CSEC Cyber Threat Capabilities

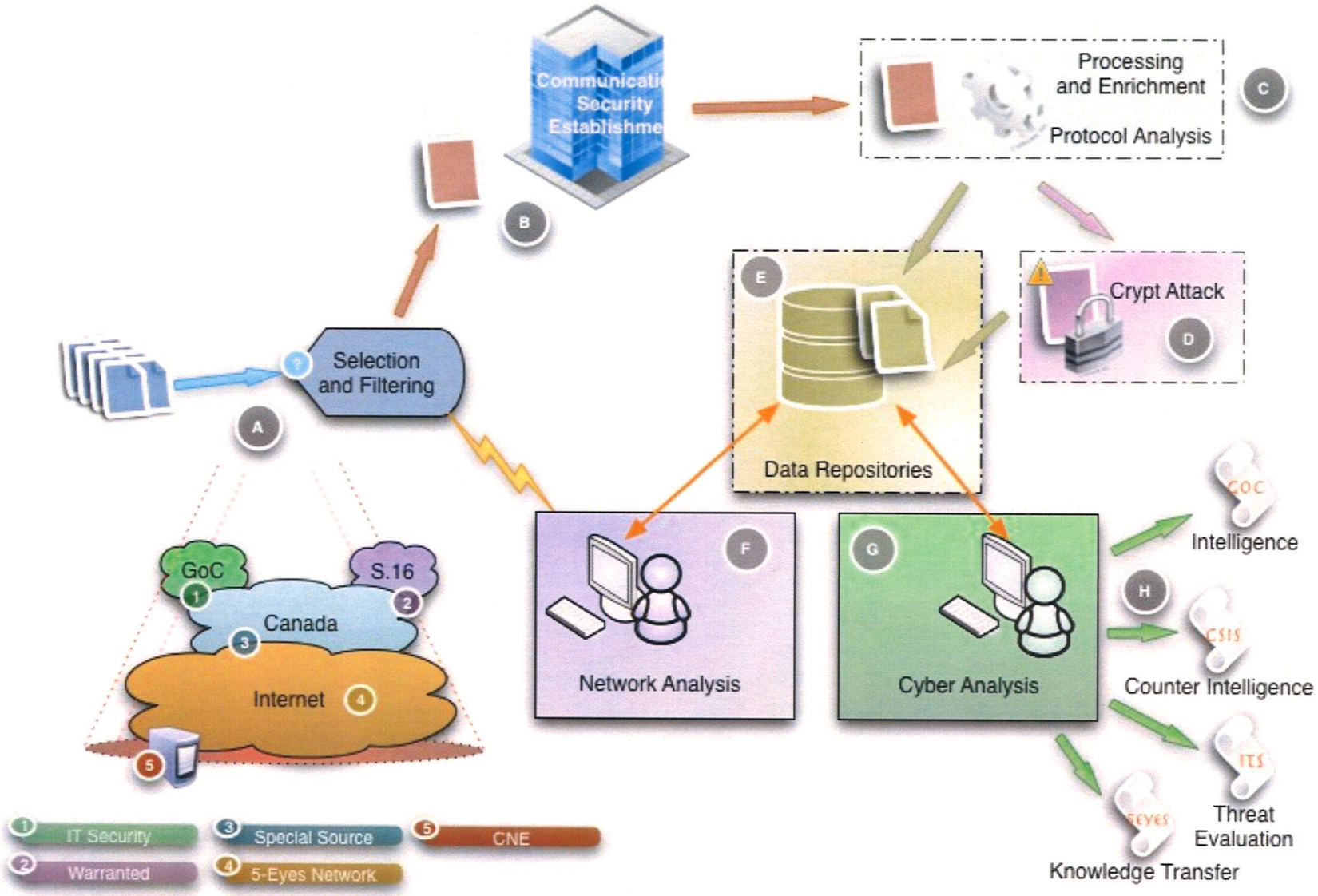
SIGINT and ITS: an end-to-end approach

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

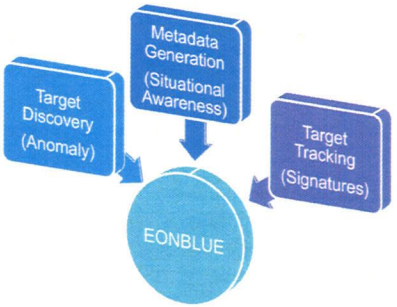
- SIGINT Detects Cyber Activity
  - Access Canadian and Allied collection to discover and track covert networks (counter-intelligence)
- IT Security Defends against Cyber Activity
  - Sensors Government of Canada networks to identify malicious activity and enhance defences

Comprehensive Cyber Capabilities



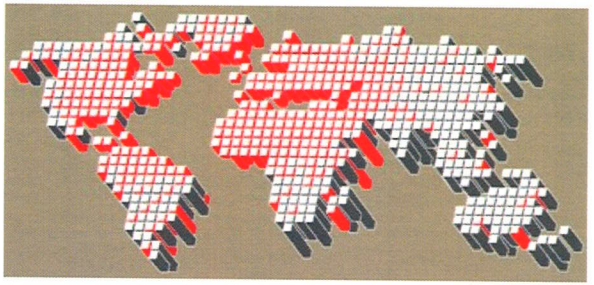
The Grand Challenge – Detection

- 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)



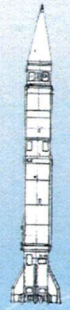
- A 6+ year effort that incorporates the best of breed detection algorithms/technology in collaboration with our 5-eyes partners
  - Based on classified knowledge
  - Scales to major ISP network speeds (10G)
  - Enables rapid prototyping to adapt to ever changing threats

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?



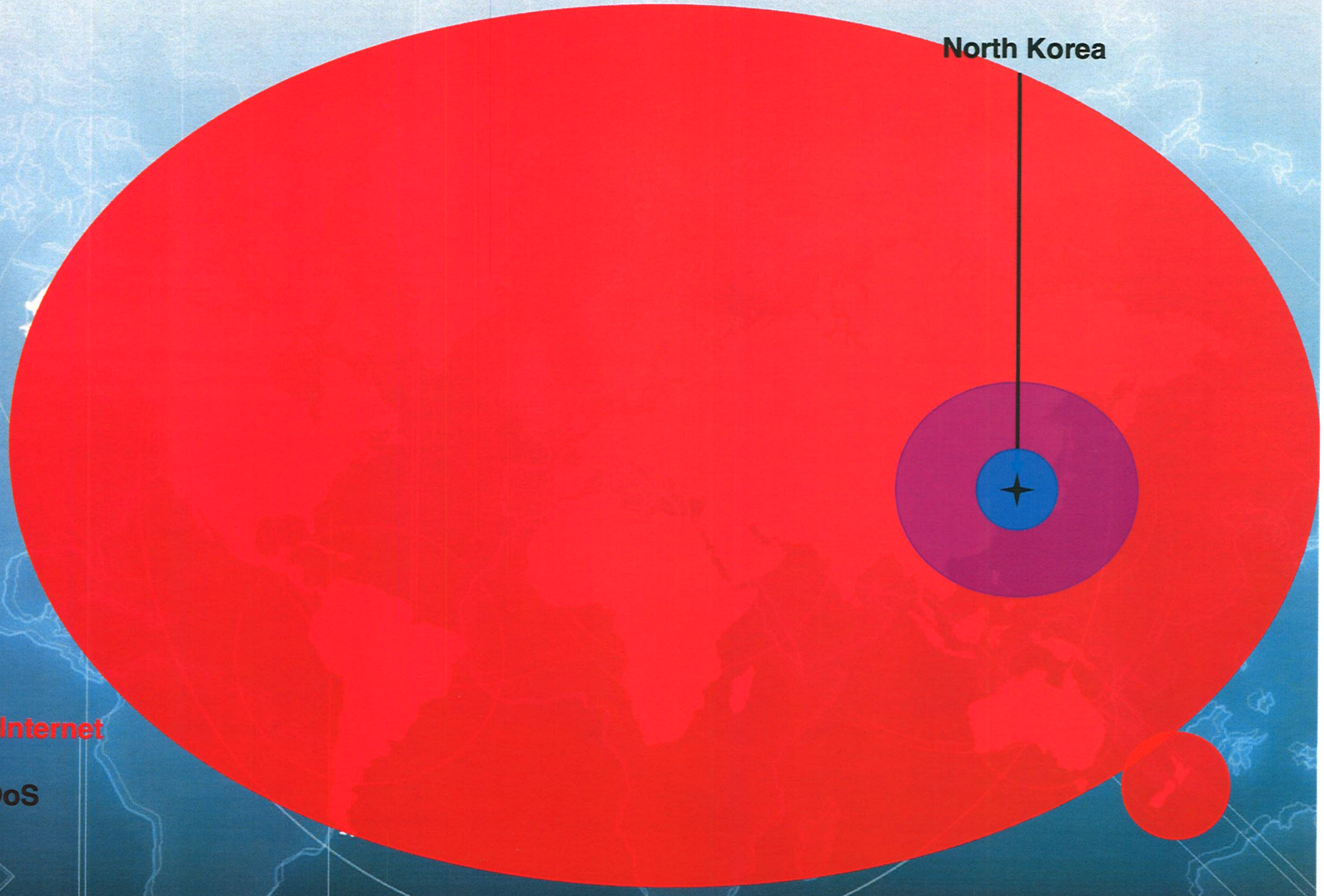
Nodong Missile
Range: 1300km
Type: Ballistic



