Case Studies of Integrated Cyber Operation Techniques

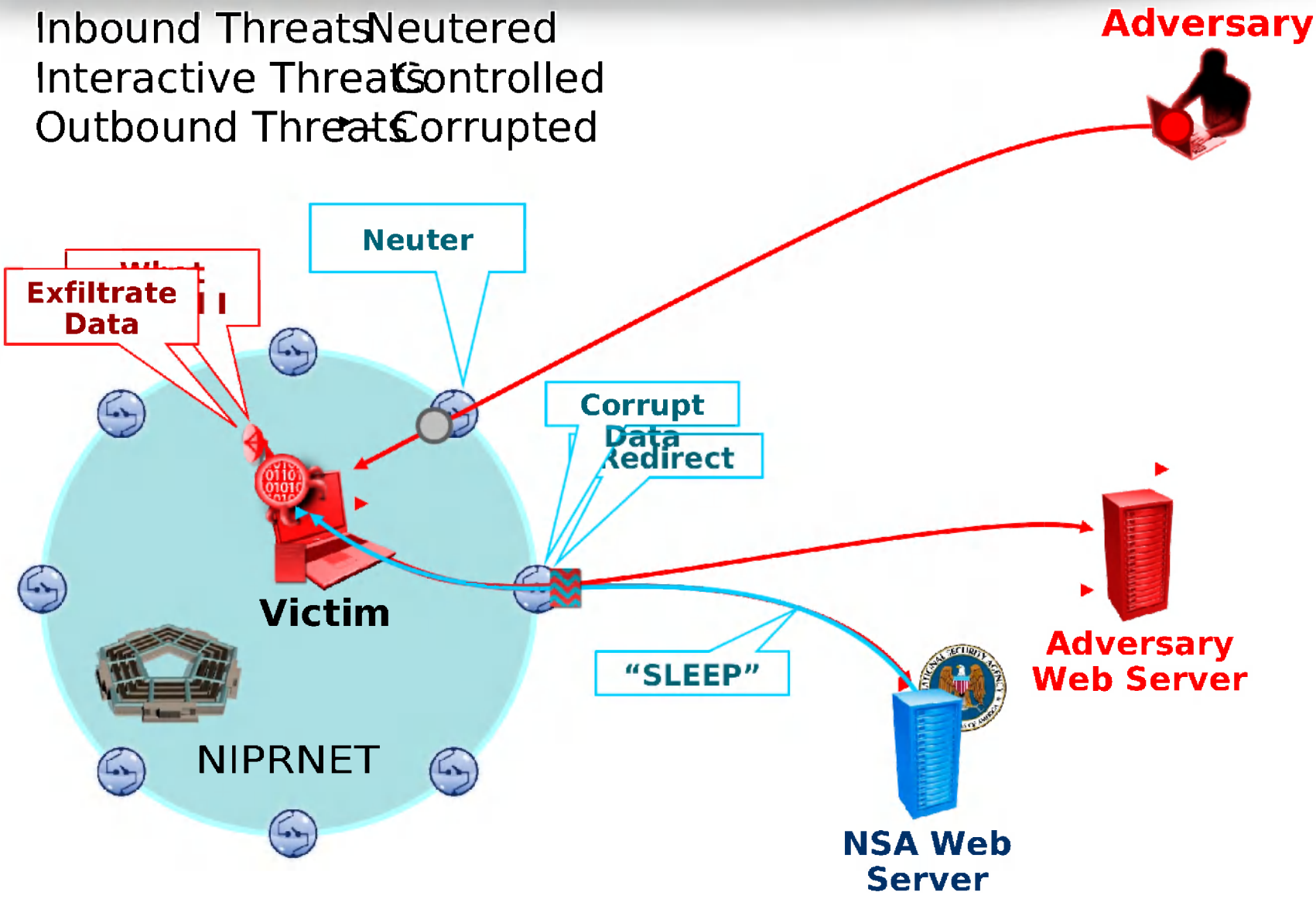
[redacted]

