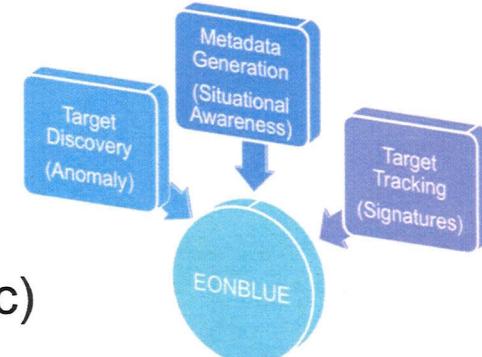




# Cyber Threat Detection

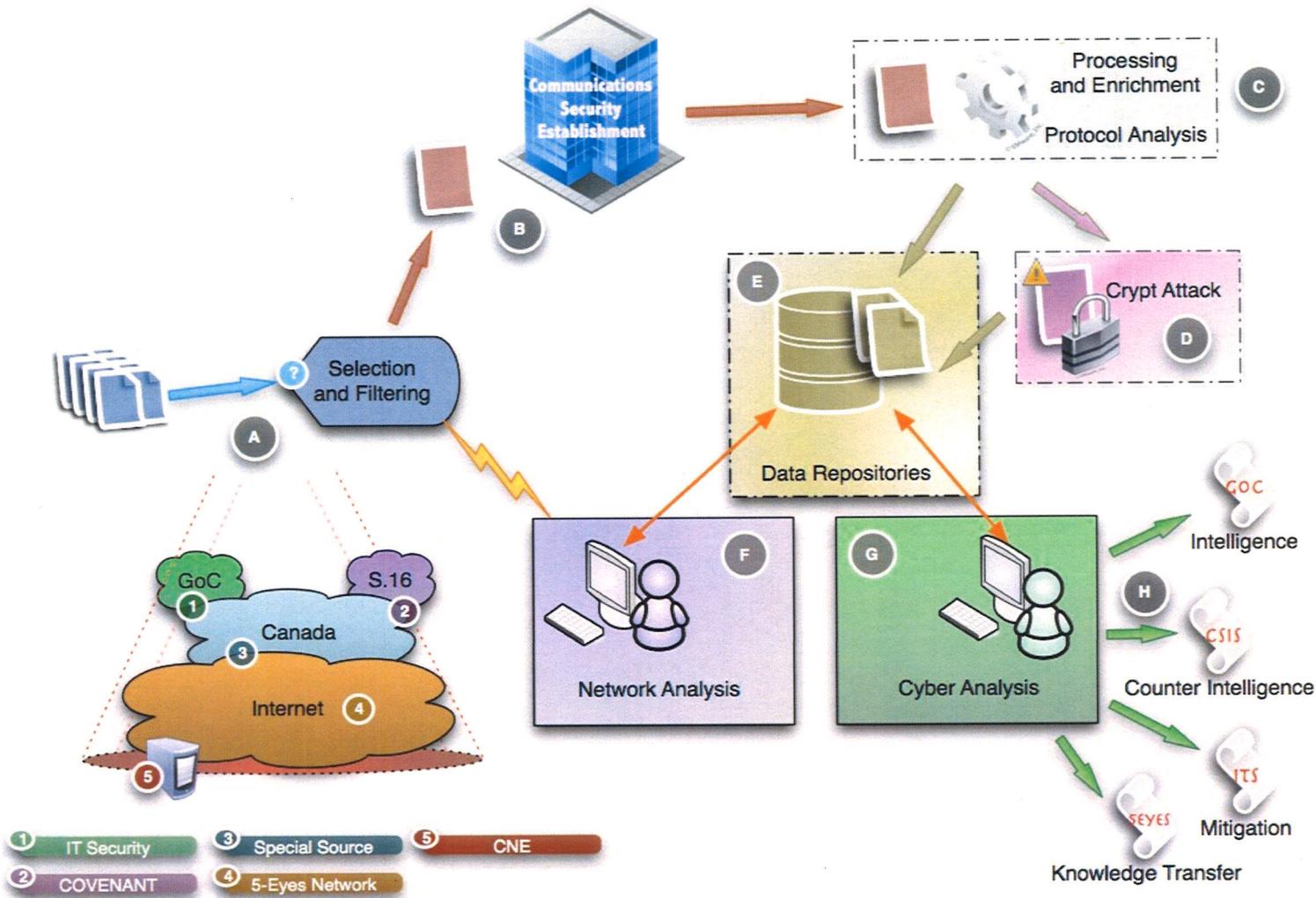
## Passive Cyber Threat Detection Platform - EONBLUE

