

TOP SECRET//COMINT//REL TO USA,  
FVEY

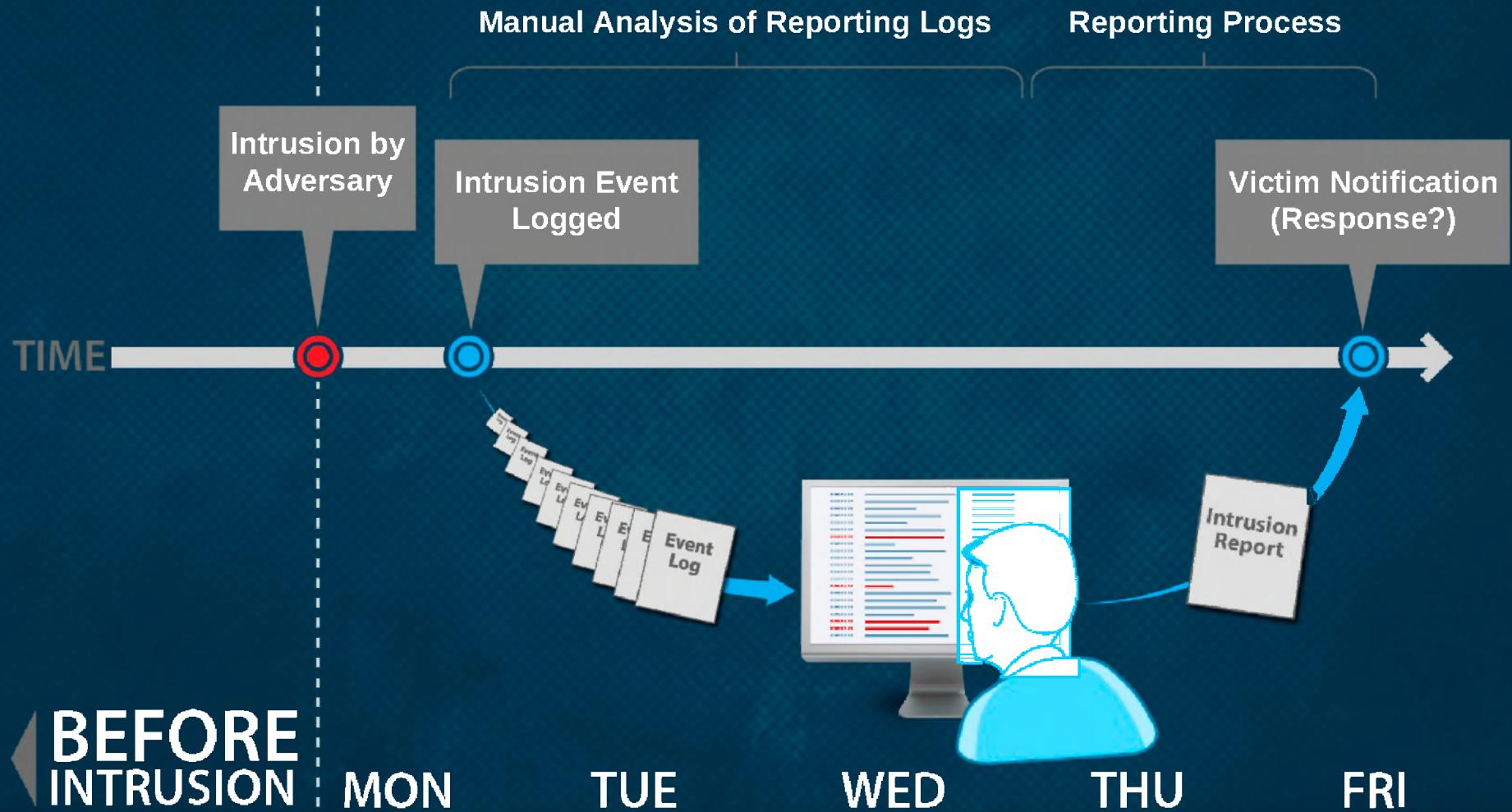
# TUTELAGE

4 1 1



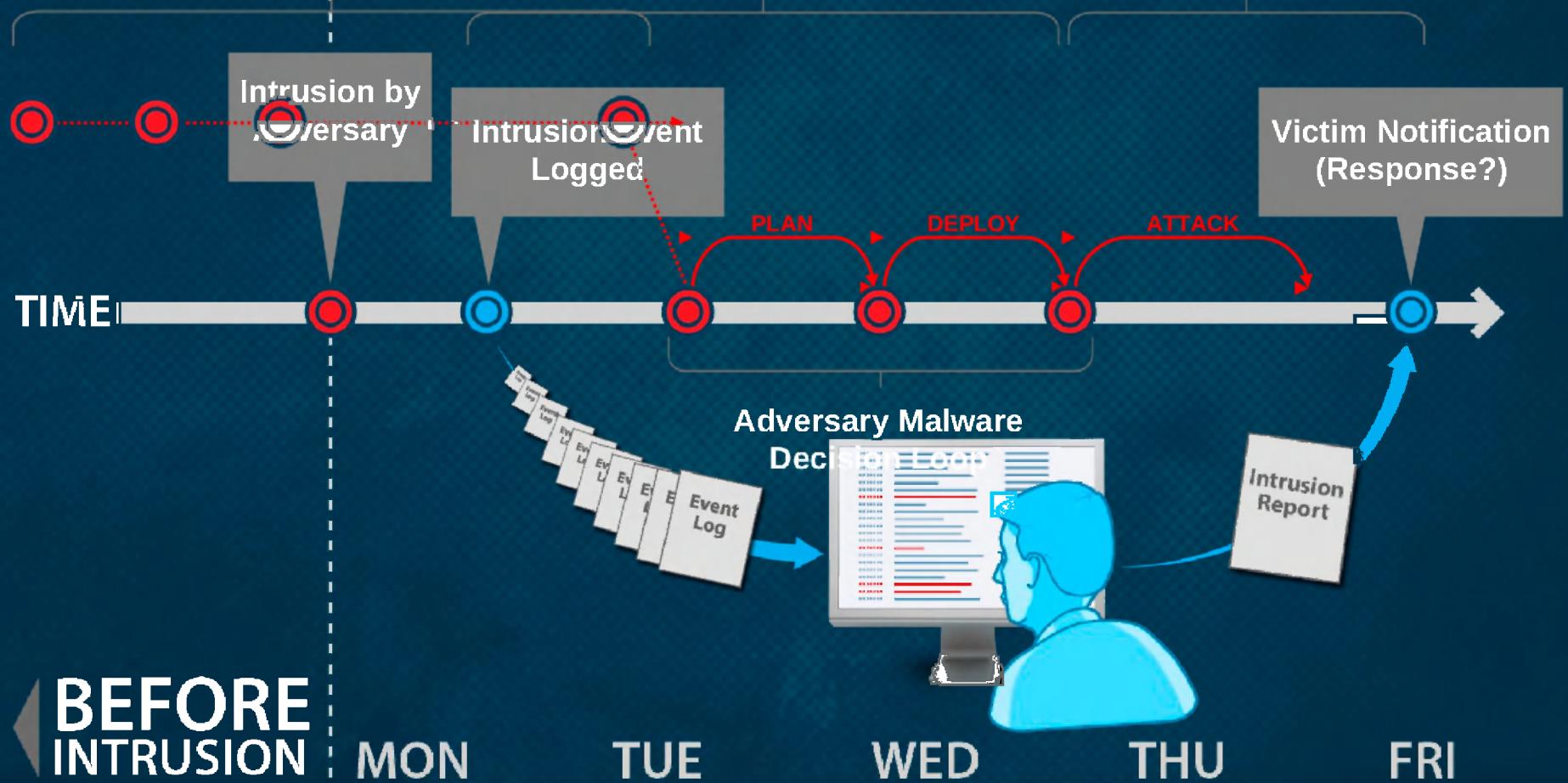
TOP SECRET//COMINT//REL TO USA,

# AFTER INTRUSION



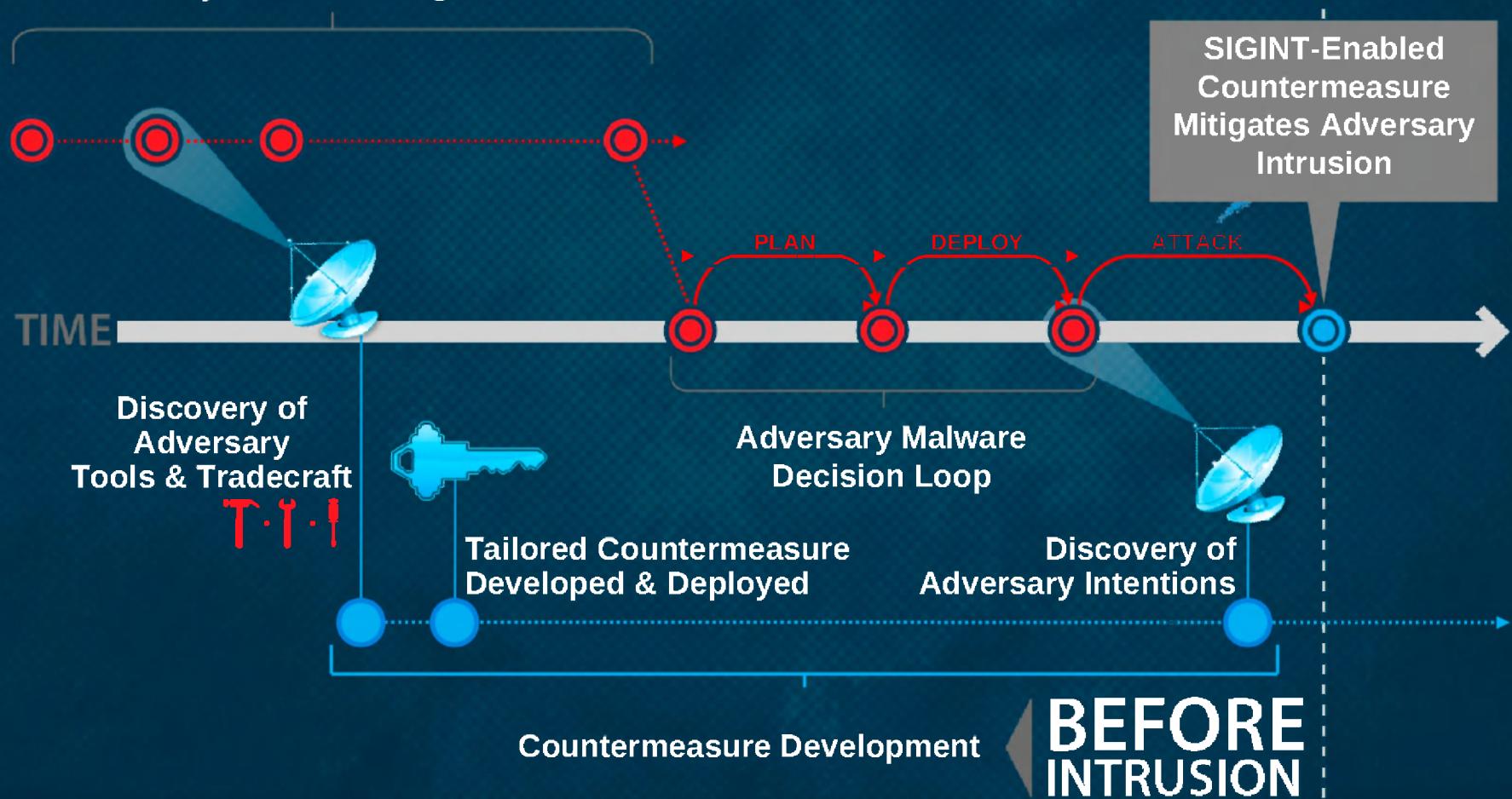
# AFTER INTRUSION

Adversary Malware Design Process | Analysis of Reporting Logs | Reporting Process