NSA/CSS Threat Operations Center

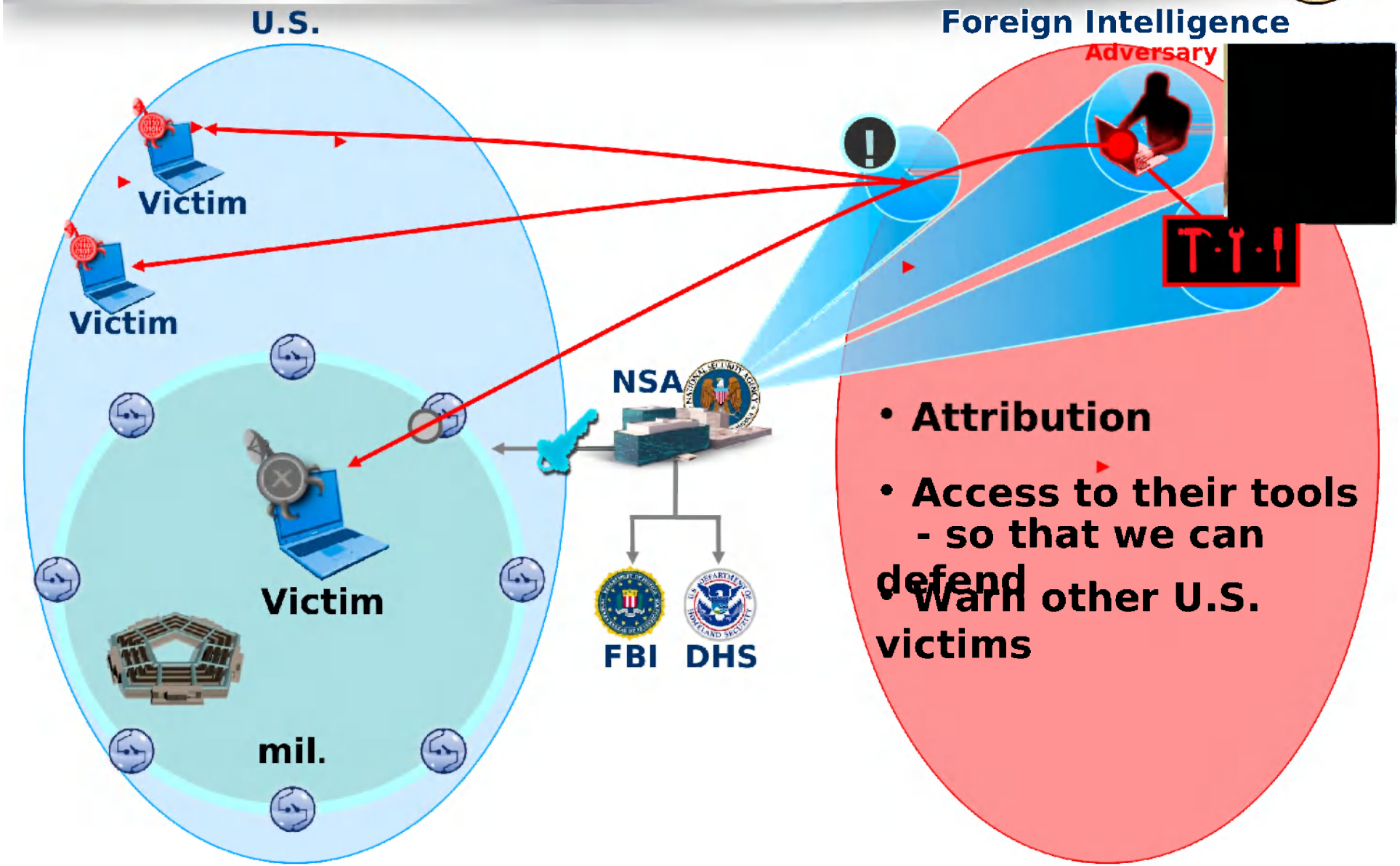
VS

(U//FOUO) TUTELAGE: Dynamic Defense

Inbound Threats → Neutered
Interactive Threats → Controlled
Outbound Threats → Corrupted