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

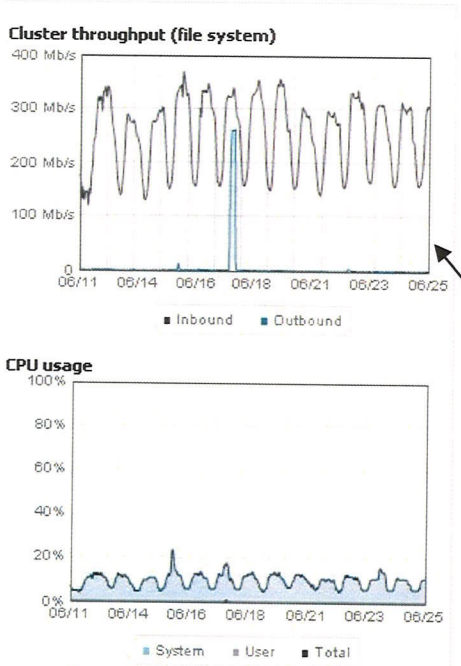
- Would I do a better job from my PC at home?
  - Enhance / Enable collaboration
  - Adopt Internet technologies on our Classified networks
    - SKYPE / Web 2.0 / Video Chat / Google Apps / etc
  - Centralize our 'cyber' analytics
    - CyberDMZ

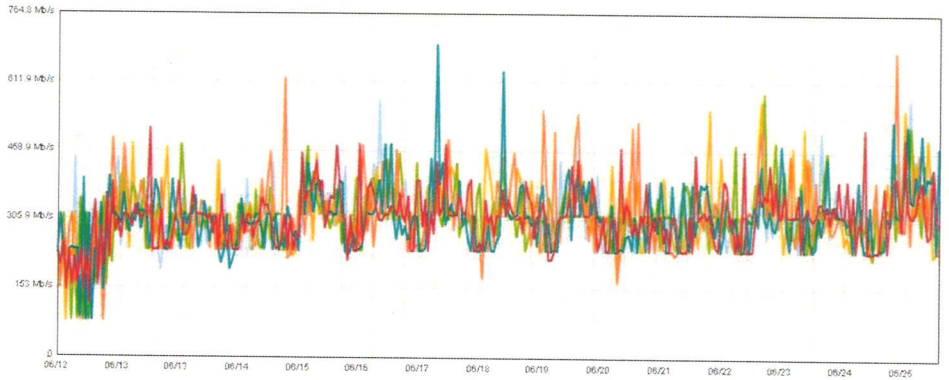
SEEDSPHERE - Discovery

- 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

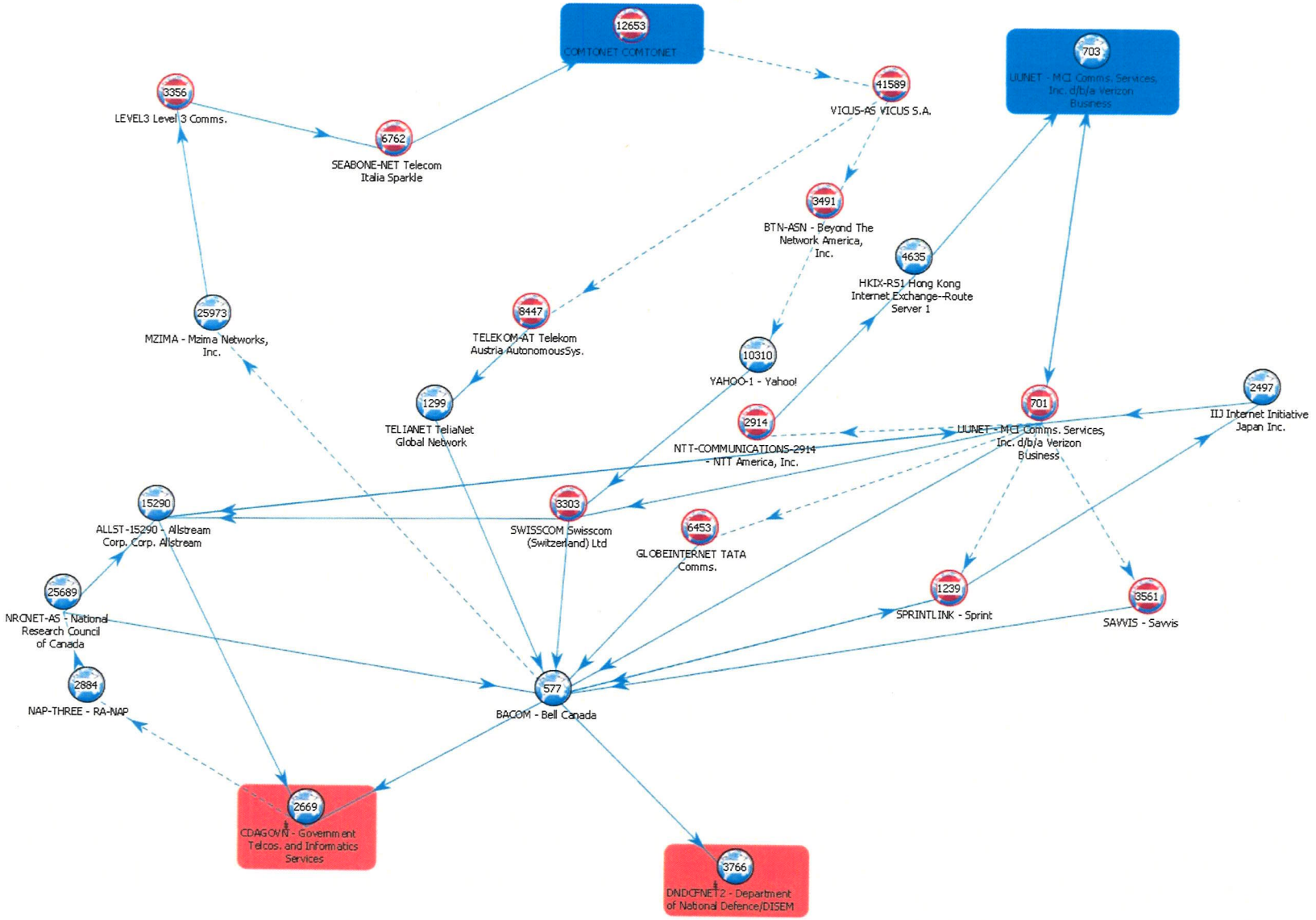
Data deduplication at sight results in much better use of limited bandwidth