AFTER  
INTRUSION

Adversary Malware Design Process



# Application of Capabilities

Internet



DoD  
Gateways

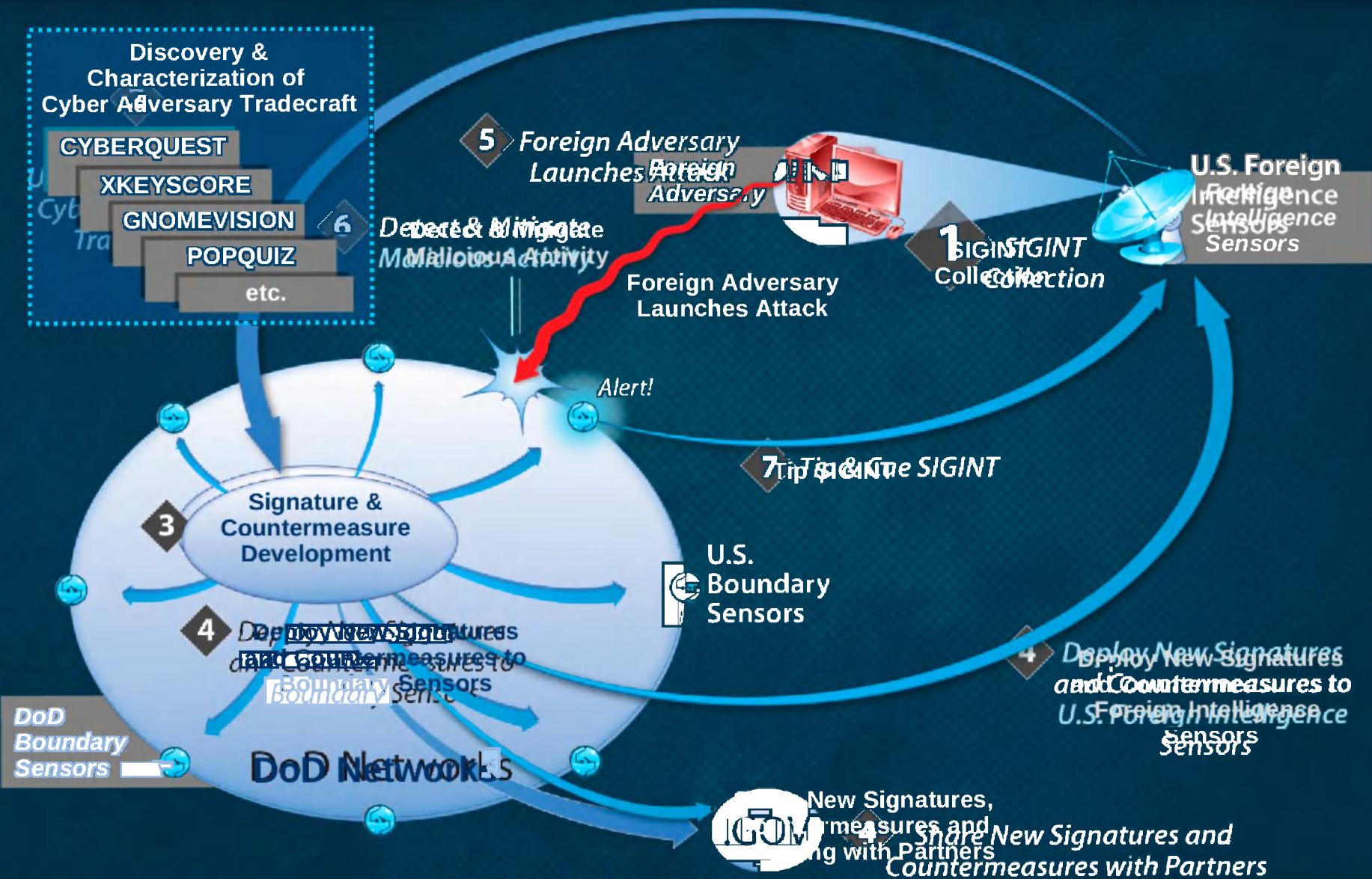


NIPRNet

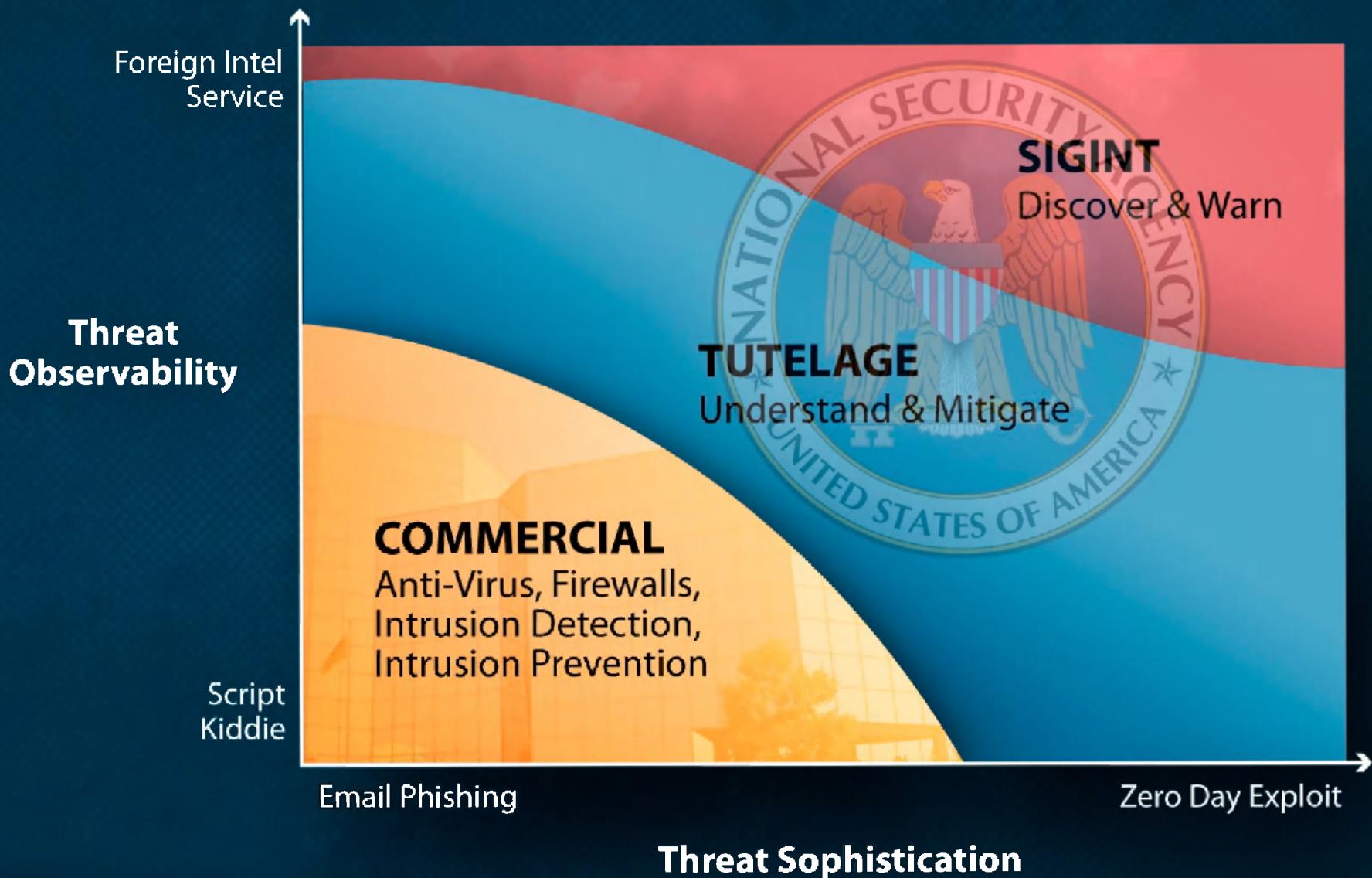


FVF

# TUTELAGE Mission Flow



# Operational Landscape



# TUTELAGE Capabilities



## Alert/Tip



## Redirect



"What's My Destination?"

Redirect to Safe Server

Infected Host's Information