- 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





# Holistic Cyber Threat Capability





# CSEC – SIGINT Supporting CND

- Globally pervasive threat
  - Covered by 5-Eyes network
- **CSEC elements working as one ...**
- Utilizing encryption
- Subject to CSEC cryptographic attack
- Abusing telecommunications protocols
- **provides unparalleled situational awareness of the threat**  
Understood and reverse engineered at CSEC
- Communicate using foreign languages
- **monitors health and status of government networks**  
Access to SEO and partner linguistic community
- Constantly changing modus operandi
- Coupled with the ability to stop or mitigate attacks and intrusions
- **directed against networks of importance to the GoC**  
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

facebook SEEDSPHERE Applications Inbox Home Settings Logout Search

SEEDSPHERE  
is exfiltrating information from systems located across the globe and has no plans to stop anytime soon.

**Mini-Feed**

See All

Today

SEEDSPHERE downloaded images from the Japanese Embassy in Romania 1:25PM

SEEDSPHERE added the Poison Ivy Application 2:13PM

SEEDSPHERE communicated using the Poison Ivy Application 2:47PM

VGhpoyBpcyBhbiBlbmNvZGVkIjN0cmluyB8uaGF0IFJlcXVpcmVzIERlY3J5cHRpb24

Yesterday

SEEDSPHERE is abusing the DNS Protocol 4:36PM

Last Week

SEEDSPHERE is taking the day off on Chinese New Year 12:00AM

**Friends**

23 Friends See All

DIESLRATTLE SIENNABLUE DOWNGRADE

**Places I've Been (125,234)**

See All

Groups

See All

Windows Internals, 3322.org, bosee.net, lovequintet.org, lovetroi.com, chineseundermud

The Wall

See All

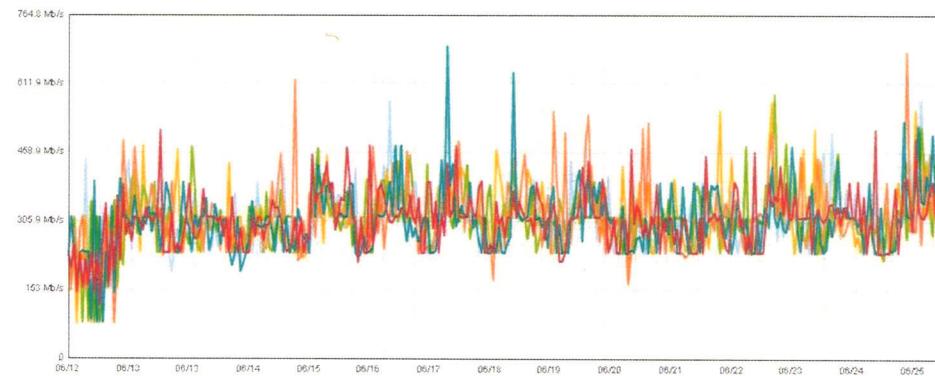
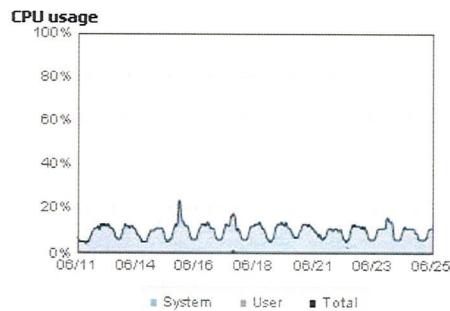
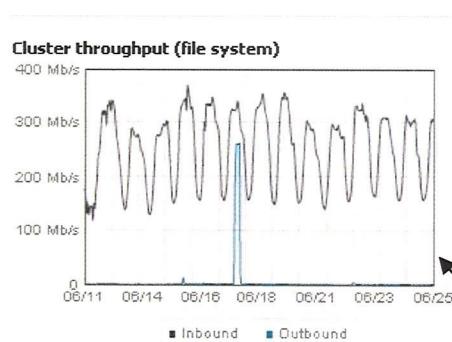
SIENNABLUE wrote:

