covert network infrastructure for info gathering, tool extraction, etc

National Security Agency/ Central Security Service

3 April 2013

Information Paper

Subject: (U//FOUO) NSA Intelligence Relationship with Canada's Communications Security Establishment Canada (CSEC)

(U) Introduction

(U//FOUO) The U.S.-Canada SIGINT relationship dates back to an alliance formed during World War II. In 1949, the relationship was formalized under the CANUSA Agreement signed with CSEC. The basic tenet of CANUSA is cooperation in all aspects of SIGINT except when considered prejudicial to the national interests of one of the parties. The formal Information Assurance (IA) relationship with CSEC is based on a 1986 Memorandum of Agreement. NSA has a close, cooperative relationship with CSEC that both sides would like to see expanded and strengthened.

(S//REL TO USA, CAN)) CSEC is a highly valued second party partner. The relationship is driven by our mutual interest in the defense of North America as a whole. Cooperative efforts include the exchange of liaison officers and integrees, joint projects, shared activities and a strong desire for closer collaboration in the area of cyber defense. Since Canada has a limited ability to produce cryptographic devices, it is a large consumer of U.S. IA products.

(C//REL TO USA, FVEY) [redacted] NSA civilian, guides the continued success of the CANUSA relationship in Canada. [redacted] staff have a close working relationship with [redacted] Together they enable productive interactions with Canadian intelligence organizations in support of U.S. Intelligence Community goals.

(U) Key Issues: NSA and CSEC cooperate closely in the following areas:

- (TS//SI//REL TO USA, CAN) active computer network access and exploitation on a variety of foreign intelligence targets, including CT, Middle East, North Africa, Europe, and Mexico;
- (U//FOUO) information assurance and critical infrastructure defense; and
- (U//FOUO) evolving cyber capabilities and network security standards.

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380401

(U) What NSA provides to the partner:

(S//SI//REL TO USA, CAN) SIGINT: NSA and CSEC cooperate in targeting approximately 20 high-priority countries [redacted]. NSA shares technological developments, cryptologic capabilities, software and resources for state-of-the-art collection, processing and analytic efforts, and IA capabilities. The intelligence exchange with CSEC covers worldwide national and transnational targets. No Consolidated Cryptologic Program (CCP) money is allocated to CSEC, but NSA at times pays R&D and technology costs on shared projects with CSEC.

[redacted]

(U) What the partner provides to NSA:

(TS//SI///REL TO USA, CAN) CSEC offers resources for advanced collection, processing and analysis, and has opened covert sites at the request of NSA. CSEC shares with NSA their unique geographic access to areas unavailable to the U.S. [redacted], and provides cryptographic products, cryptanalysis, technology, and software. CSEC has increased its investment in R&D projects of mutual interest. [redacted]

[redacted]