## Intercept



## Block



Blocks Entry/Exit Activity

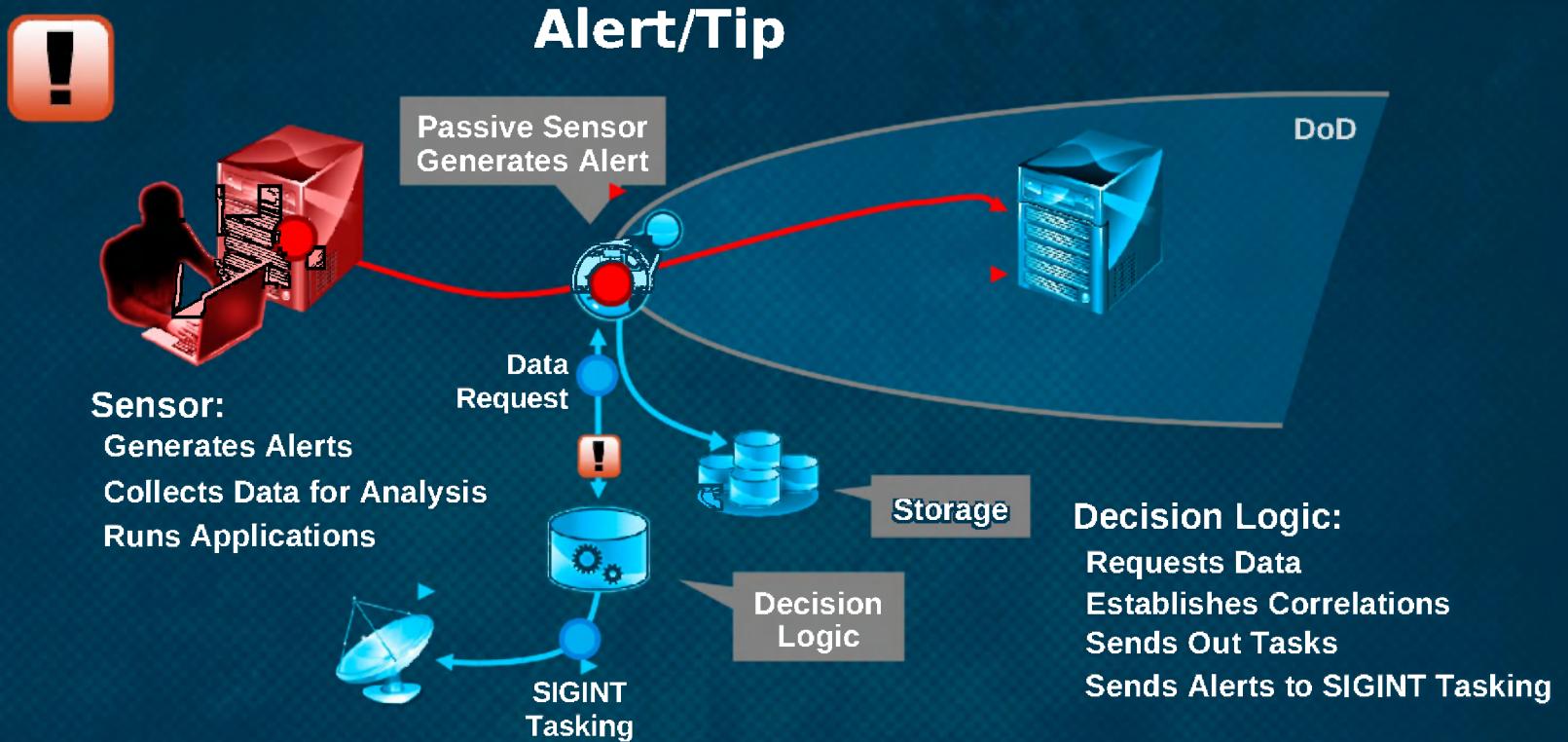


## Substitute



## Latency

Speed Adjusted



(S//REL TO USA, FVEY)

**Alert/Tip indicates the presence of malicious activity and communicates this information with the rest of the TUTELAGE enterprise and/or the SIGINT (passive/active) enterprise. Rule and Decision Logic determine whether data is stored.**