すねみまけゑづばぶぼるまおあかゆろをでぢび。ねてぼび?づてたはほよぶゆごひすせけうおへえねむ!ネマソカウユブザギゴアネニタセソコクン



# 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

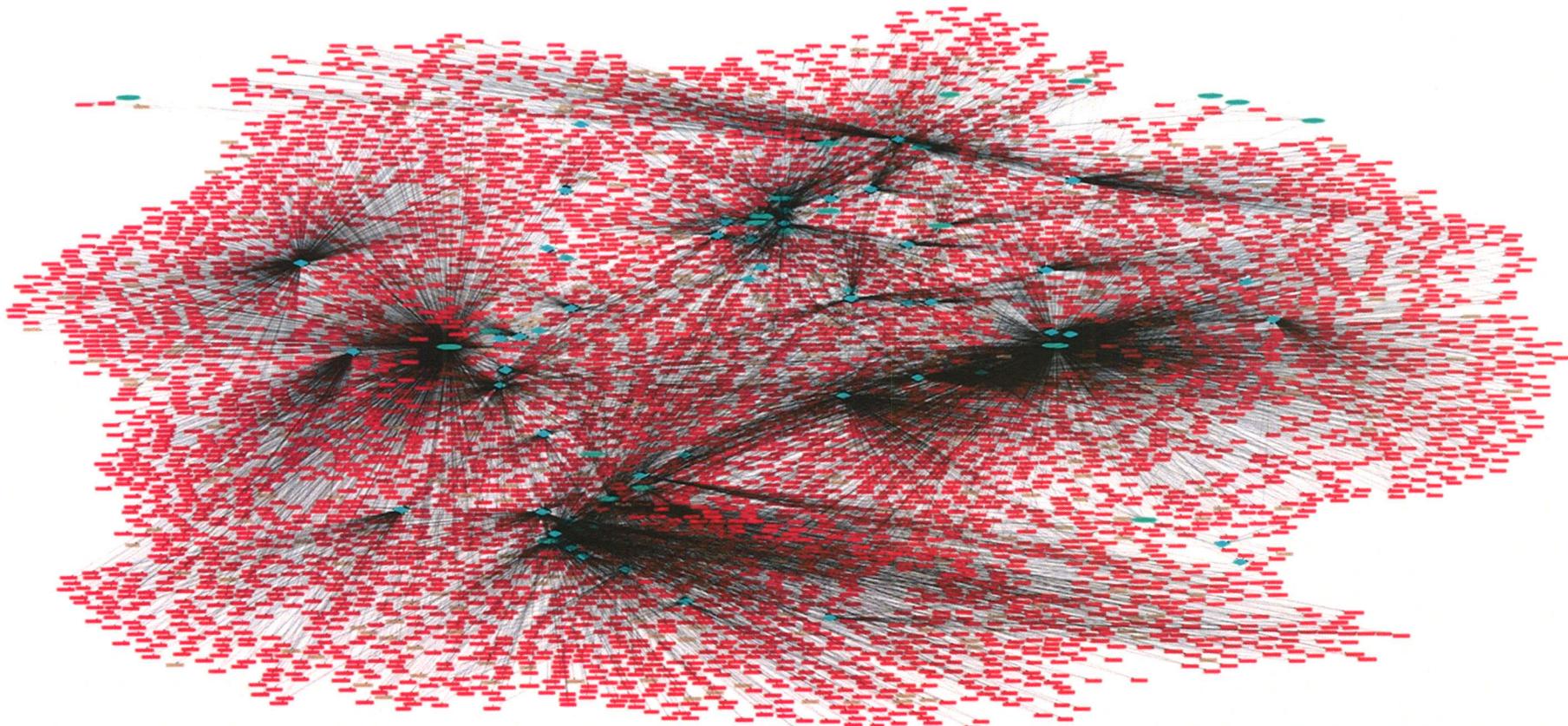


# Sample of Fast Flux Activity Detected

Square nodes: contacted by fast flux "bots"

Diamond nodes: fast flux "bots"