(S//REL) Foreign Intelligence in Support of Dynamic Defense



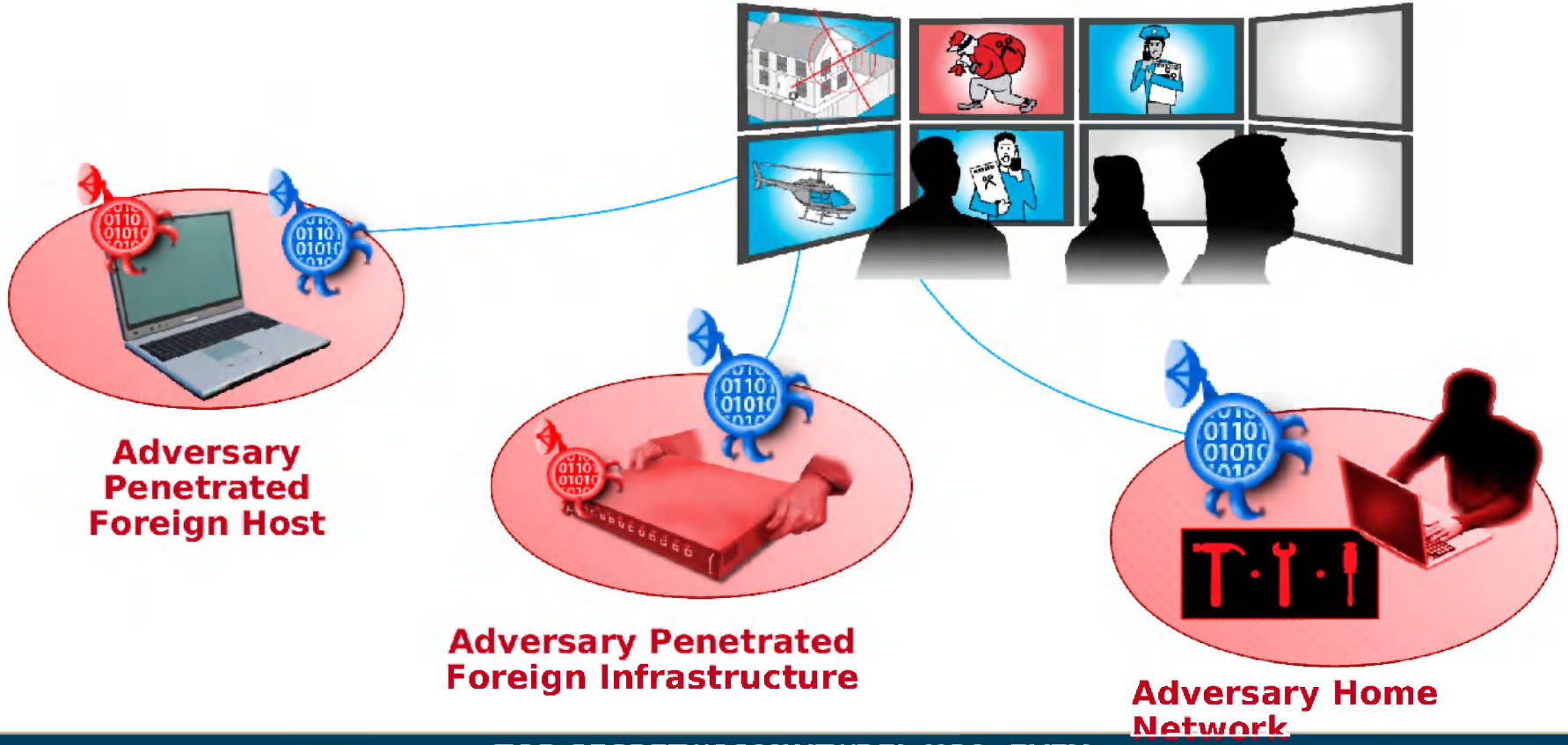
(U//FOUO) Counter-CNE: Support to CND

S//REL) Use CNE to penetrate the operations of foreign cyber actors

U) Two major classes of CNE techniques

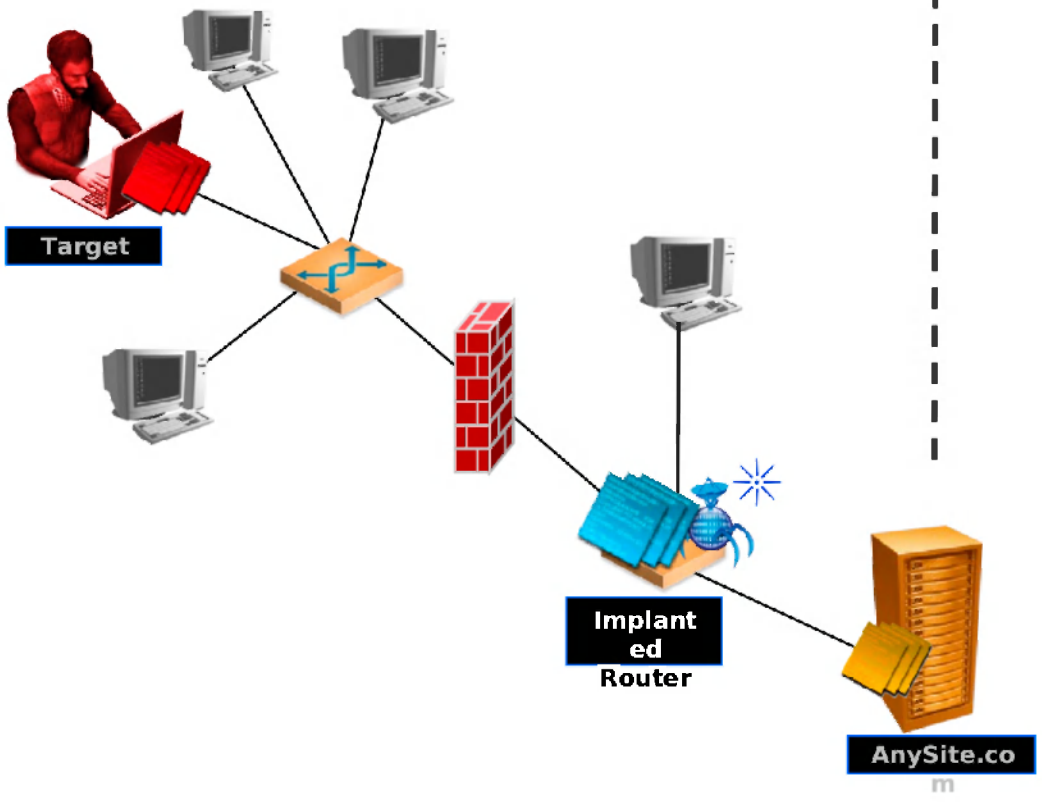
- (U) Man-in-the-middle
- (U) Man-on-the-side