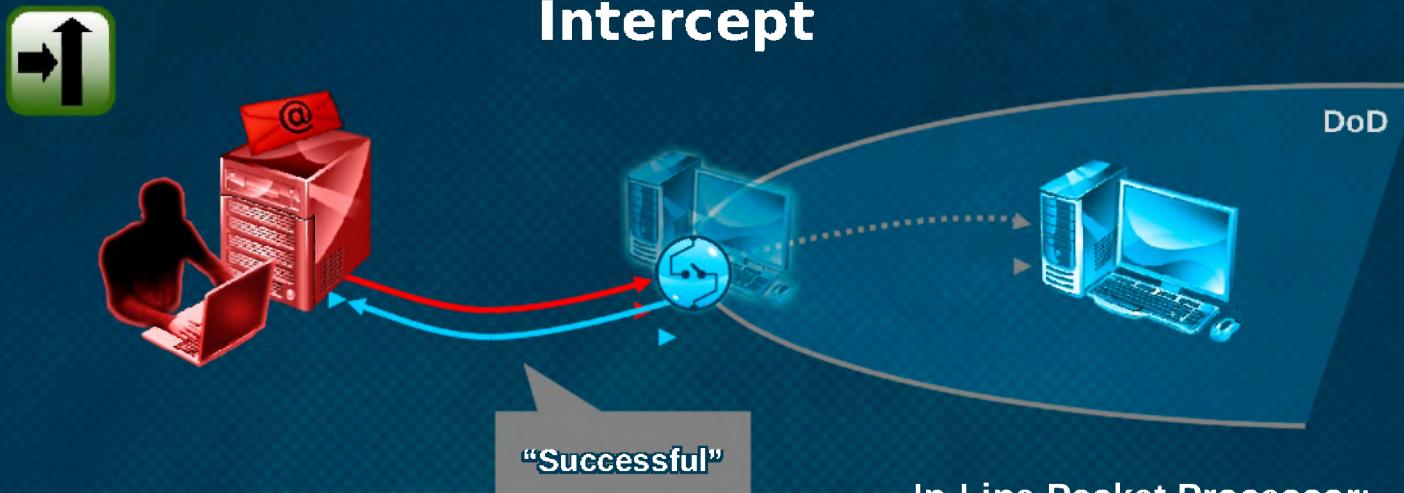
◀ MENU

SECRET//COMINT//REL TO USA,

FVEY

## TUTELAGE Capabilities

### Intercept



#### In-Line Packet Processor:

- Re-routes traffic dynamically
- Modify inbound & outbound packets
- Insert and/or delete packets

(S//REL TO USA, FVEY)

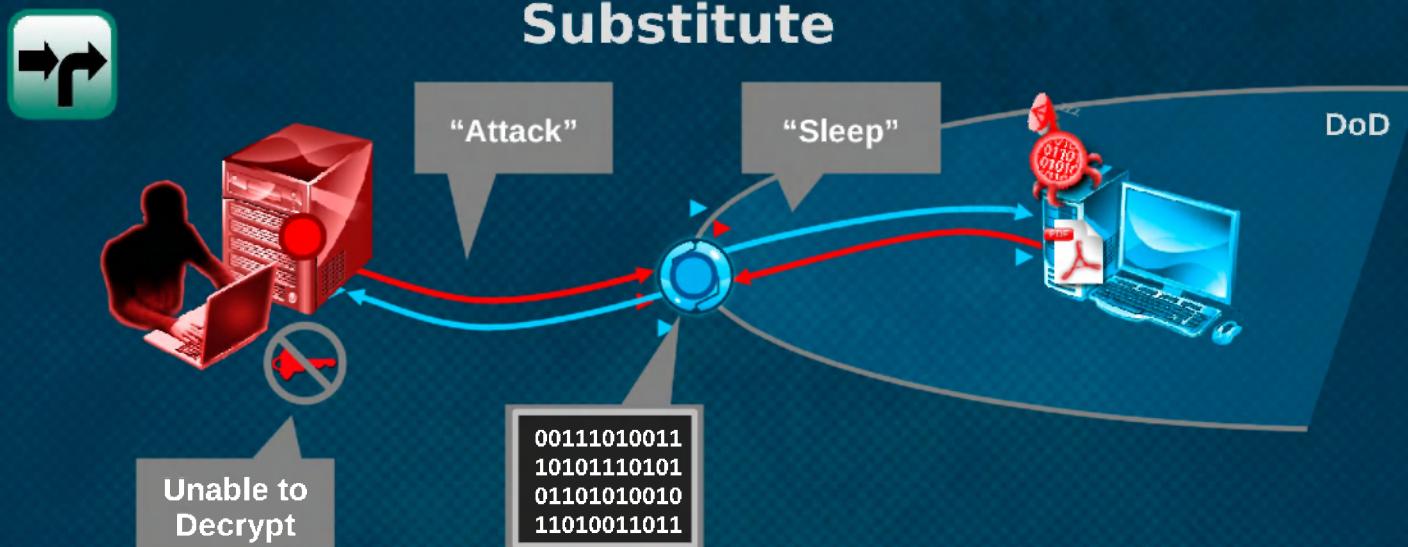
**Intercept is the means by which the TUTELAGE in-line packet processor can transparently intervene in adversarial activities, permitting the activity to appear to complete without disclosing that it did not reach/affect the intended target.**

<MENU

SECRET//COMINT//REL TO USA,

FVEY

# TUTELAGE Capabilities



(S//REL TO USA, FVEY)

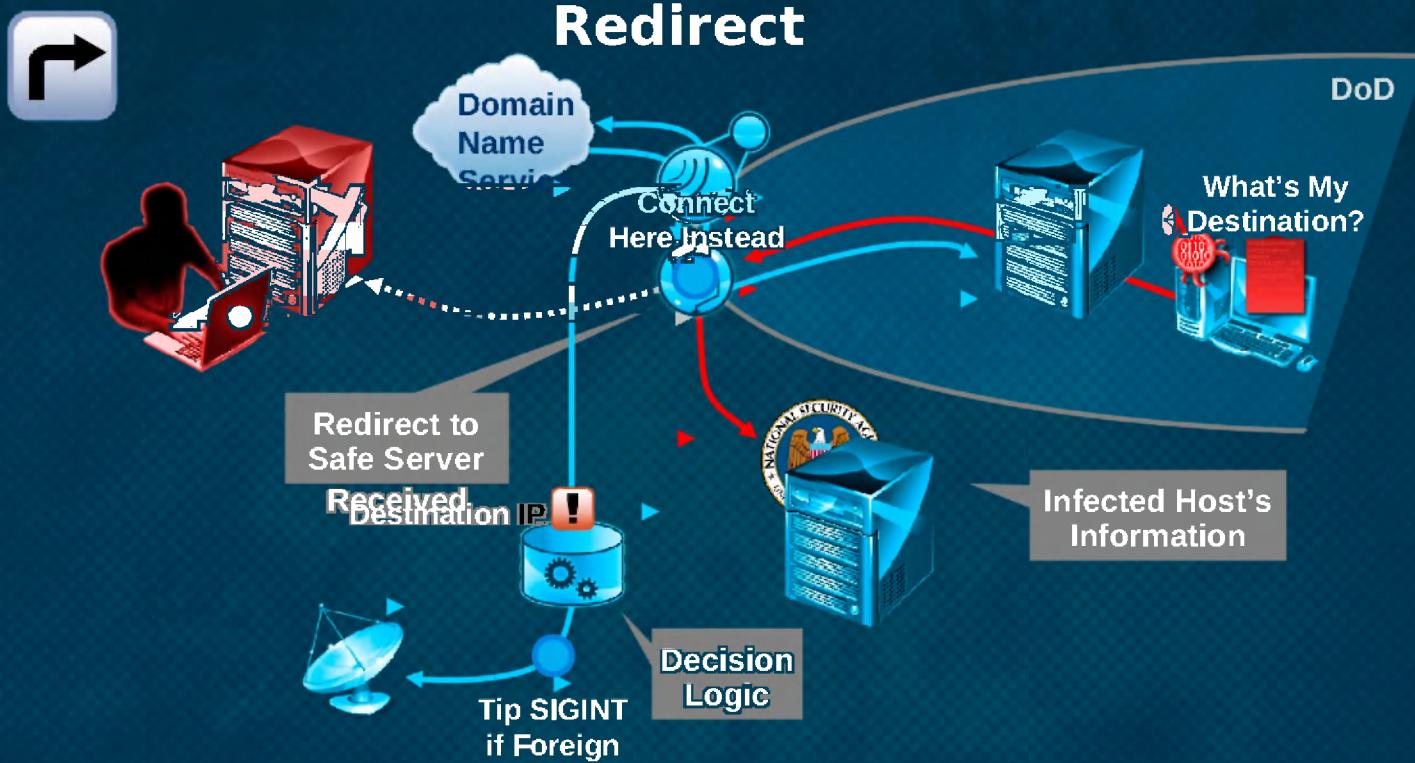
**Substitute** is the TUTELAGE in-line packet processor's ability to perform bidirectional content detection and replacement.