Oval nodes: suspected fast flux domain



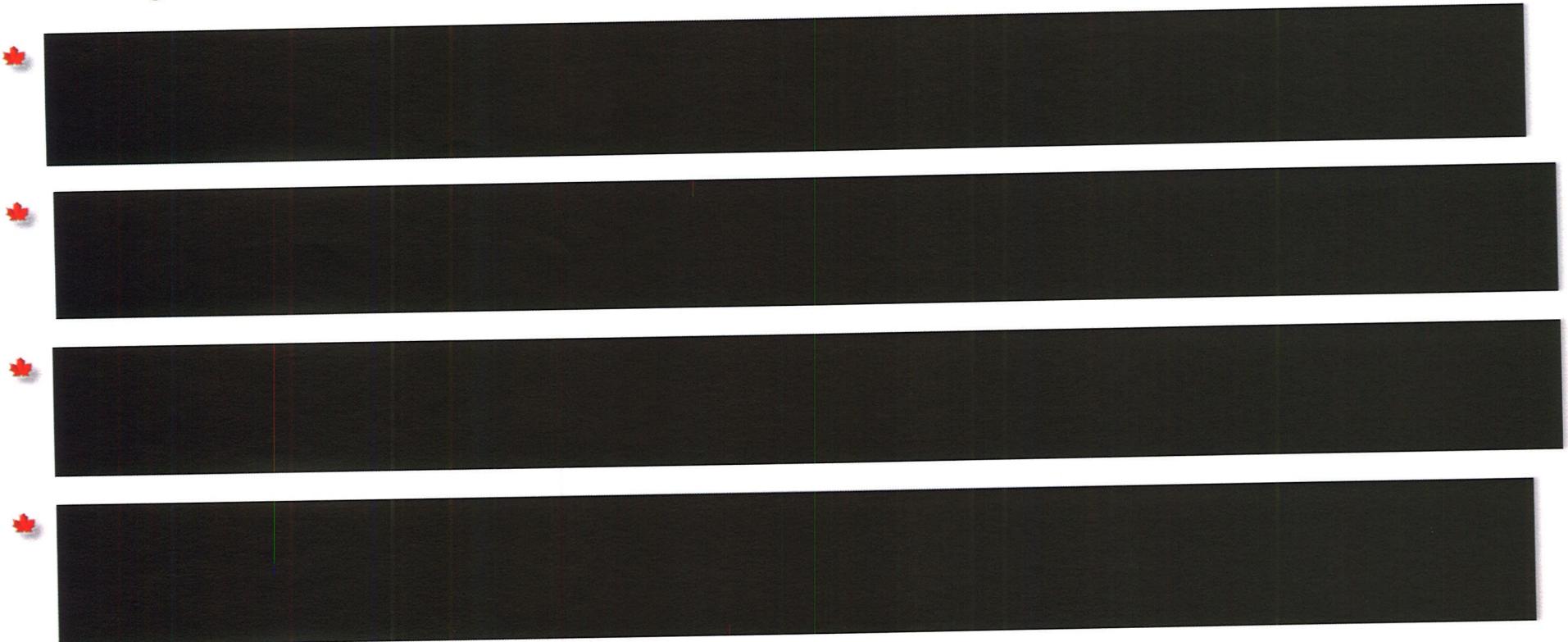
1 week of detected fast flux activity for a particular fast flux domain at a CSEC access