U//FOUO) Steal their tools, tradecraft, targets and take

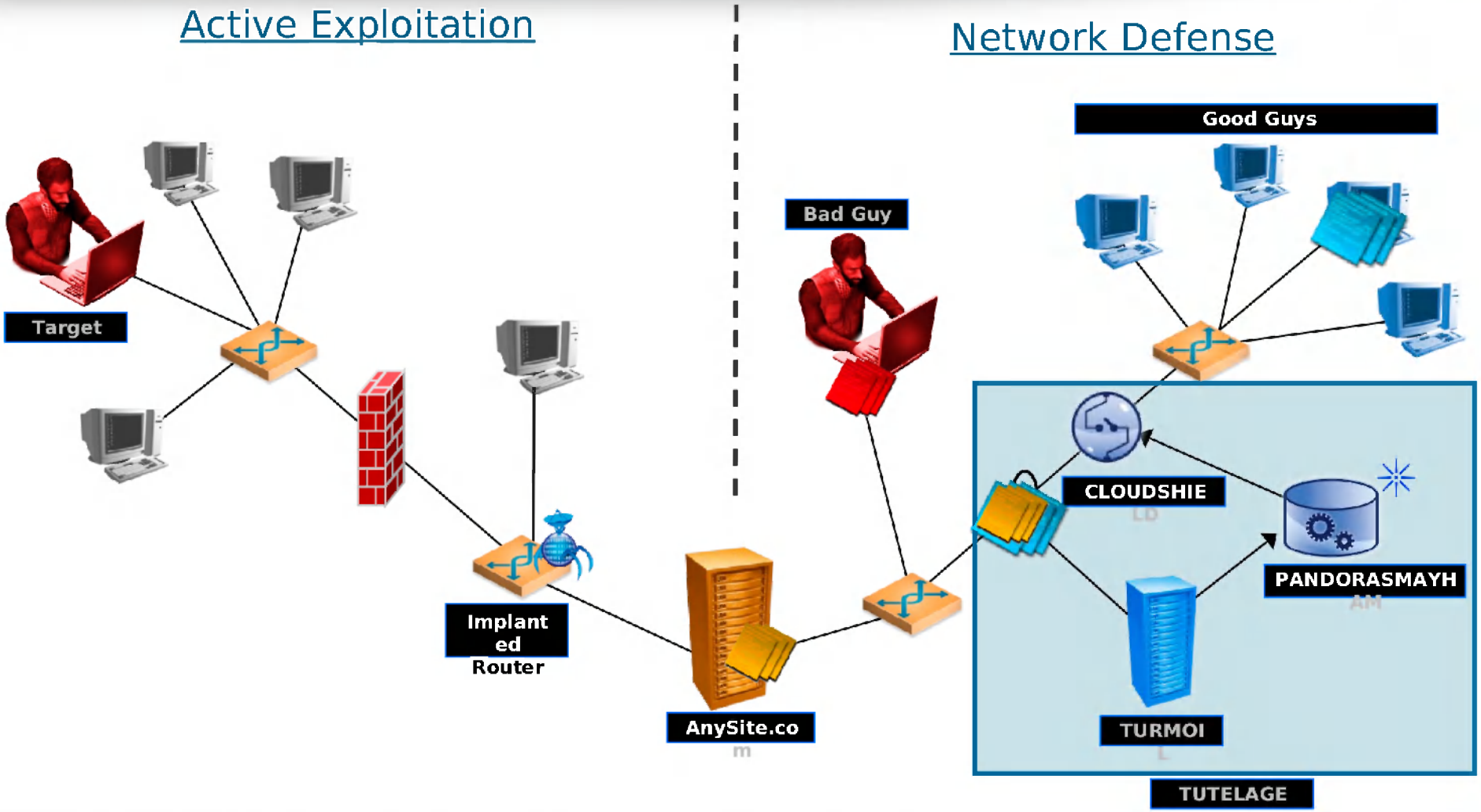


(U) Man-in-the-Middle Has Multiple Uses

Active Exploitation



(U) Man-in-the-Middle Has Multiple Uses



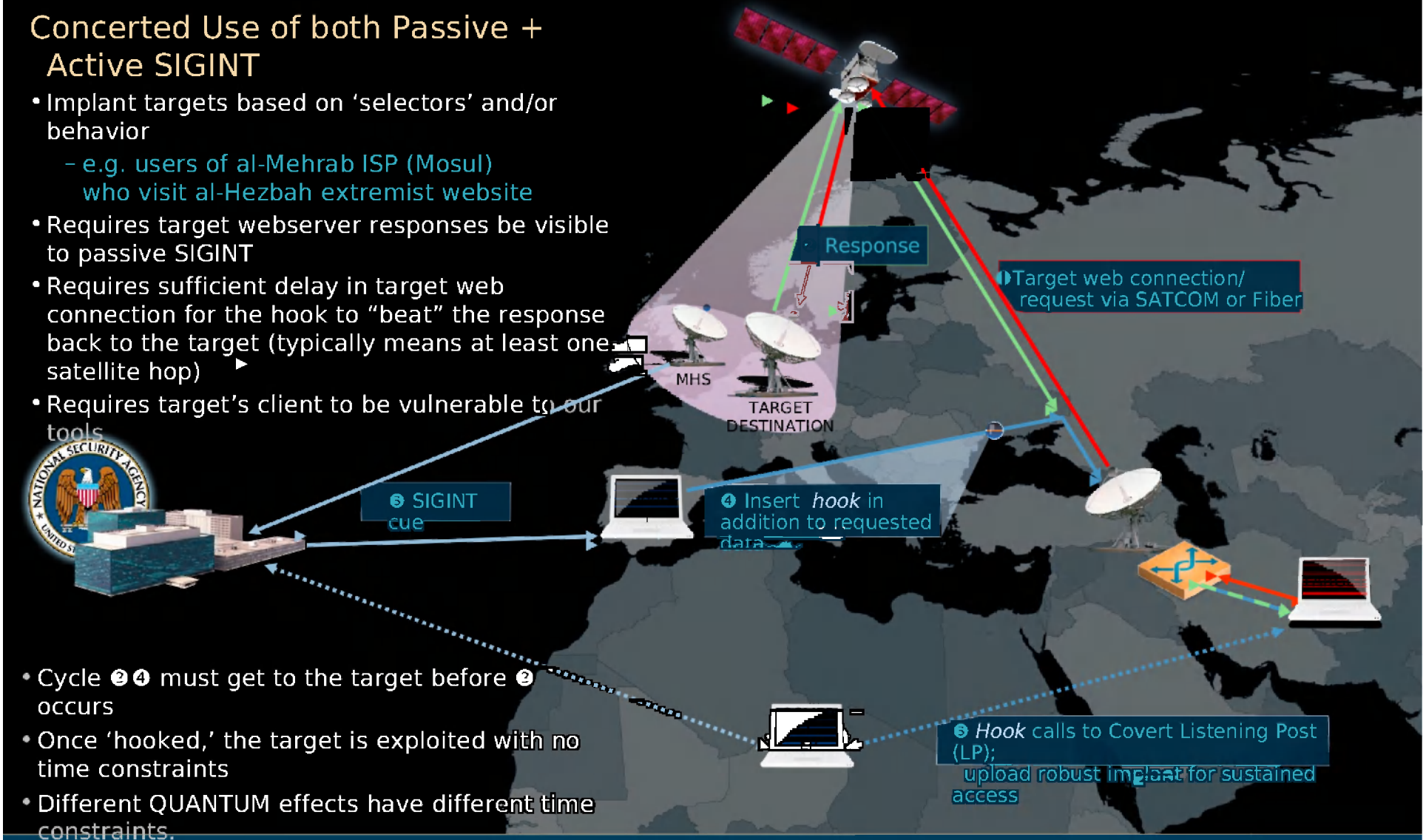
S//REL) TUTELAGE is a man-in-the-middle technique

(U//FOUO) Using TUTELAGE to enable active exploitation is integrated cyber operations.

(S//REL) QUANTUMTHEORY: Man-on-the-Side Active Exploitation

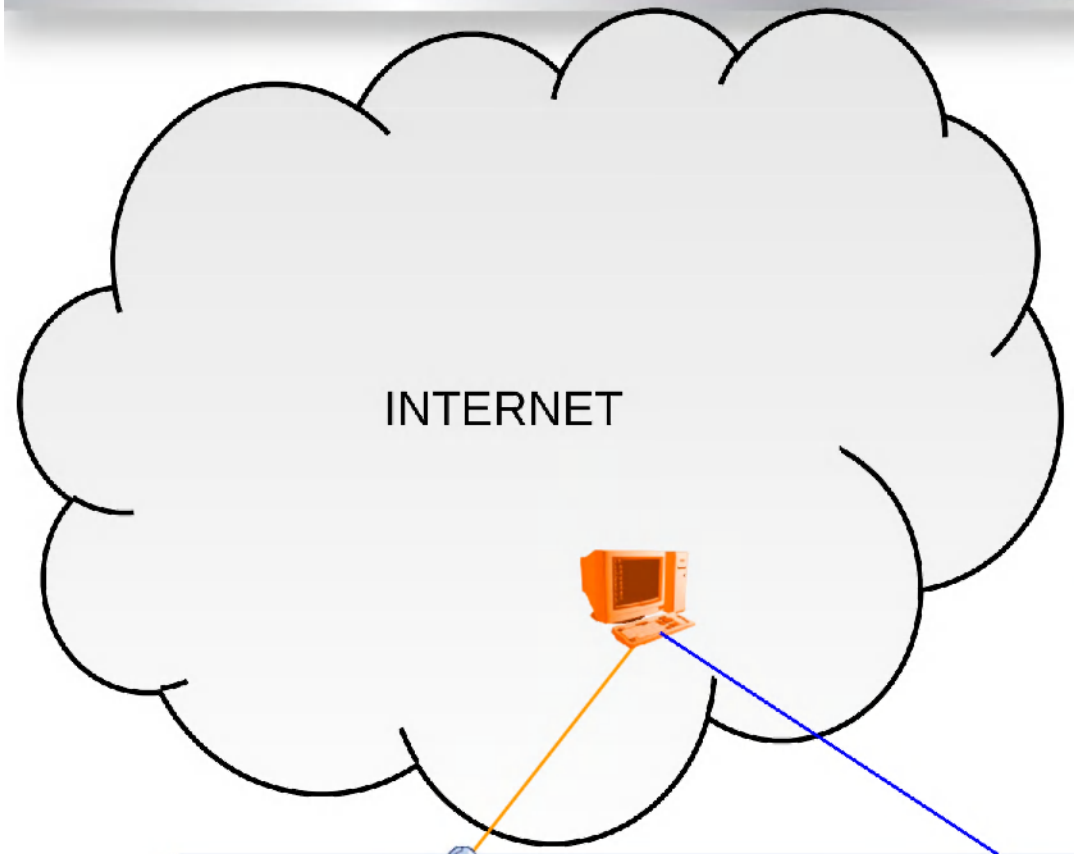
Concerted Use of both Passive + Active SIGINT

- Implant targets based on 'selectors' and/or behavior
  - e.g. users of al-Mehrab ISP (Mosul) who visit al-Hezbah extremist website
- Requires target webserver responses be visible to passive SIGINT
- Requires sufficient delay in target web connection for the hook to "beat" the response back to the target (typically means at least one satellite hop)
- Requires target's client to be vulnerable to our tools