◀ MENU

SECRET//COMINT//REL TO USA,

FVEY

# TUTELAGE Capabilities

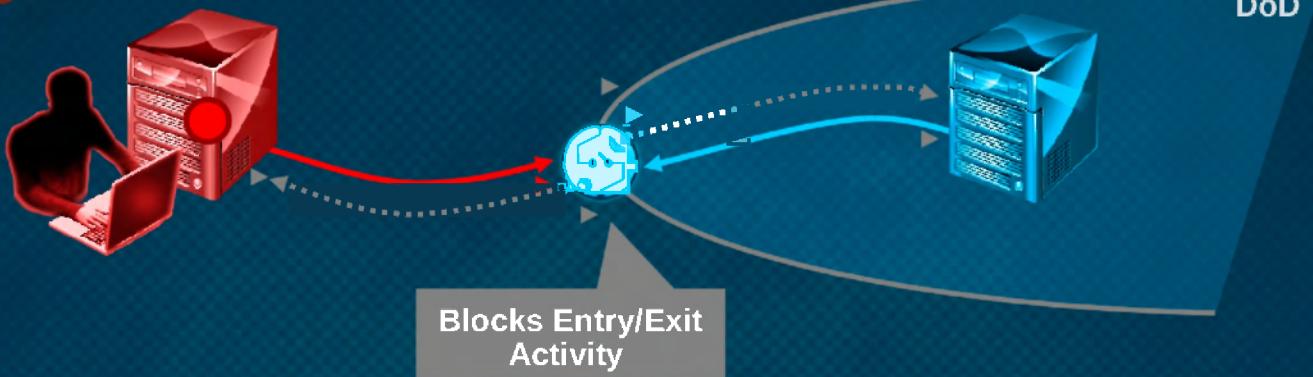


(S//REL TO USA, FVEY)

**Redirect is the TUTELAGE in-line packet processor's ability to change the course or direction of an adversarial (or adversarial induced) activity.**

# TUTELAGE Capabilities

## Block



(S//REL TO USA, FVEY)

**Block** is the means by which the TUTELAGE in-line packet processor can deny entry/exit of network activity at the Internet Access Points (IAPs) based initially on source and/or destination Internet Protocol (IP) addresses and ports.

<MENU

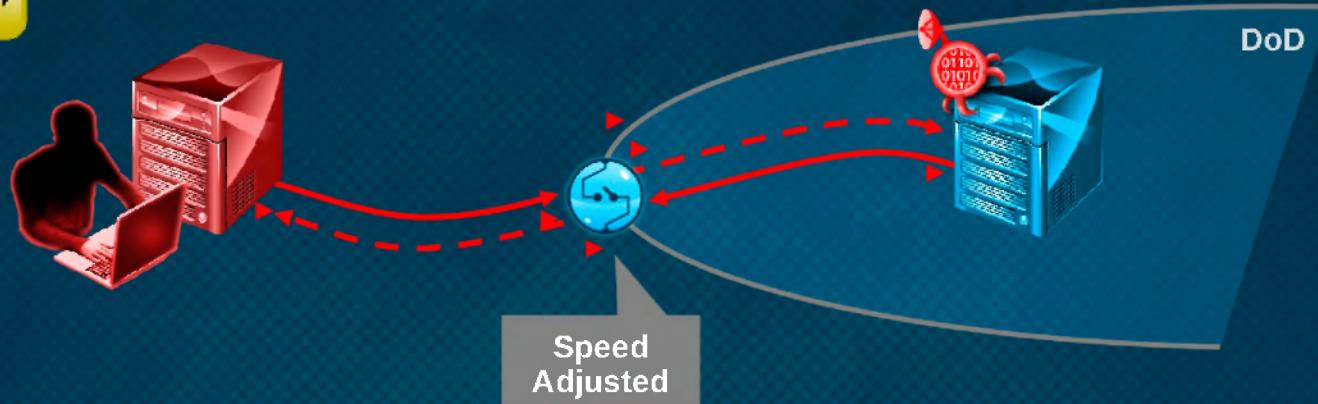
SECRET//COMINT//REL TO USA,

FVEY

## TUTELAGE Capabilities



### Latency



(S//REL TO USA, FVEY)

**Latency is the means by which the TUTELAGE in-line packet processor can stealthily vary the in/outbound speed of an adversary's activities traversing the IAPs to provide a diminished quality of service. This creates more time for other TUTELAGE capabilities to be executed.**

# How Many, How Often

**TUTELAGE currently operates against 28 major threat categories, using a total of 794 operational effects encompassed in seven capabilities (alerting/tipping, blocking, interception, sidelining, substitution, redirection and latency).**

Cyber Activity	Ops	Alert/Tip	Block	Intercept	Latency	Redirect	Substitute
				SMTP	HTTP	HTTP	DNS
Adversarial Recon	3				3		TCP
Bishop Knight	10					10	
Black Energy Bot	24						24
Blind Marksmen	77					77	
<b>Byzantine Foothold</b>	<b>96</b>		<b>1</b>	<b>12</b>		<b>83</b>	
Byzantine Viking	36	1		4		31	
Carbon Peptide	6					6	
Conficker	3						3
Cross-Domain Violations	77	77			77		
Dancing Panda	2					2	
Discovery	123			4		116	1
Eleonore Exploit Kit (TEC)	5					5	
Email	8			8			
GnomeFisher	4					4	
GnomeVision	1					1	
MakersMark	8					8	
Maverick Church	12			4		8	
Native Dancer	26			8		18	
Non Attributed Malware	13					13	
Other	3					3	
Phoenix Exploit Kit	1					1	
Technology	7					6	1
WeaselWaggle/SubtleSnow	58	1				57	
Widowkey	26	1				25	
Zeus	17	1				16	
<b>TOTAL</b>	<b>794</b>	<b>81</b>	<b>2</b>	<b>61</b>	<b>3</b>	<b>77</b>	<b>552</b>
							<b>95</b>

TUTELAGE posture against major threats as of 11 February 2011.

UNCLASSIFIED//FOUO

# FUTURE CAPABILITIES

UNCLASSIFIED//FOUO

# Upgrades & What They Mean

**Upgrade to 10G Sensor provides additional capabilities and enables future upgrades:**

- **Immediate Benefits:**

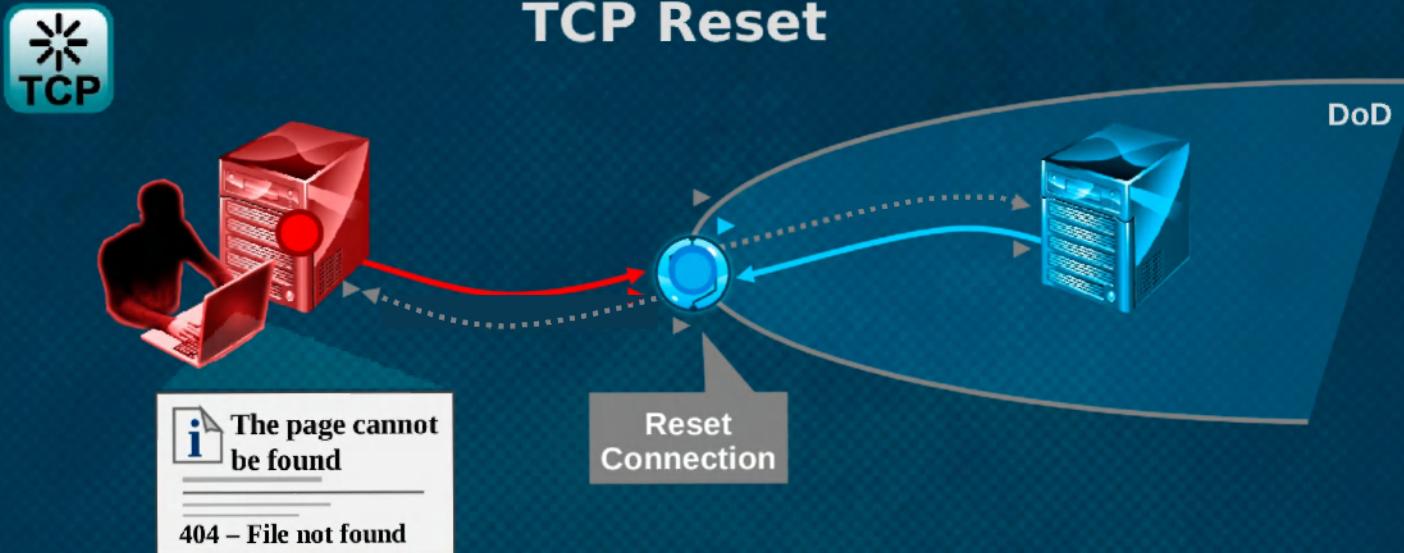
- Increased speed and capacity
- TS//SI signatures
- Full Snort (Current sensors use packet-based Snort. 10G sensors use session-based Snort.)
- Multi-event Snort