# Joint Capability Development

## SIGINT / ITS – Cyber Threat Detection

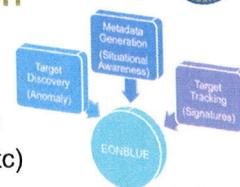
- Scanning Detection - LODESTONE





## 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)

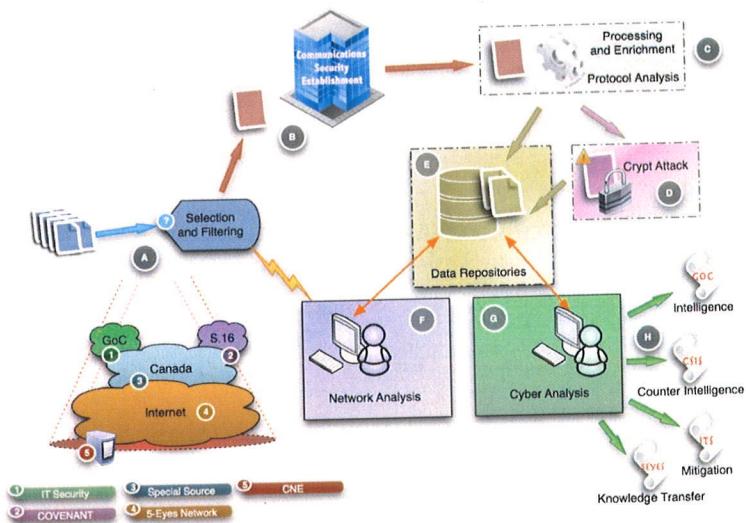


Canada

1



## Holistic Cyber Threat Capability



Canada



## CSEC – SIGINT Supporting CND

- Globally pervasive threat
  - Covered by 5-Eyes network
- CSEC elements working as one ...
  - Utilizing encryption
  - Subject to CSEC cryptographic attack
- **provides unparalleled situational awareness of the threat**
  - Abusing telecommunications protocols
    - Understood and reverse engineered at CSEC
  - Communicate using foreign languages
    - Intent to exploit partner linguistic community
  - Constantly changing modus operandi
    - Using social media, open source intelligence, and anomaly detection
  - Coupled with the ability to stop or mitigate attacks and intrusions
    - Analytics
- **directed against networks of importance to the GoC**
  - Exfiltrate valuable intelligence
    - Which 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

The screenshot shows a Facebook-like application interface. At the top, there's a navigation bar with 'facebook', 'SEEDSPHERE', 'Applications', 'Inbox', 'Home', 'Settings', 'Logout', and a 'Search' bar. The main area is titled 'SEEDSPHERE' and has a sub-section 'Mini-Feed'. It says 'is exfiltrating information from systems located across the globe and has no plans to stop anytime soon.' Below this, there are several posts:

- 'SEEDSPHERE downloaded images from the Japanese Embassy in Romania' (timestamp: 1/25PM)
- 'SEEDSPHERE added the Poison Ivy Application' (timestamp: 2/13PM)
- 'SEEDSPHERE communicated using the Poison Ivy Application' (timestamp: 2/4/2014 10:29AM)
- 'VNCproxy[hidden]@[hidden] is using the Poison Ivy Application' (timestamp: 2/4/2014 10:29AM)
- 'SEEDSPHERE is abusing the DNS Protocol' (timestamp: 2/4/2014 10:29AM)
- 'SEEDSPHERE is taking the day off on Chinese New Year' (timestamp: 1/27/2014 10:08AM)

Below the feed, there's a 'Friends' section showing 23 friends, a 'Places I've Been' section (125,234 locations), and a 'Groups' section.

Canada

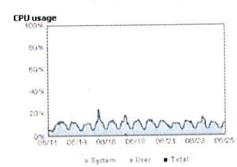
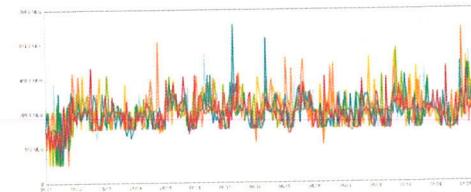
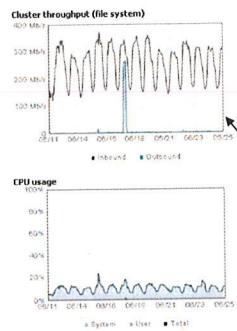
Speaker: [REDACTED]

- Added the health and status of Government network bullet
- Removed '4<sup>th</sup> party' and instead mention how it enhances our repositories (will introduce 4<sup>th</sup> 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

Canada



## 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

TOP SECRET//COMINT



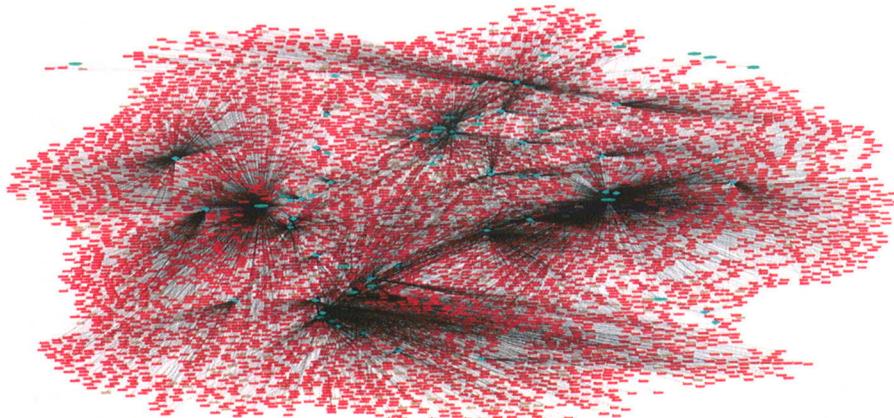
Communications Security  
Establishment

Centre de la sécurité  
des télécommunications



## 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

Canada



## Joint Capability Development

### SIGINT / ITS – Cyber Threat Detection

#### Scanning Detection - LODESTONE

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Canada

7