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

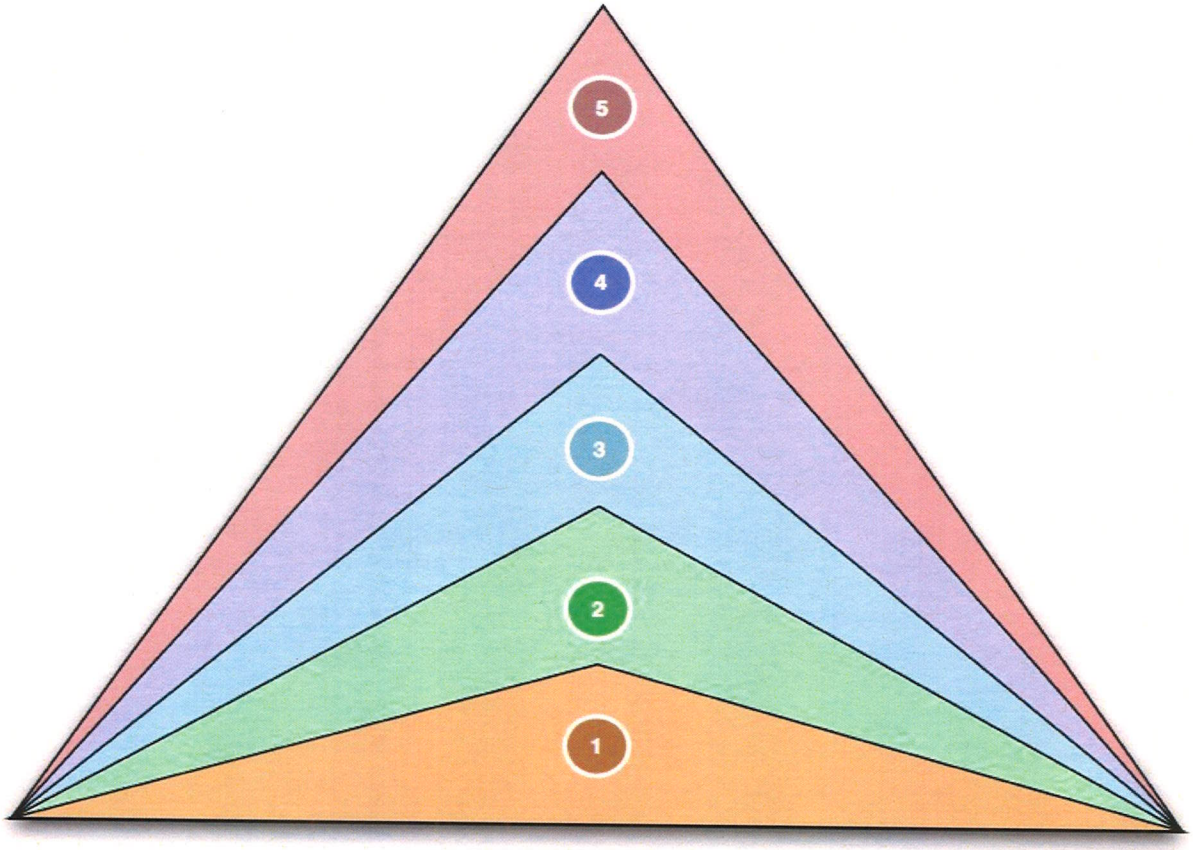
Cyber Repositories

- 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

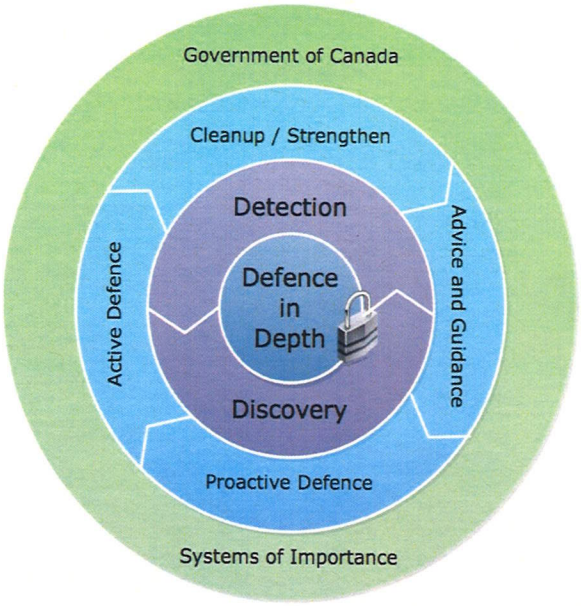
4 Network Analysis

3 Malware Reverse Engineering

2 Traffic Analysis

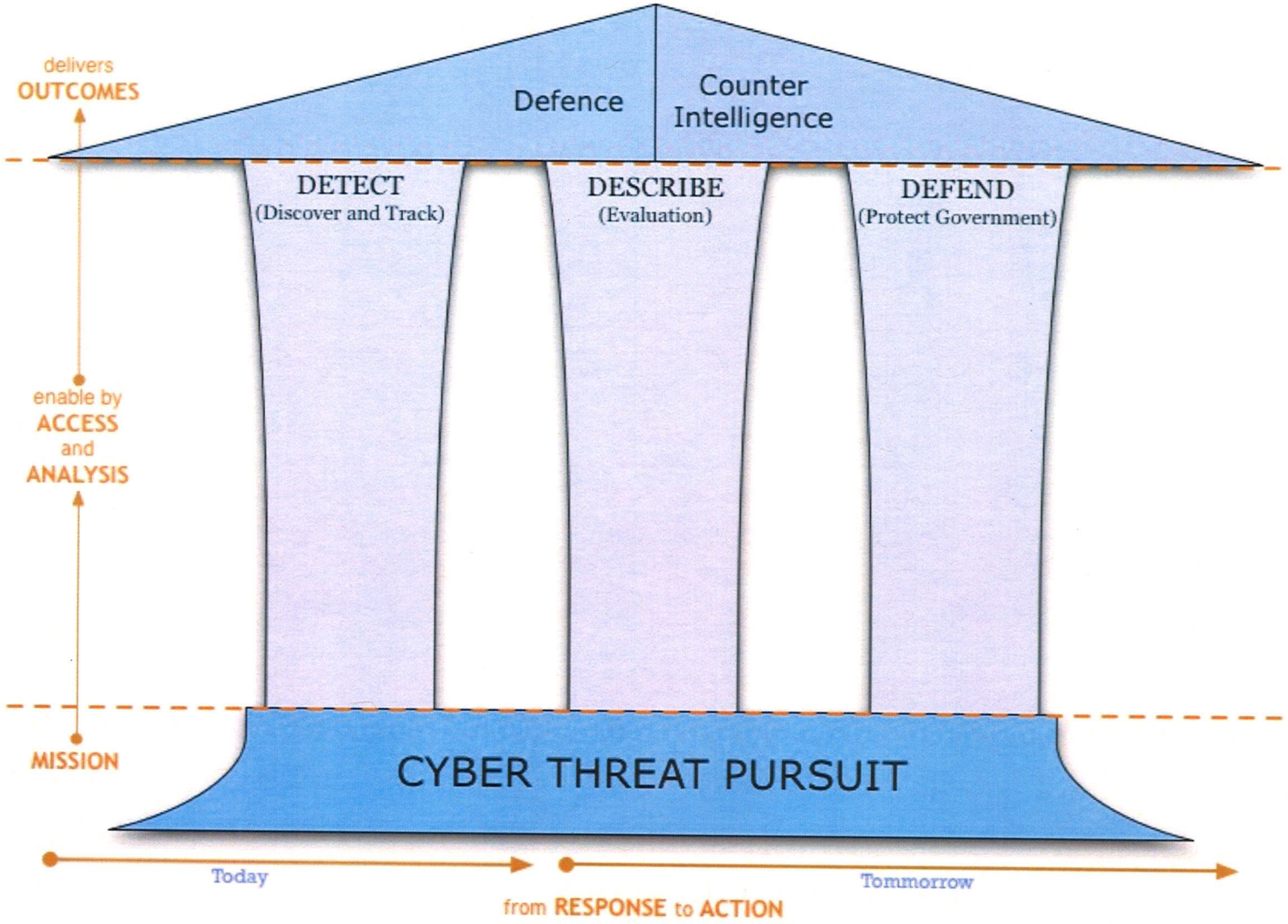
1 Tasking and Collection

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

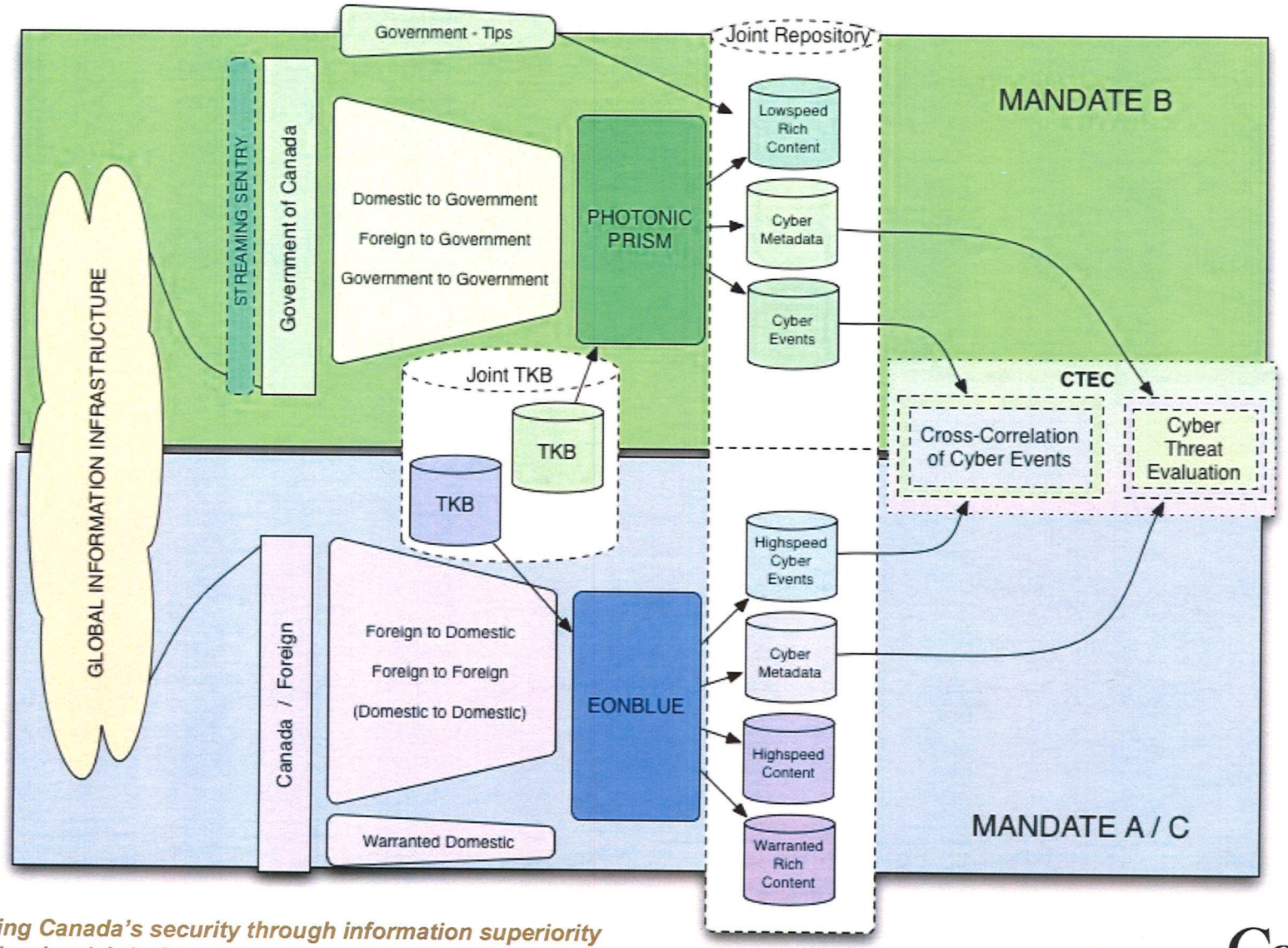
Positioning for the future