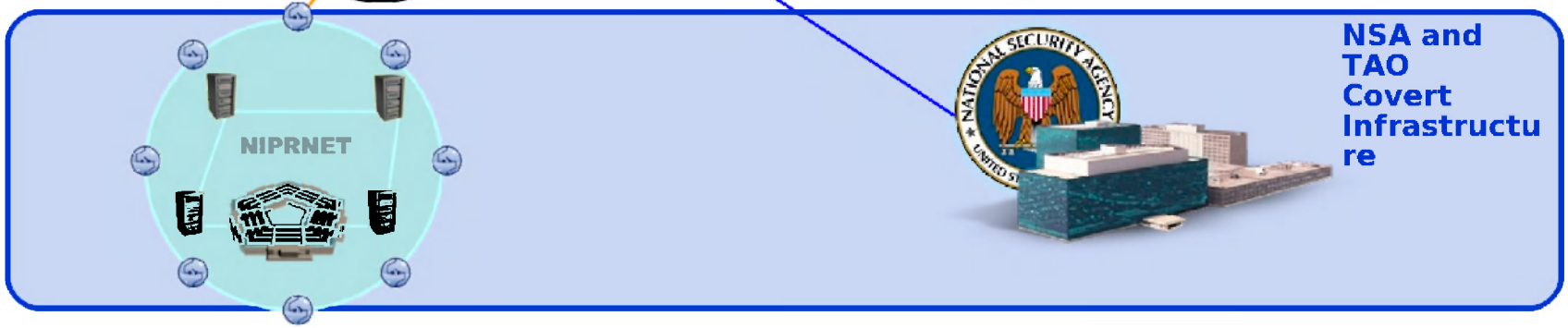


- Cycle ❷❹ must get to the target before ❷ occurs
- Once 'hooked,' the target is exploited with no time constraints
- Different QUANTUM effects have different time constraints.