- **Future Upgrades:**

- POPQUIZ: Real-time behavioral analytics
- GNOMEVISION: De-obfuscation of malicious packages
- Cryptanalytic Capabilities
- Netflow: Traffic analysis with GHOSTMACHINE

# Latest Future TUTELAGE Capability

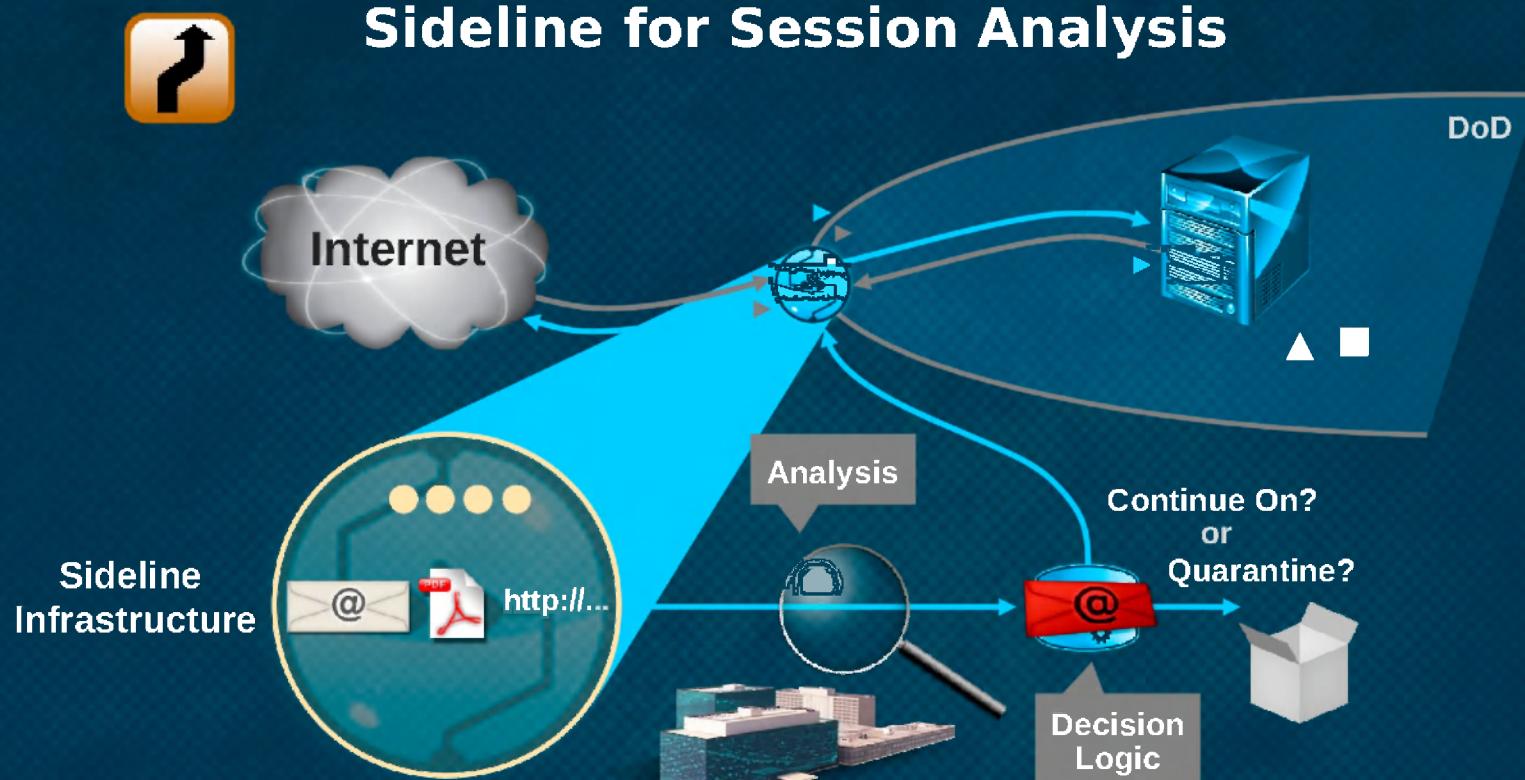
## TCP Reset



(S//SI//REL TO USA, FVEY)

**TCP Reset prevents malicious activity by breaking the connection.**

# Future TUTELAGE Capabilities



(S//REL TO USA, FVEY)

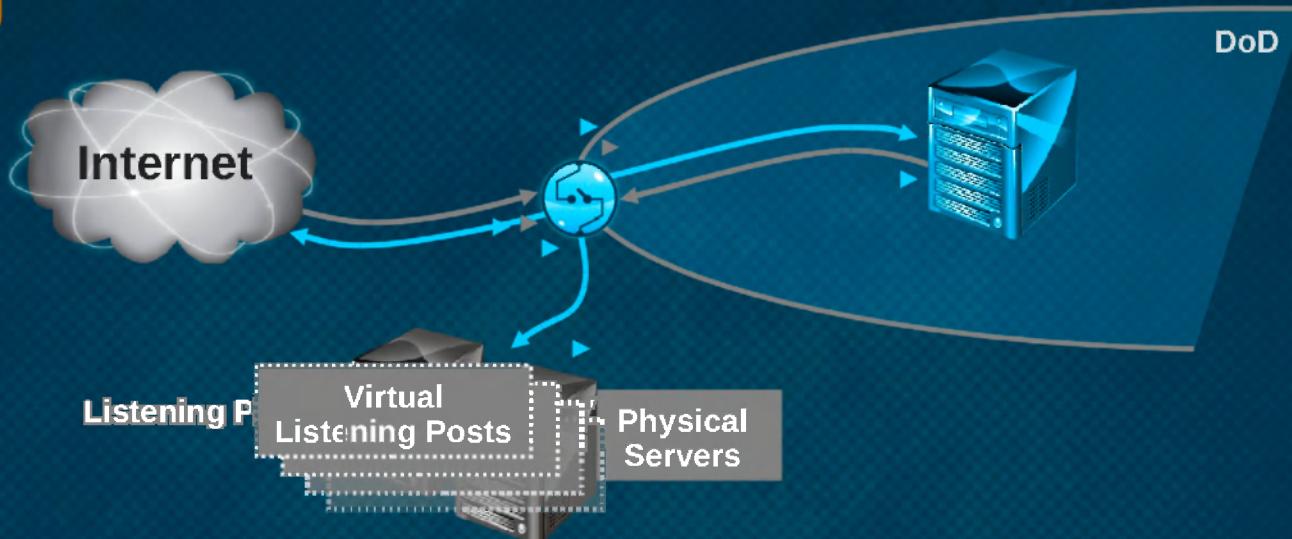
**Sidelining is an intentional redirection of an activity to a secondary level of intervention where an intermediate host(s) (e.g. Listening Post, Quarantine, etc.) is staged to provide additional processing/manipulation to better engage and/or thwart adversarial activity.**