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

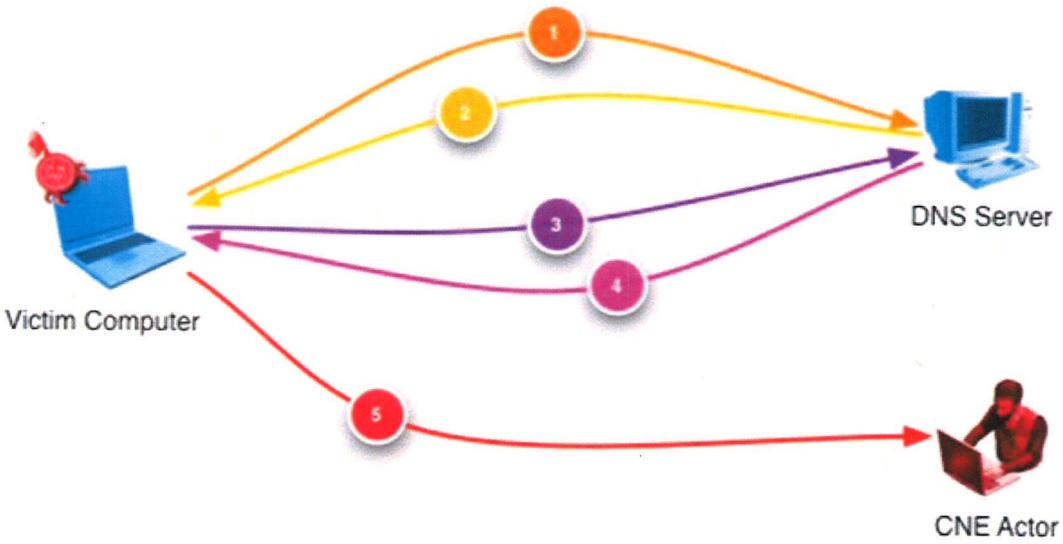
Situational Awareness

- 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



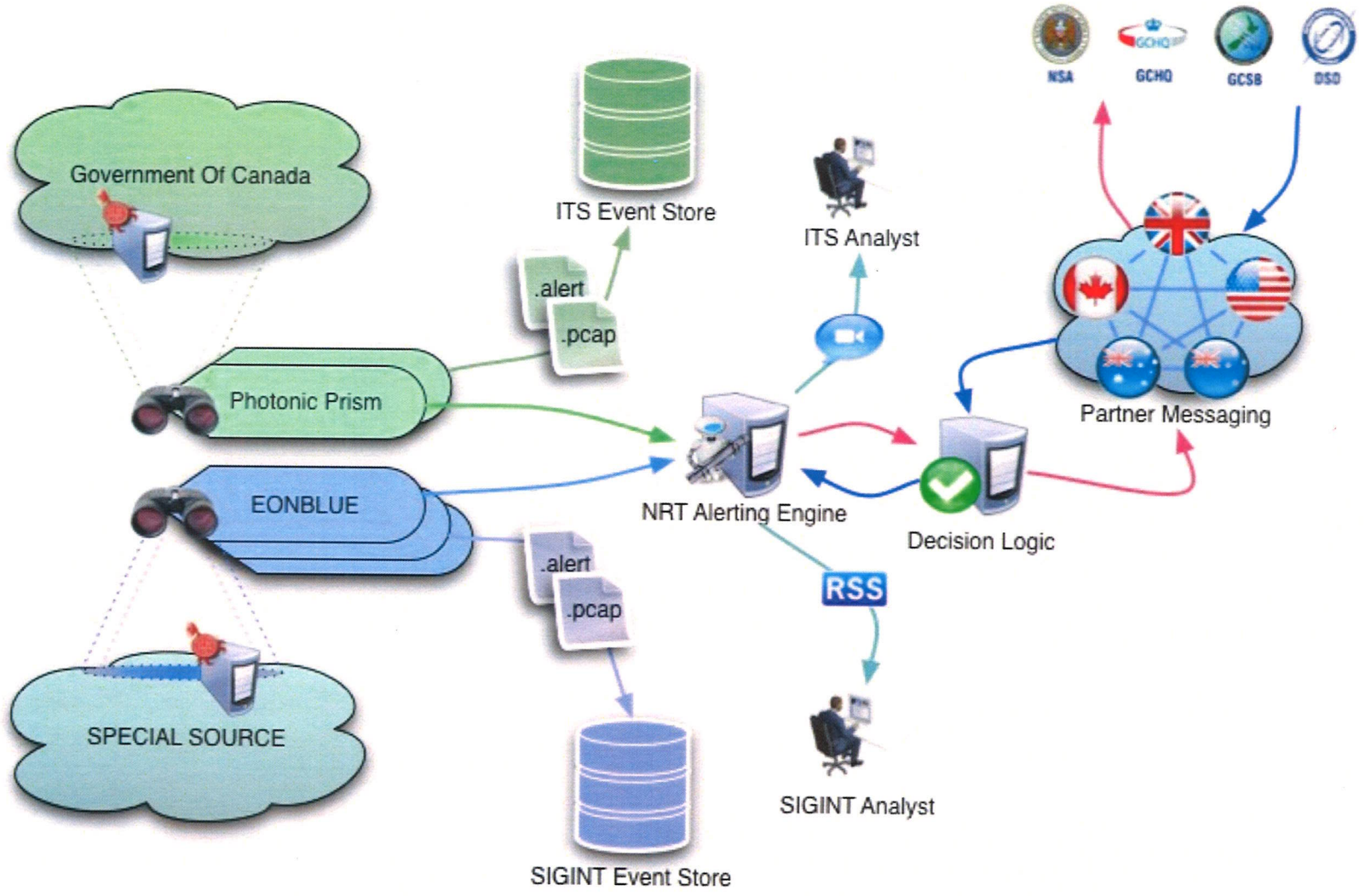
- In the Cyber Context:
  - Gathering and enabling access to cyber information
    - Event Metadata / Event Content / Near Real-Time Exchange
  - Data mining of cyber information to create understanding in broader context
  - Predict our adversaries actions based on this knowledge

