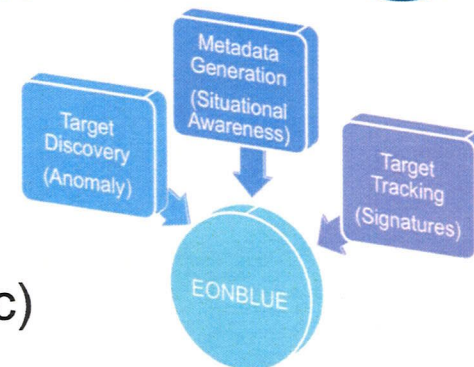




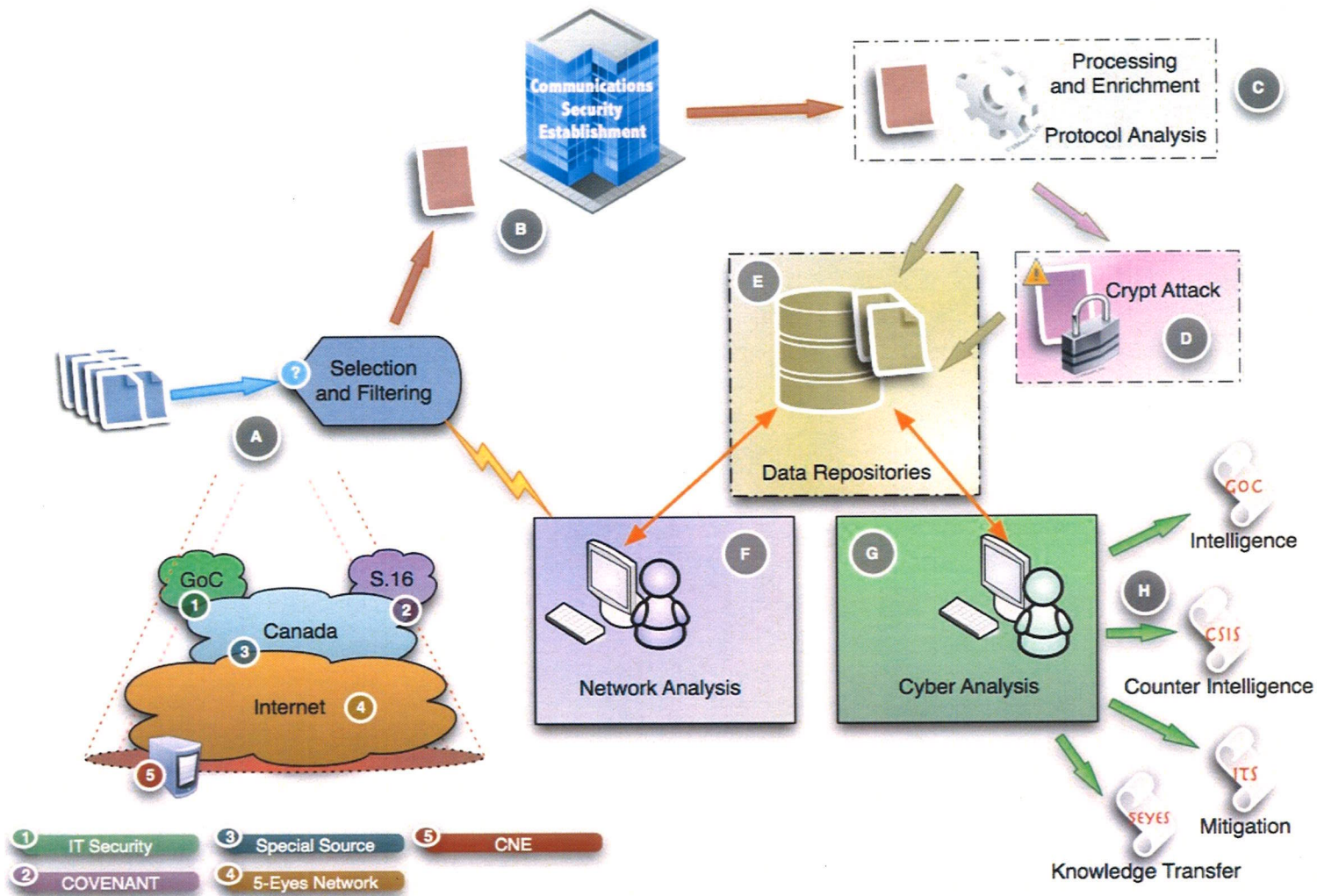
Cyber Threat Detection



- 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

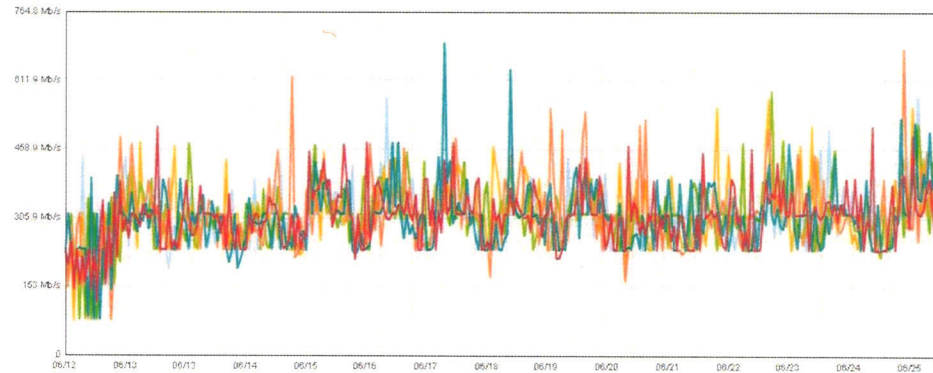
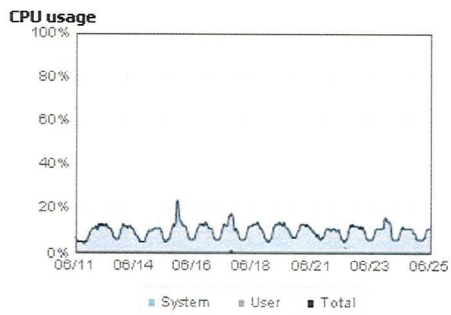
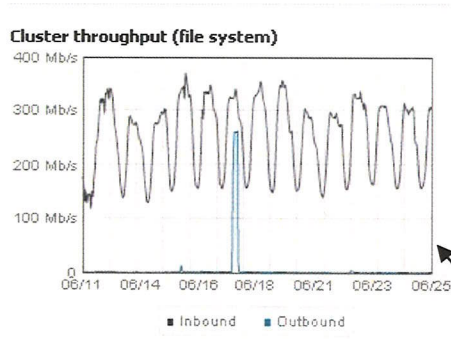
- Globally pervasive threat
 - Covered by 5-Eyes network
- **CSEC elements working as one ...**
 - Utilizing encryption
 - Subject to CSEC cryptographic attack