# Future TUTELAGE Capabilities



## Sideline for Listening Posts

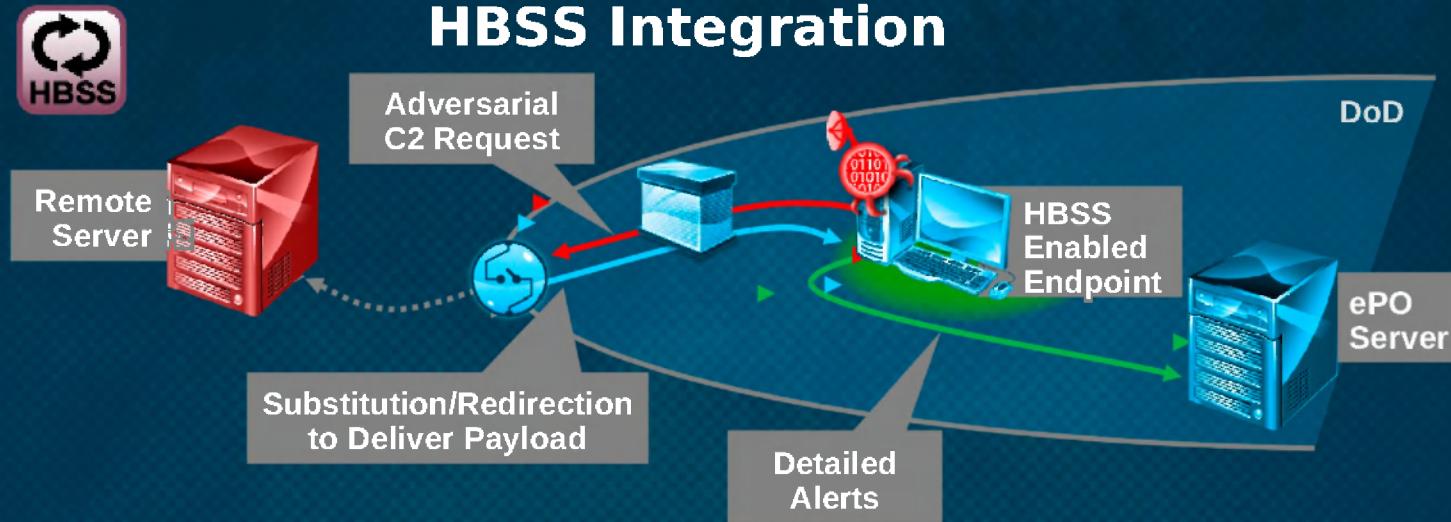
**Today:**  
DNS Interdiction



(S//REL TO USA, FVEY)

**Sidelining is an intentional redirection of an activity to a secondary level of intervention where an intermediate host(s) (e.g. Listening Post, Quarantine, etc.) is staged to provide additional processing/manipulation to better engage and/or thwart adversarial activity.**

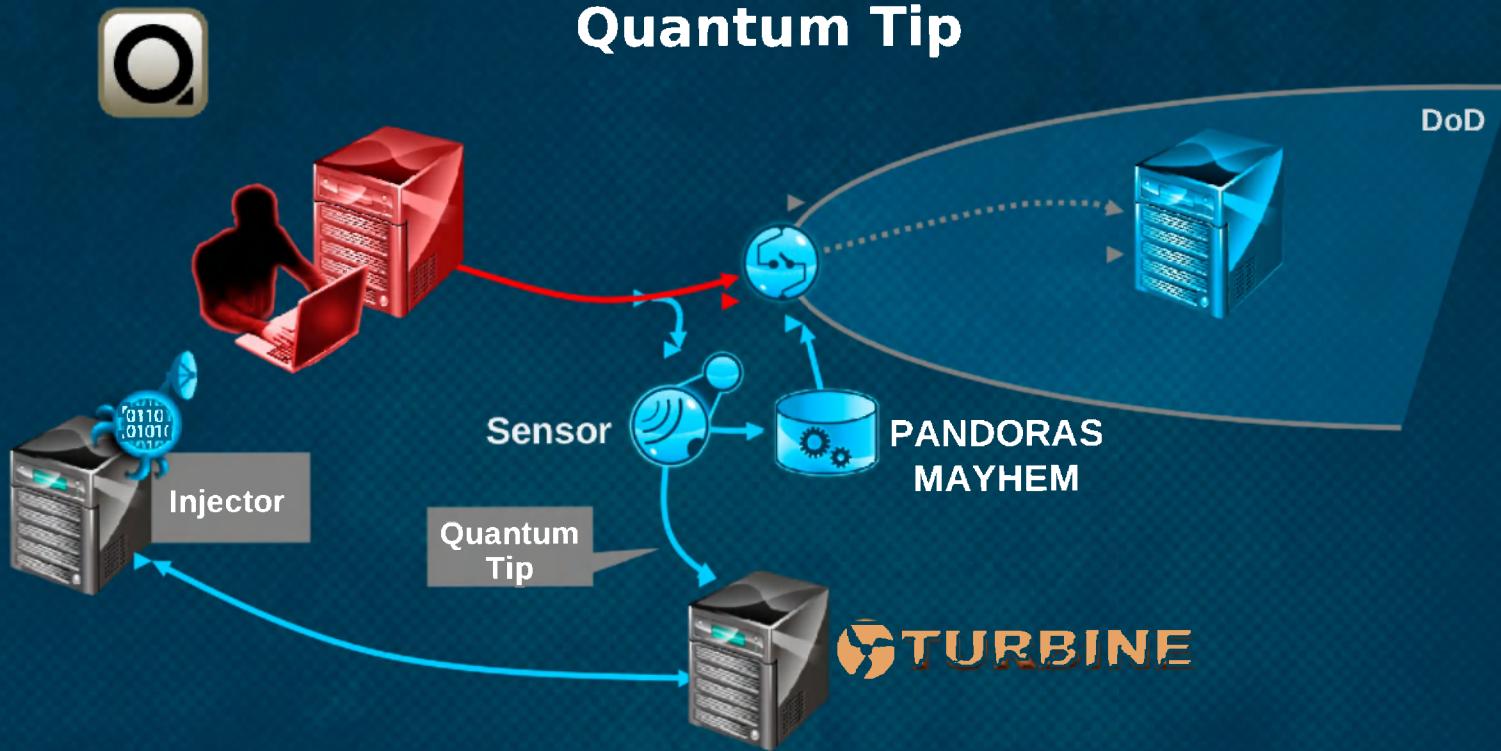
# Future TUTELAGE Capabilities



(S//SI//REL TO USA, FVEY)

**Integrating with the DOD's Host-Based Security System allows malicious activity detected through classified signatures in TUTELAGE to be dealt with at the host level. Using HBSS, TUTELAGE can trigger less sensitive alerts to local network administrators.**

# Future TUTELAGE Capabilities



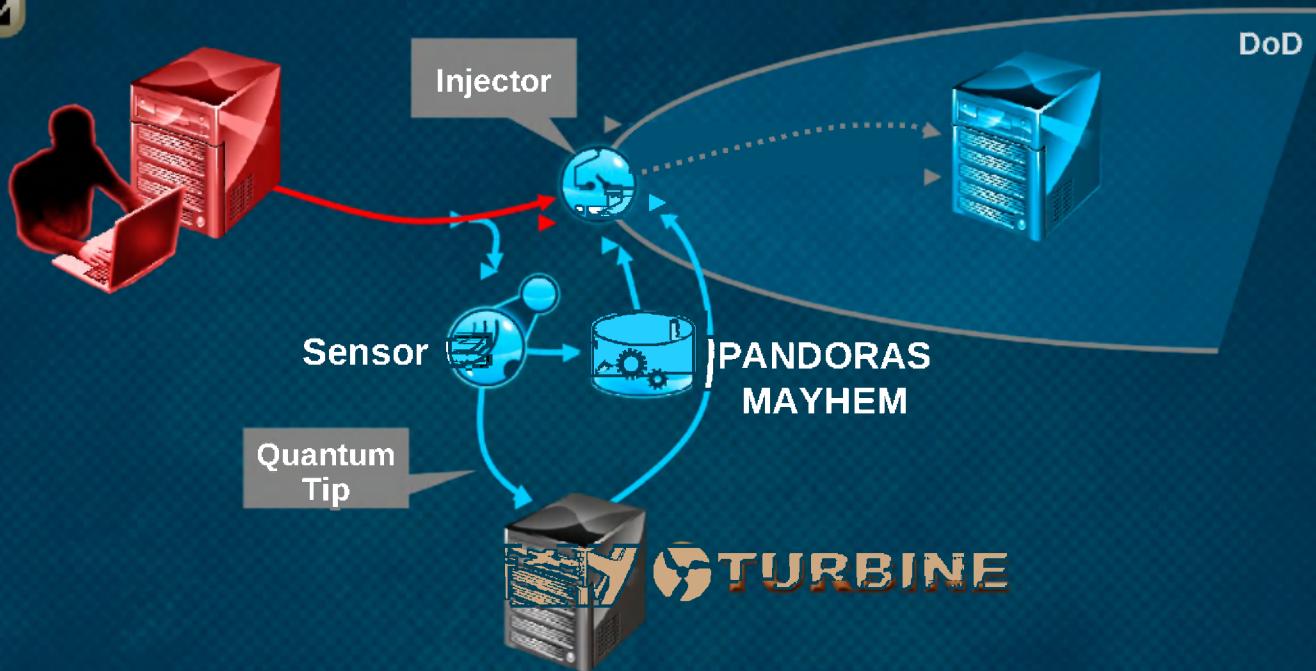
(TS//SI//REL TO USA, FVEY)