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



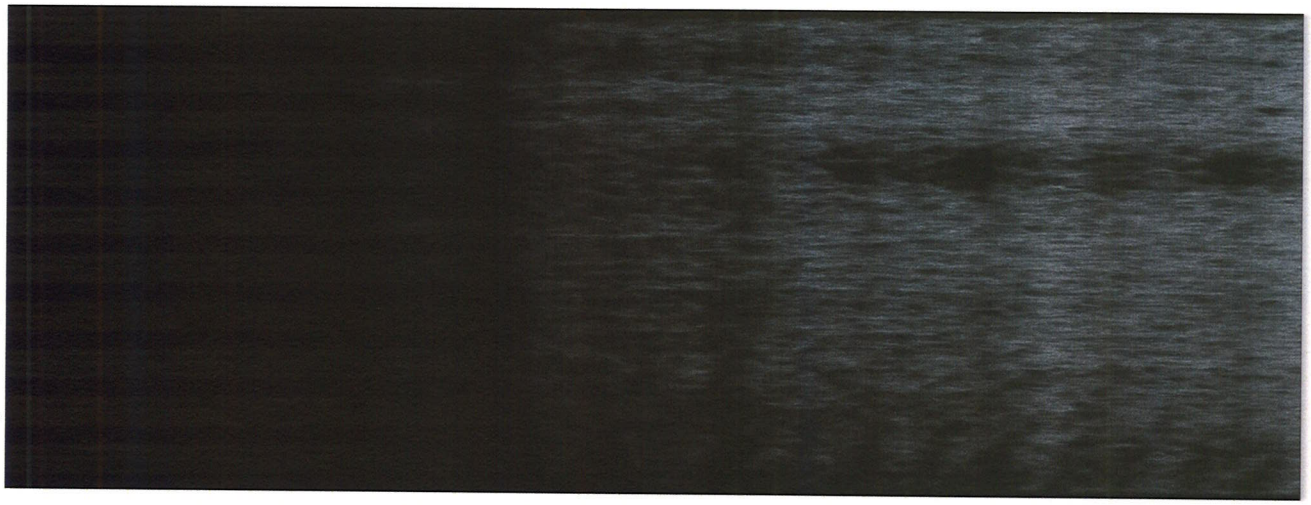
Tipping and Cueing (Why)

- 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** -



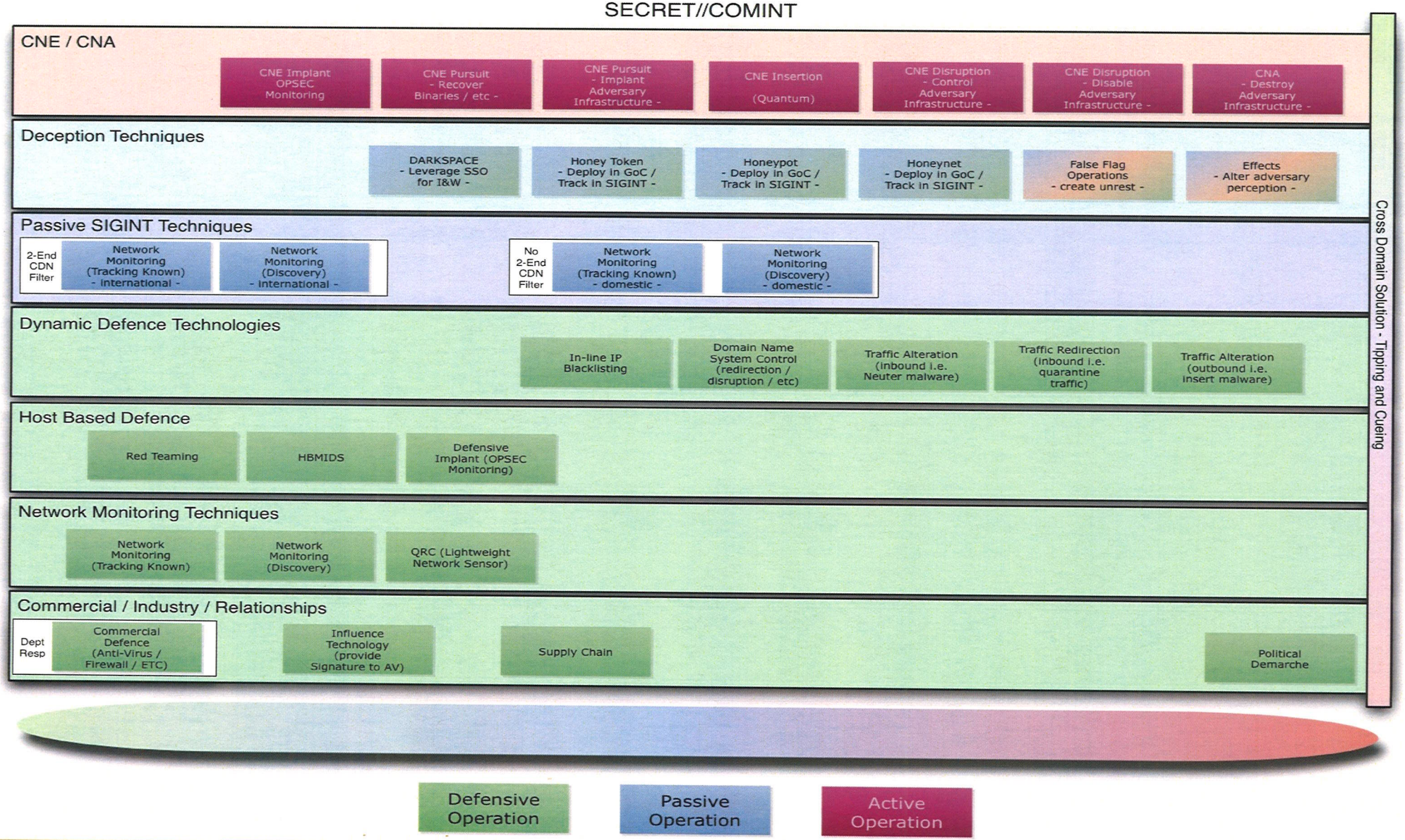
The Network Name is: canadian house of commons
The Network Name is: environment canada
The Network Name is: federal office of regional development (quebec)
The Network Name is: forestry canada
The Network Name is: public works and government services canada