- **Abusing telecommunications provides unparalleled situational awareness of the threat**
 - Understood and reverse engineered at CSEC
- **Communicate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





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

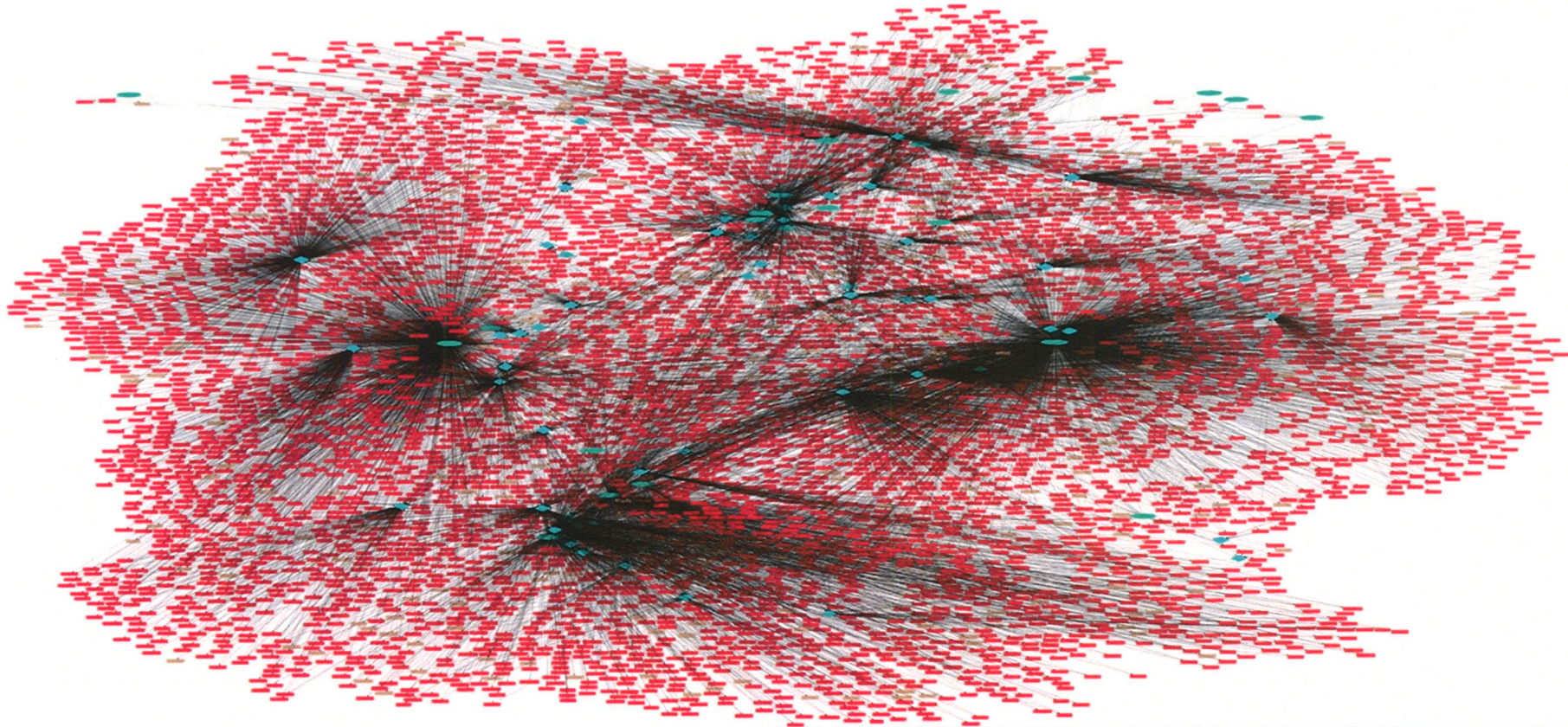
SIGINT / ITS – Cyber Threat Detection

- 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 content]



[Redacted content]



[Redacted content]



[Redacted content]