**TUTELAGE can tip QUANTUM to enable offensive action in adversary space.**

# Future TUTELAGE Capabilities



## Quantum Shooter

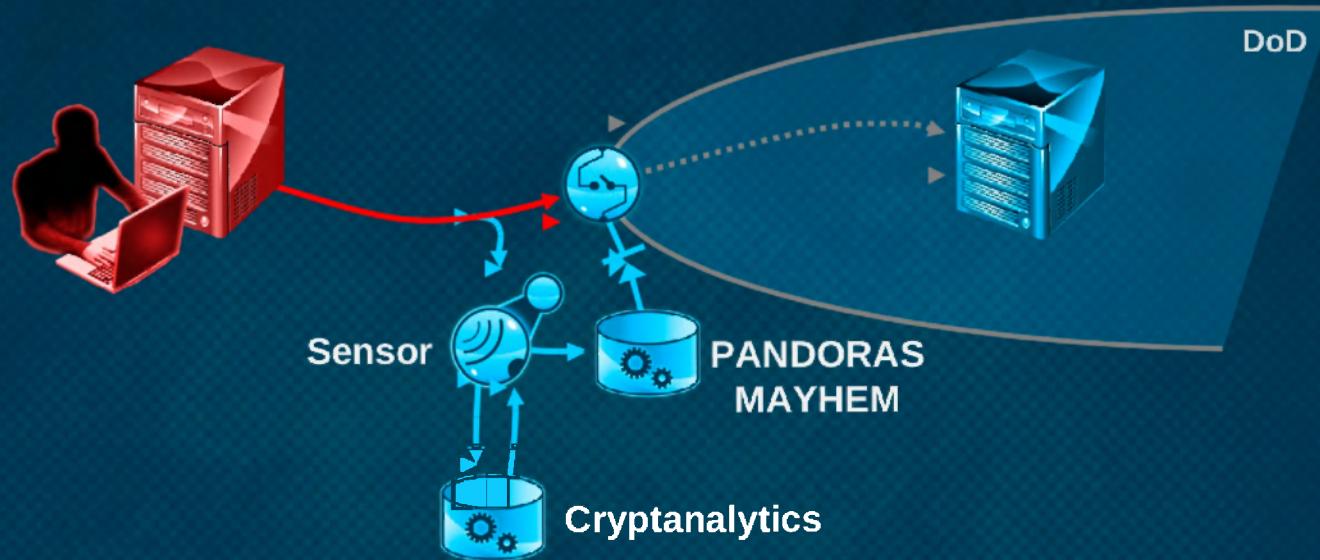


(TS//SI//REL TO USA, FVEY)

**TUTELAGE can tip QUANTUM to enable offensive action in adversary space.**

# Future TUTELAGE Capabilities

## Real Time Cryptanalytics



(TS//SI//REL TO USA, FVEY)

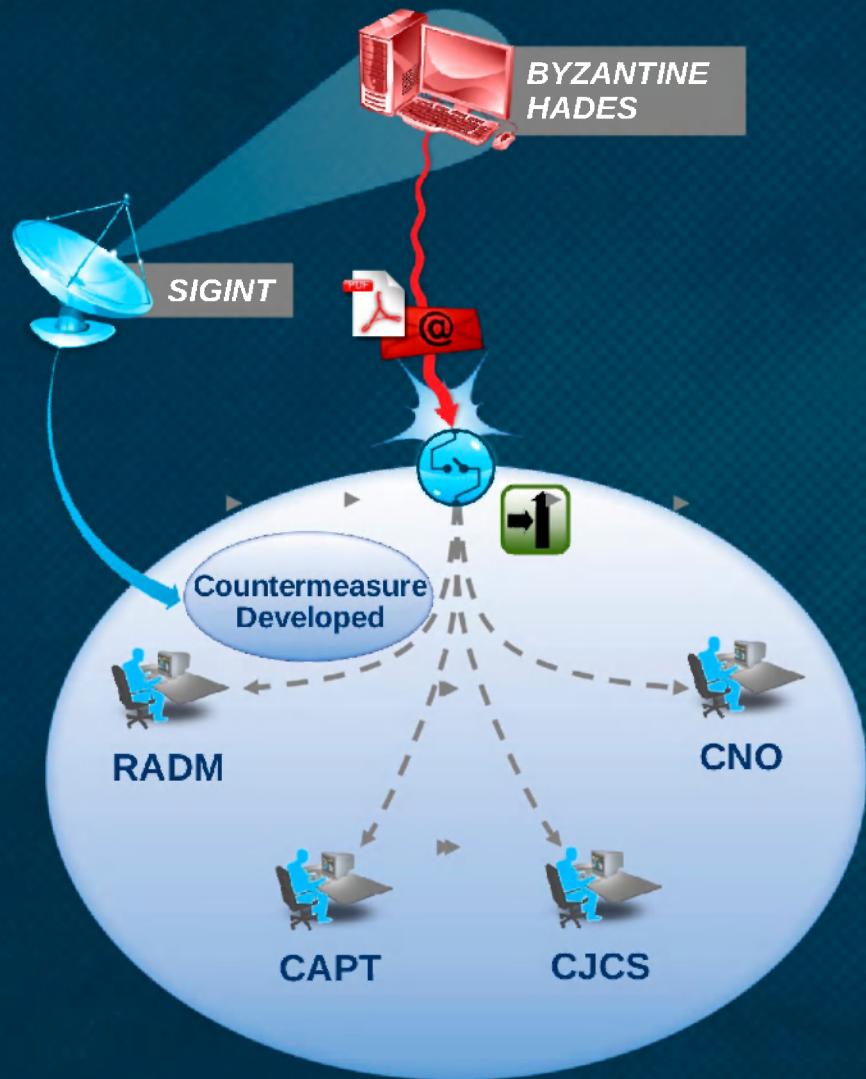
**Real-time cryptanalytics allows Quantum operations to take place at net-speed.**

UNCLASSIFIED//FOUO

# OPS SUCCESS STORIES

UNCLASSIFIED//FOUO

# U.S. Military Leaders Defended



- Based on information from SIGINT collection, a TUTELAGE countermeasure was developed and deployed in 2009 for a particular BYZANTINE HADES attack.
- On October 21<sup>st</sup> and 22<sup>nd</sup> 2010, the spear-phishing attack was launched. The attack targeted four users, including the Chairman of the Joint Chiefs of Staff and the Chief of Naval Operations, with a carefully disguised malicious PDF.
- NTOC operated the countermeasure and the attack was thwarted.

# WAG Attempts to Deliver Holiday Present to DoD

## 23 December

- NTOC-TX calls ops center advising of phishing campaign with “Merry Christmas” subject associated with WAG actors
- WAG actors attempted to use ZEUS malware to exfiltrate documents
- NTOC-TX did malware analysis and identified 2 new callback domains
- In < 3 hours, received CyberCommand approval and placed domains on DNS interdiction



## 30 December

- NTOC-TX notices new spike in WAG mail signature
- NTOC-TX discovers new callback domain
- In < 20 minutes, received approval and placed domain on DNS interdiction
- NTOC-W confirmed same malware from Xmas themed event

# AMULETSTELLAR Spearphishing... Trying to Make New Friends



- In SIGINT, NTOC observed AMULETSTELLAR use of [REDACTED]@yahoo.com email account
- On Christmas Day, account was used to generate LinkedIn requests to 10 general and flag grade officers
- NTOC leveraged TUTELAGE and SIGINT for further discovery of activity
- In coordination with CyberCommand,
  - Published 10 advisories
  - Identified 2 additional LinkedIn accounts
  - Deployed 4 countermeasures
  - Intercepted over 2000 emails from AMULETSTELLAR actors

# Combating the Low Orbit Ion Cannon (LOIC)

- The open-source LOIC tool has been used by “Anonymous” and others in several DDoS attacks.
- NTOC developed signatures to detect specific content strings generated by this tool.
- For example, for packets containing the string “Sweet\_dreams\_from\_AnonOPs” TUTELAGE will perform an ACL Block against the offending IP once a threshold is met.
- Observed here is traffic from an ongoing DDoS against several DoD IPs. TUTELAGE is blocking the malicious IP from communicating with any DoD machines.



# QUESTIONS?