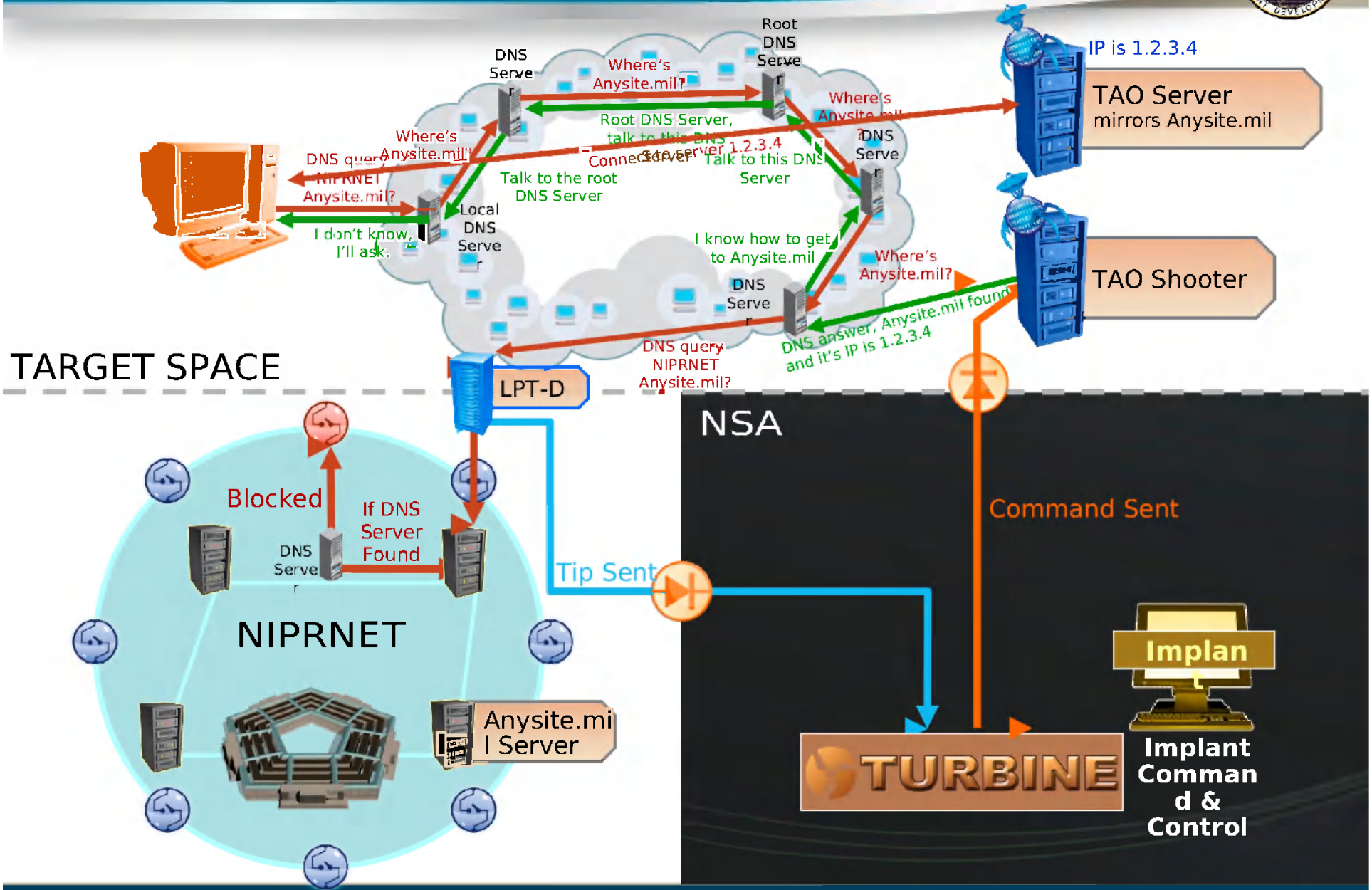
(U//FOUO) BOXINGRUMBLE Case Study



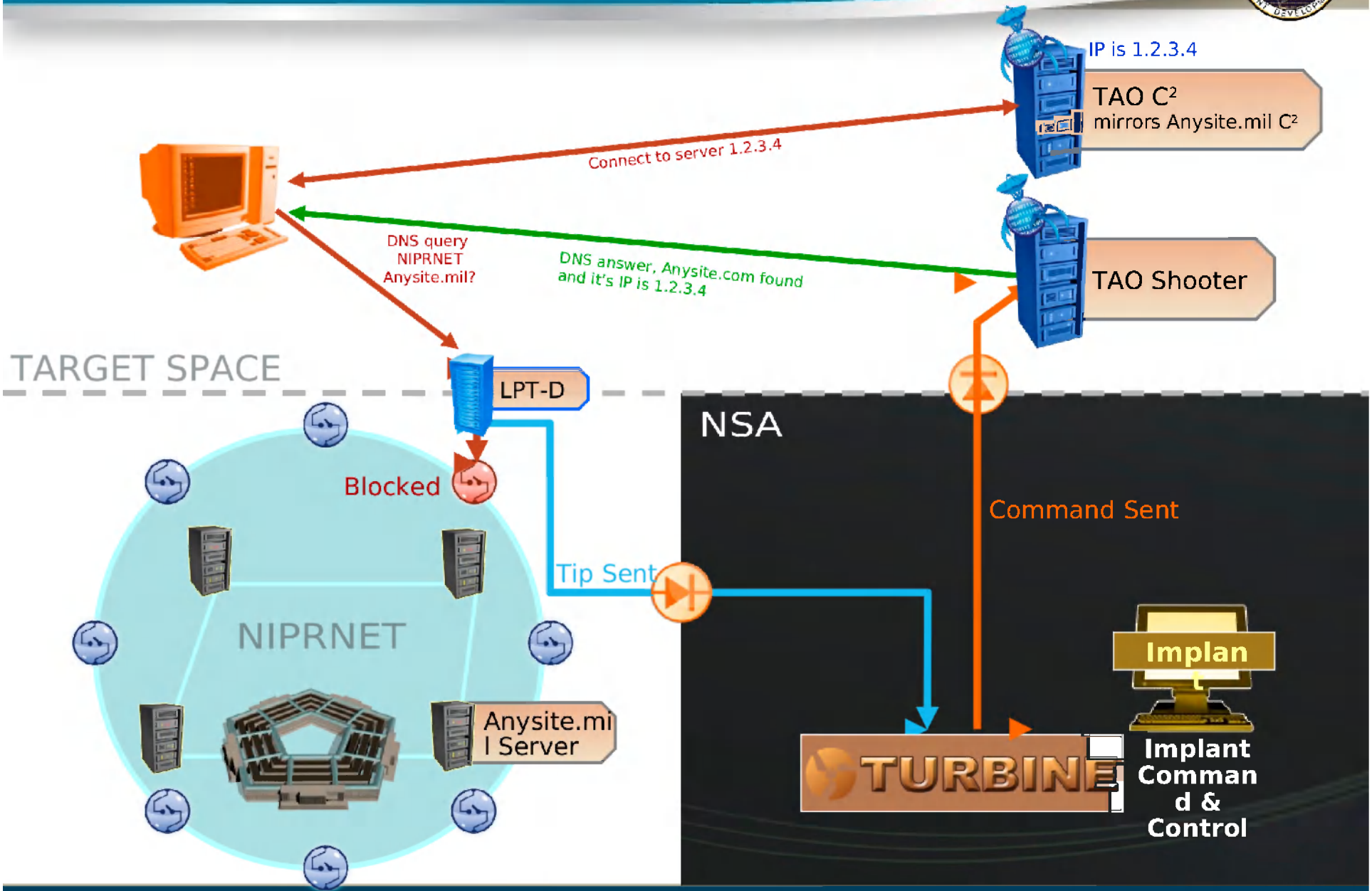
- (S//REL) DNS requests entering NIPRnet domain
  - (S//REL) Destination IP not a NIPRnet DNS server
  - (S//REL) Domain name not within NIPRnet
- (S//REL) DNS behavior of host is suspicious but not dangerous
- (TS//SI//REL) TAO uses QUANTUMDNS to redirect the requesting host



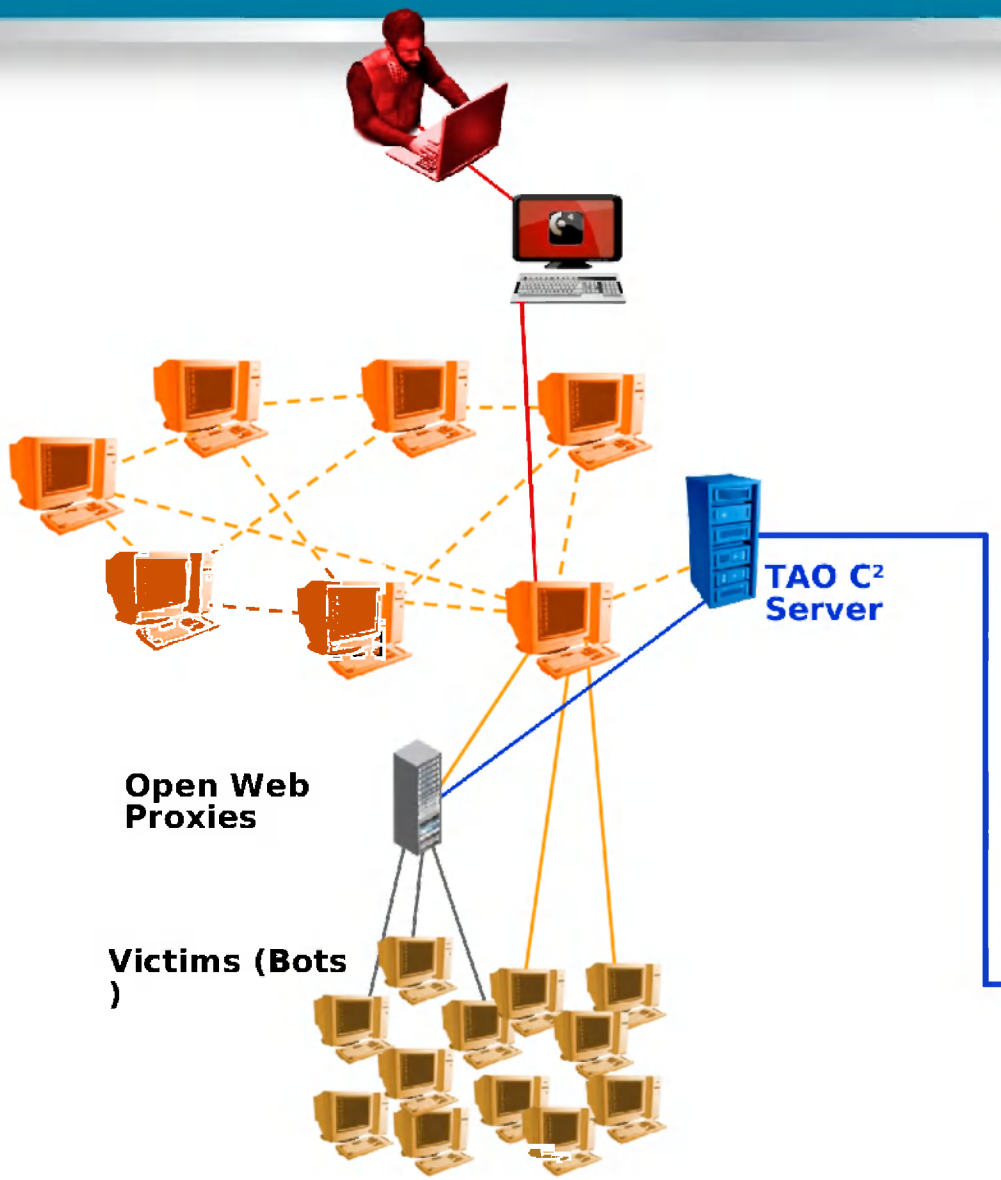
(S//REL) QUANTUMDNS: An Integrated Cyber Operation