Dynamic Defense

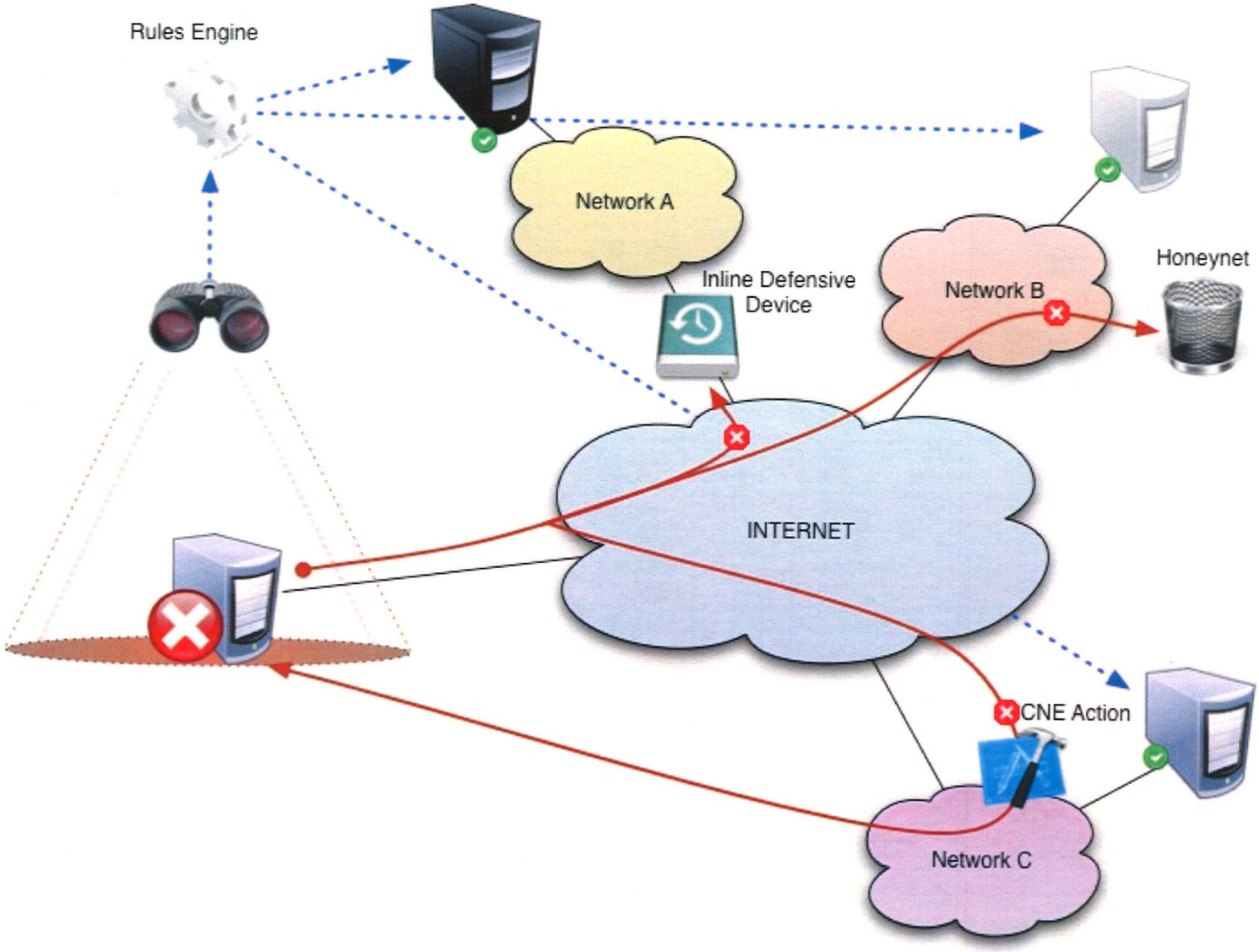
- All elements acting as one
- Defence at:
  - Network Edge (ITS)
    - Localized/tailored mitigation (e.g. blocking, binary neutering, redirection)
    - Focused response to ongoing and potential threats
  - Network Core (SIGINT)
    - Global mitigation possible (e.g. redirection, null routing, filtering)
    - 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)

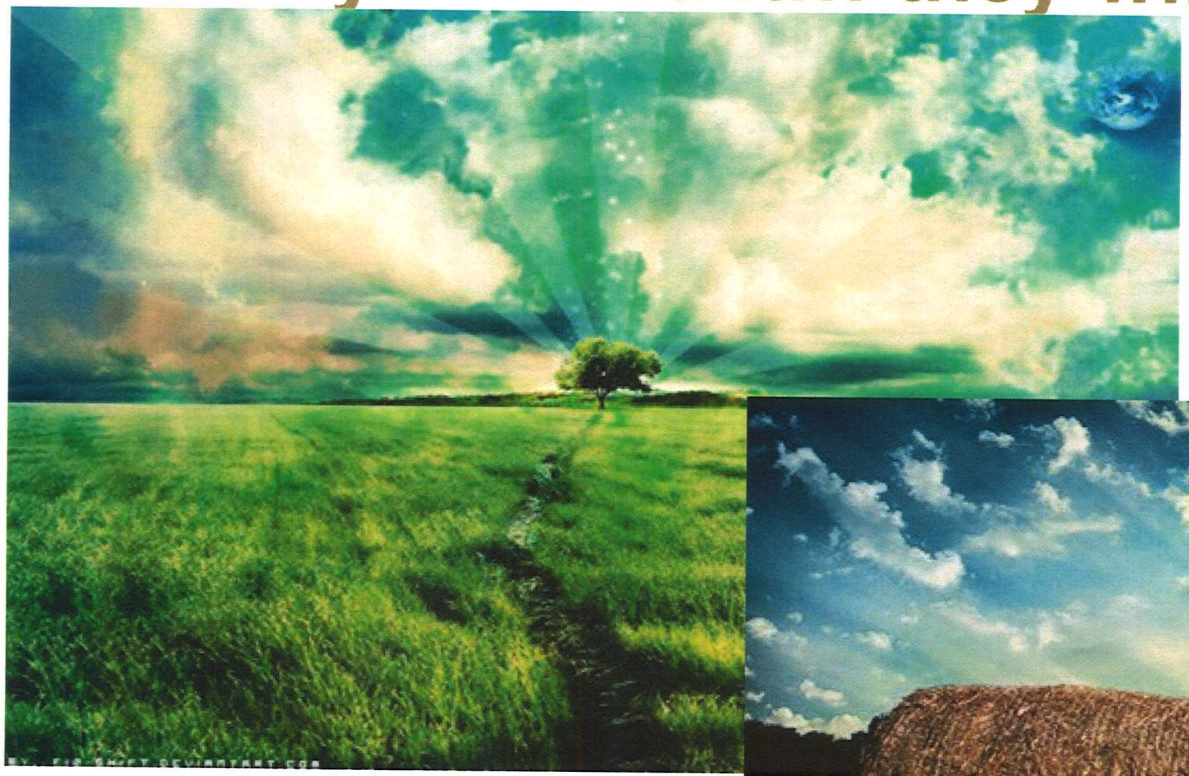
Consider

- Legislative Amendments
- Develop Career Framework

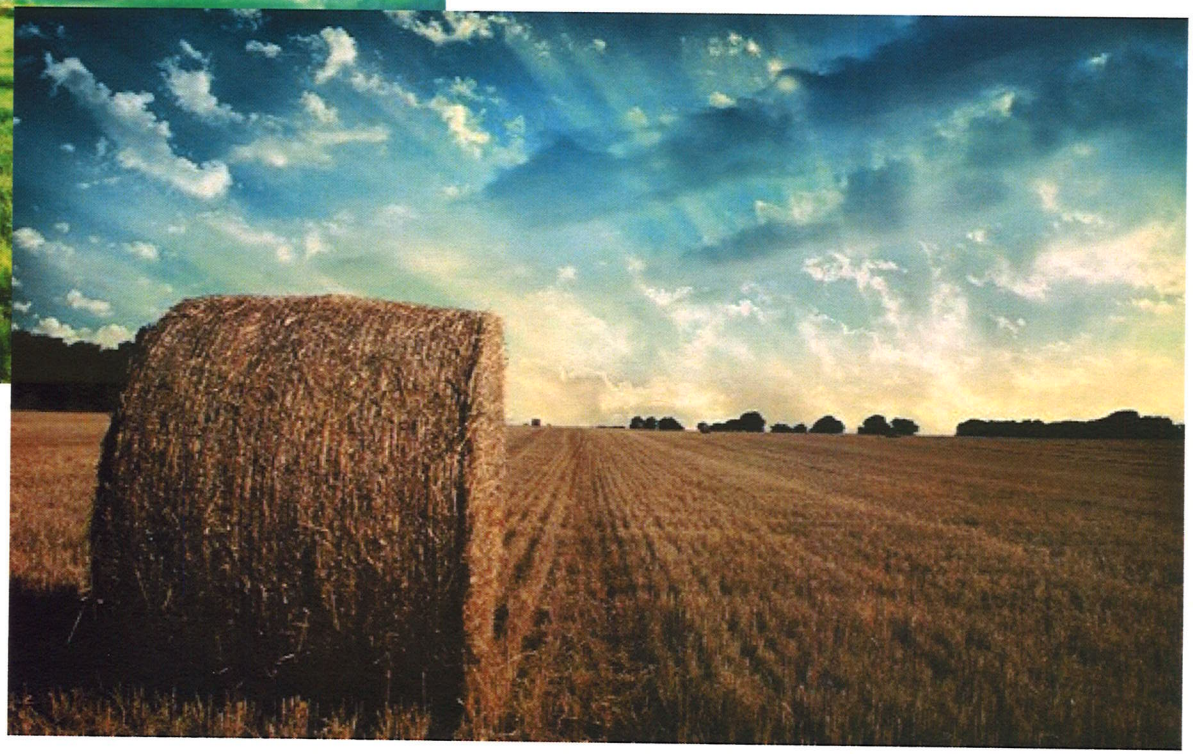
International

- 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

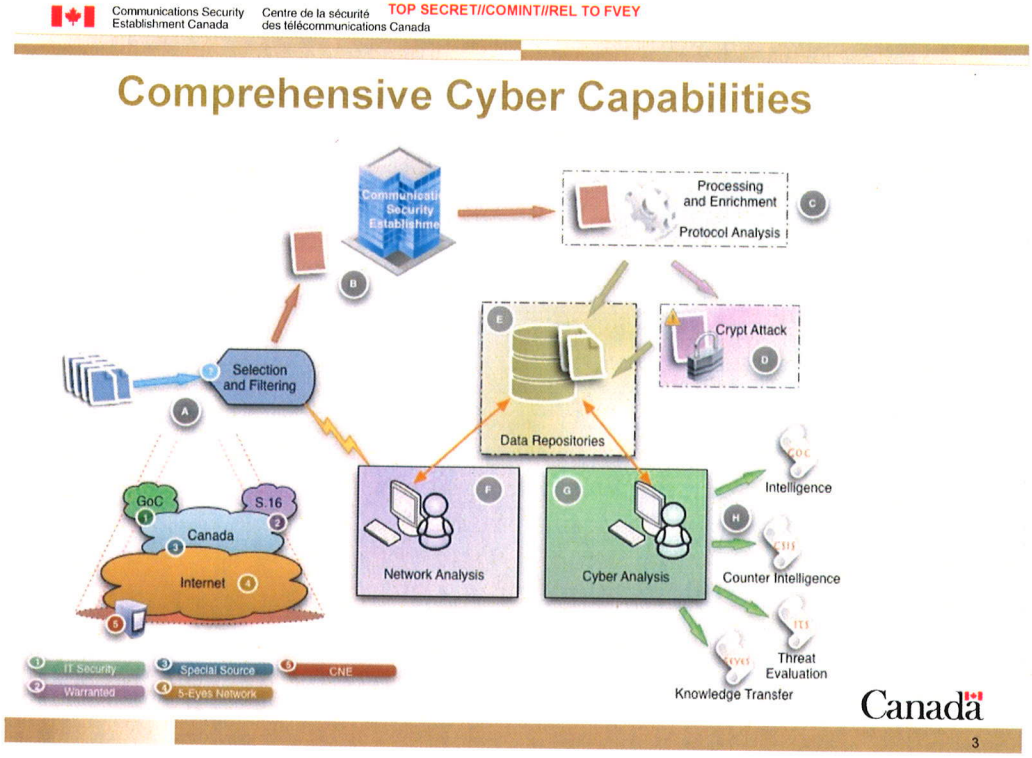
Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

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

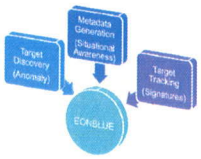


Speak: [redacted] (GA4)

- 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)

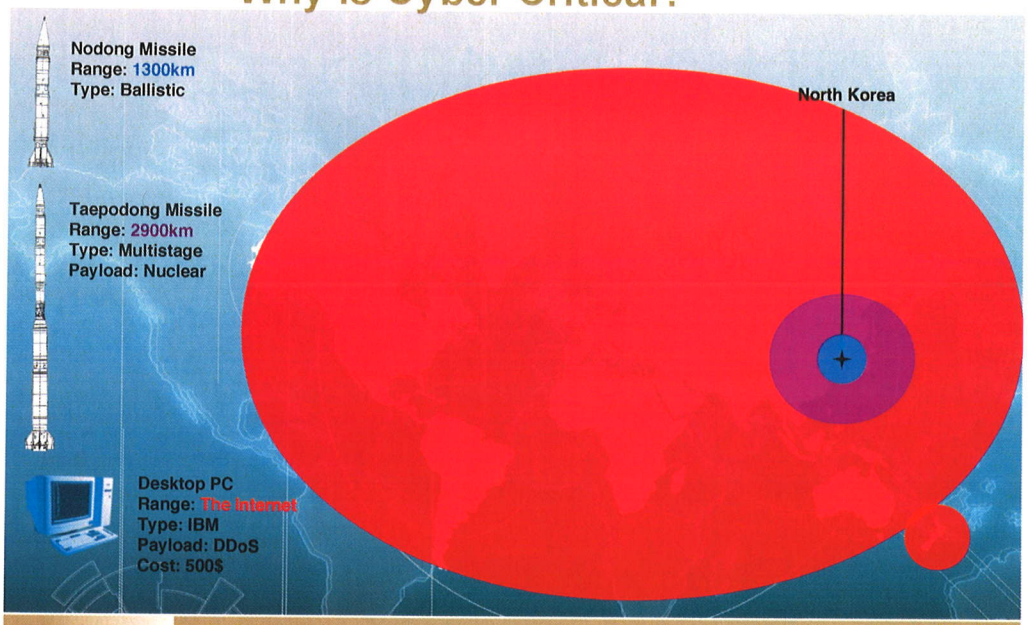
- Message is commercial is not enough

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

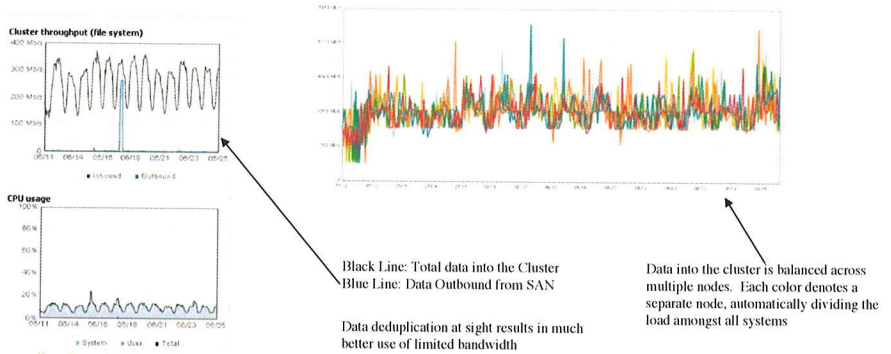
-Explain the value of COVENANT to seed new discovery

-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]