(S//REL) QUANTUMDNS: As Used Against BOXINGRUMBLE

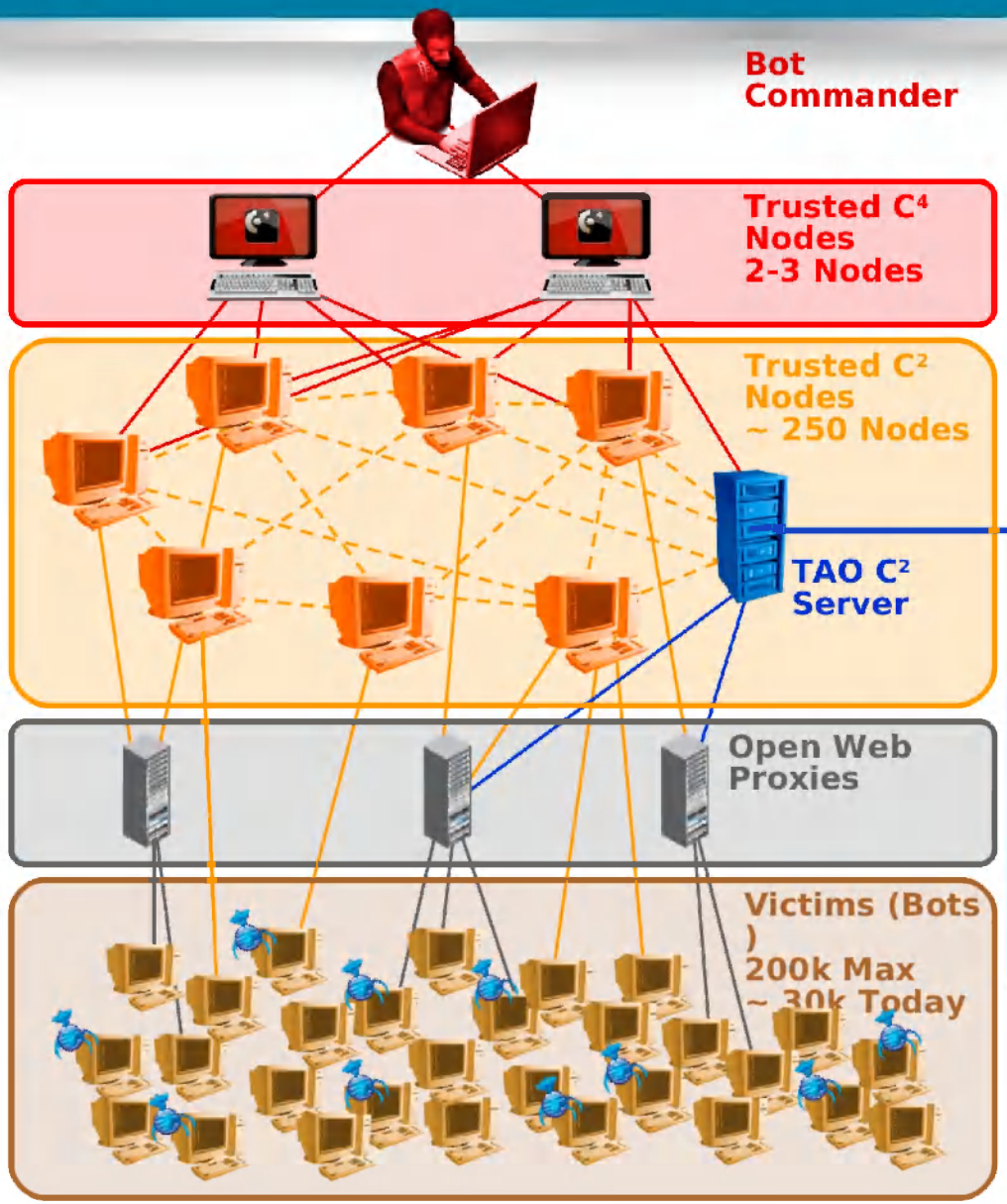


(U//FOUO) BOXINGRUMBLE Case Study



- (TS//SI//REL) TAO establishes itself as a trusted C2 node
- (U//FOUO) Captured traffic indicates the existence of a bot net
  - (S//REL) Command and control split into two layers (C2 and C4)
  - (S//REL) C2 layer has a peer-to-peer mesh network topology with direct connection to a C4 node
- (S//REL) C2 nodes connect directly to victims as well as through open web proxies

(U//FOUO) BOXINGRUMBLE Case Study



- (TS//SI//REL)TAO C2 server can see all bot tasking
- (TS//SI//REL) TAO C2 server can push tasking
- (S//REL) BOXINGRUMBLE bots
  - (S//REL) ~ 45% Vietnamese dissidents
  - (S//REL) ~45% Chinese dissidents
  - (S//REL) ~10% Other
- (TS//SI//REL) Adding BOXINGRUMBLE bots to DEFIANTWARRIOR