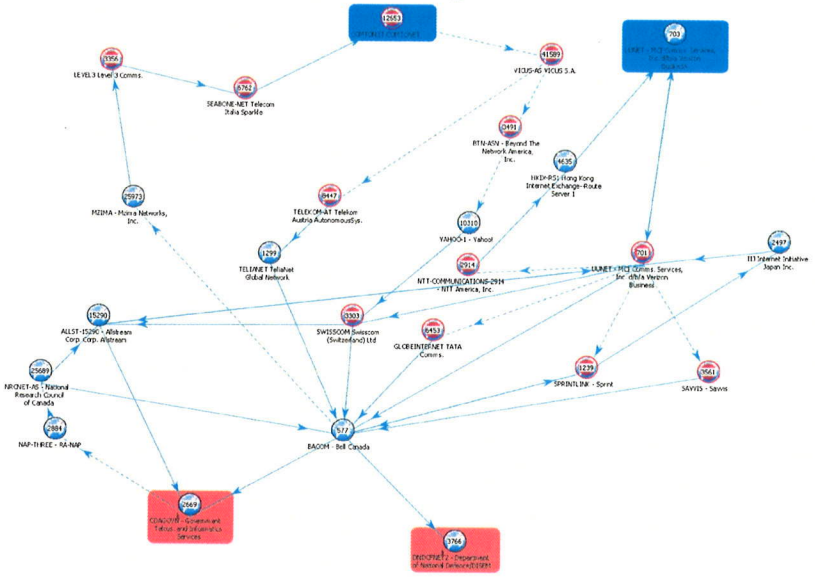
Major Point (Traffic breakdown is 70/30 for SIGINT)

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)

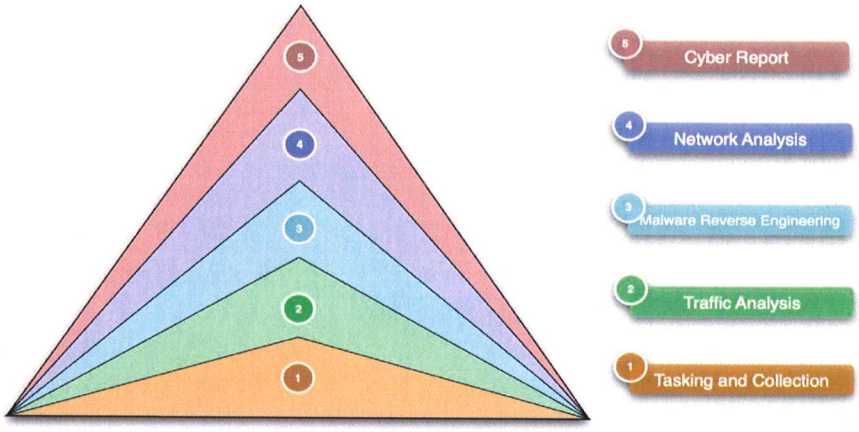
F: Network Analysis



Speaker: [redacted]

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

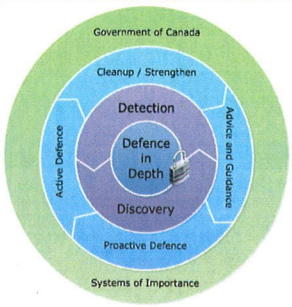
Cyber Analysis



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

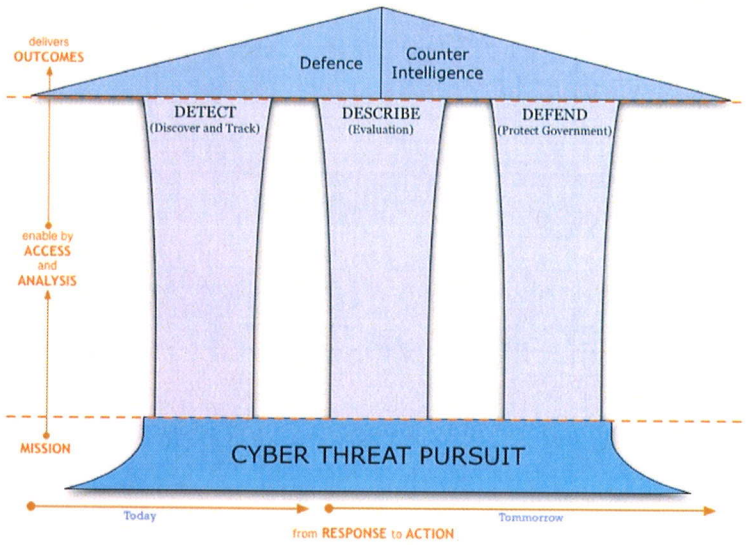
Mitigation



- 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]

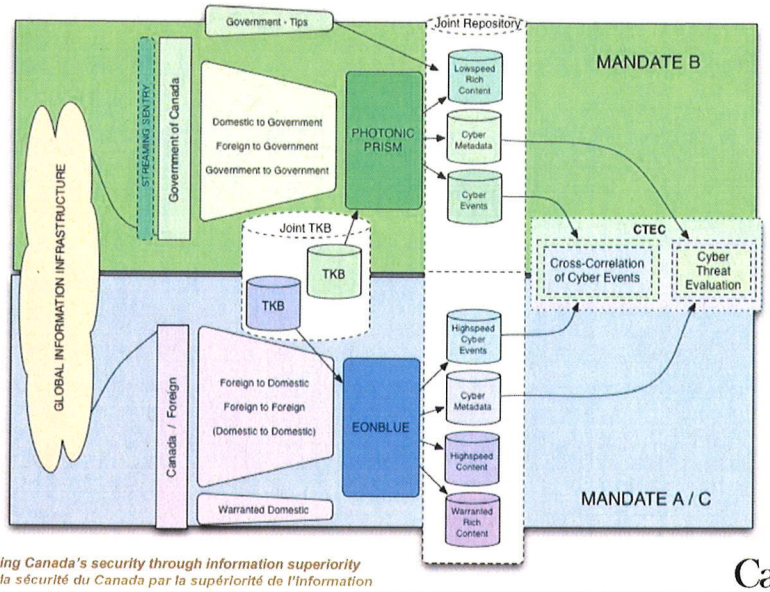
Positioning for the future



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

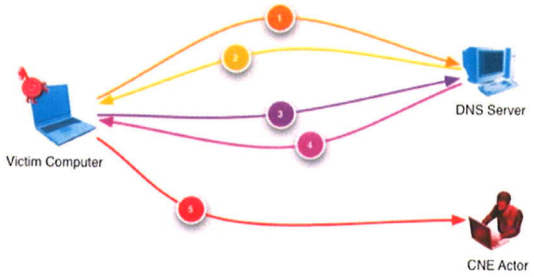
Situational Awareness

- 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



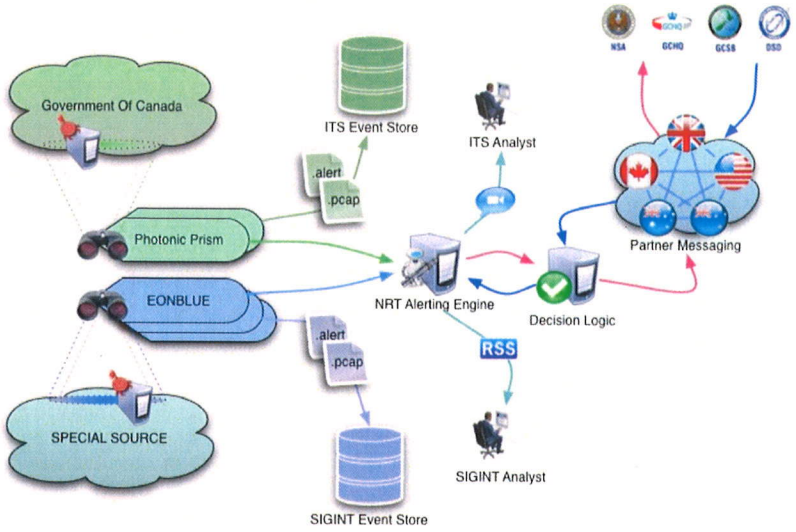
- In the Cyber Context:
  - Gathering and enabling access to cyber information
    - Event Metadata / Event Content / Near Real-Time Exchange
  - Data mining of cyber information to create understanding in broader context
  - Predict our adversaries actions based on this knowledge

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



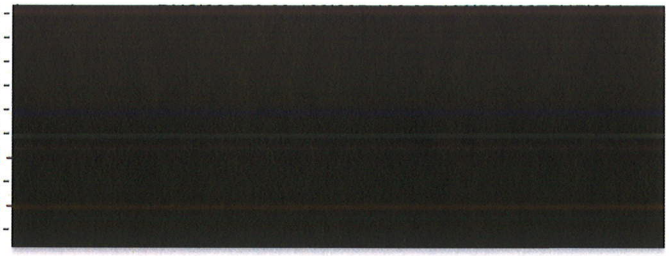
Tipping and Cueing (Why)

- 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