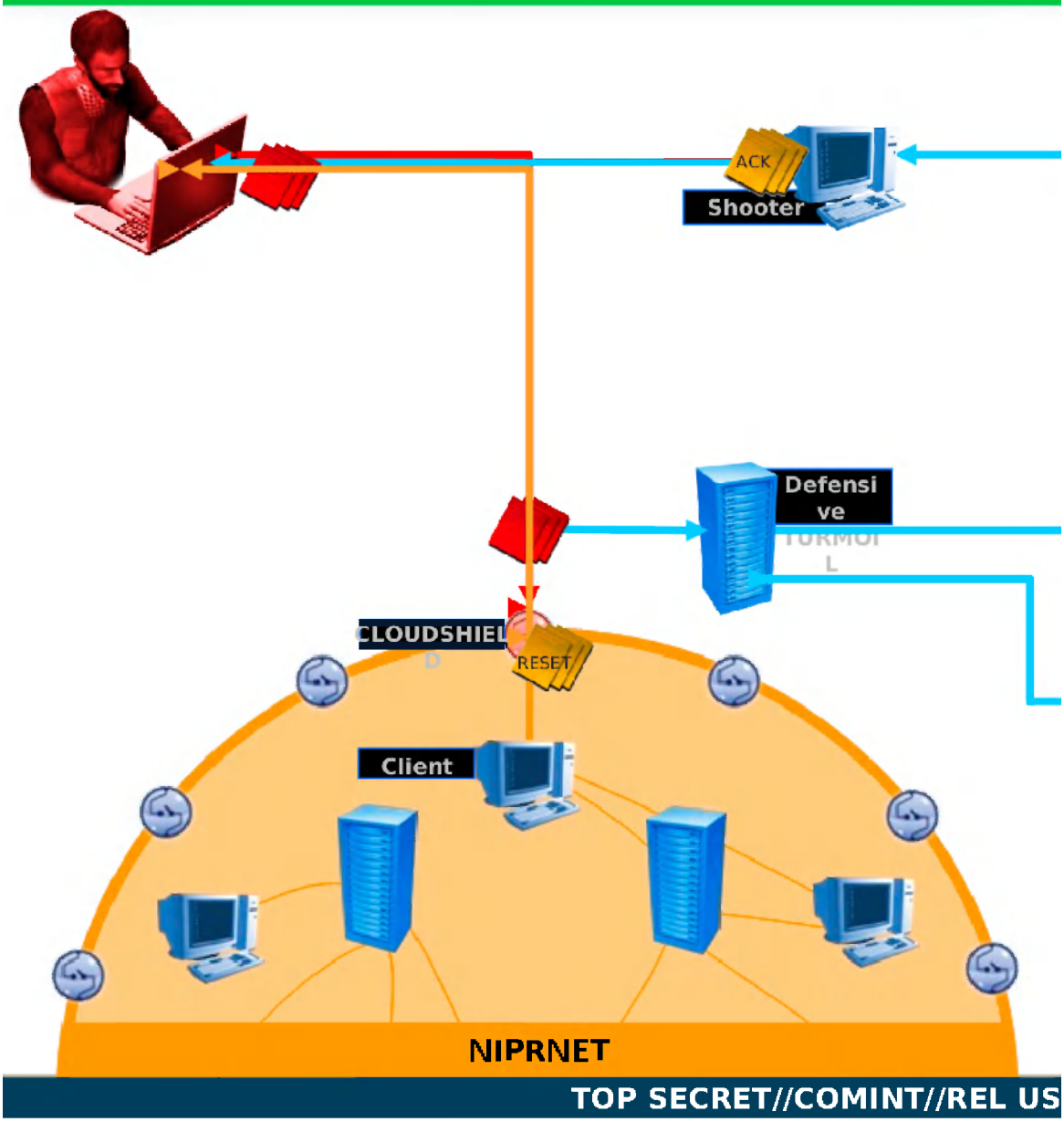
(U) There is More Than One Way to QUANTUM

TS//SI//REL

Name	Description	Inception Date	Status	Operational Success
	CNE			
QUANTUMINSERT	• Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation	2005	Operational	**Highly Successful** (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
QUANTUMBOT	• Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel	Aug 2007	Operational	**Highly Successful** (over 140,000 bots co-opted)
QUANTUMBISCUIT	• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.	Dec 2007	Operational	**Limited success at NSAW due to high latency on passive access** (GCHQ uses technique for 80% of CNE accesses)
QUANTUMDNS	• DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers.	Dec 2008	Operational	**Successful** (High priority CCI target exploited)
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	**Successful**
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	**N/A**
	CNA			
QUANTUMSKY	Denies access to a webpage through RST packet spoofing.	2004	Operational	**Successful**
QUANTUMCOPPER	File download/upload disruption and corruption.	Dec 2008	Live	**N/A**

TS//SI//REL

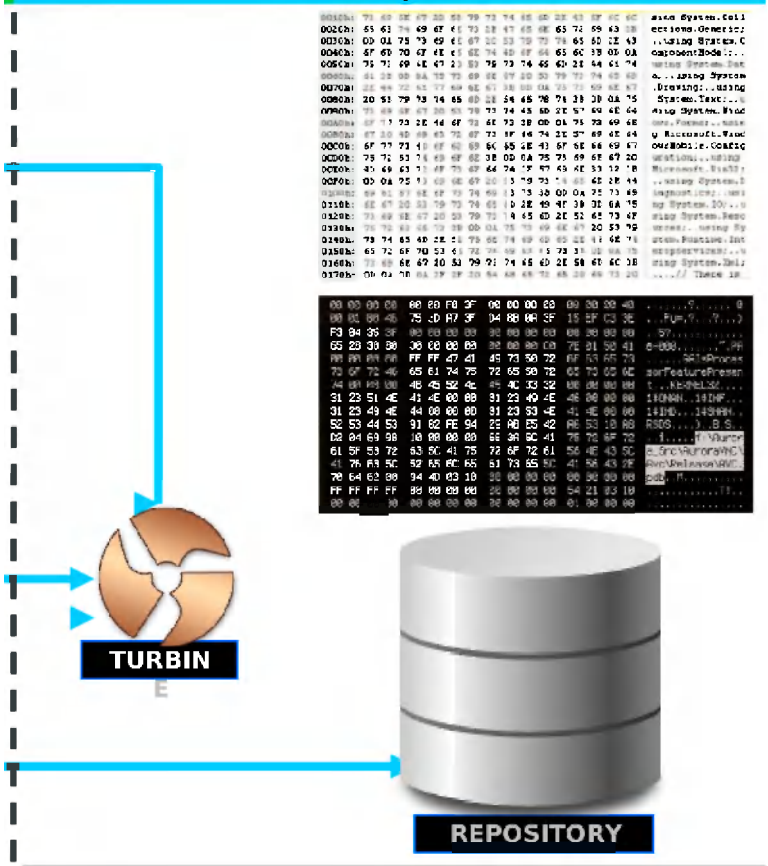
(U//FOUO) QUANTUMSMA



A, FVEY

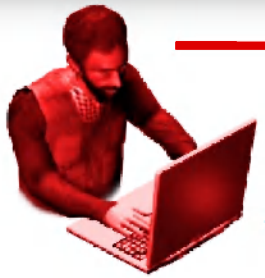
ACKDOWN

NSA Space



1. A client requests connection to malicious server. Request is detected by TURMOIL. CLOUDSHIELD terminates client-side connection.
2. The malicious server's response is blocked by CLOUDSHIELD.
3. TURMOIL tips TURBINE, which then tasks a shooter to send the acknowledgement to the malicious server.
4. Malicious server assumes connection and forwards

(U//FOUO) Future Capability: QUANTUMSANDMAN

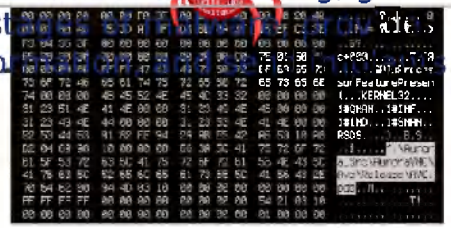


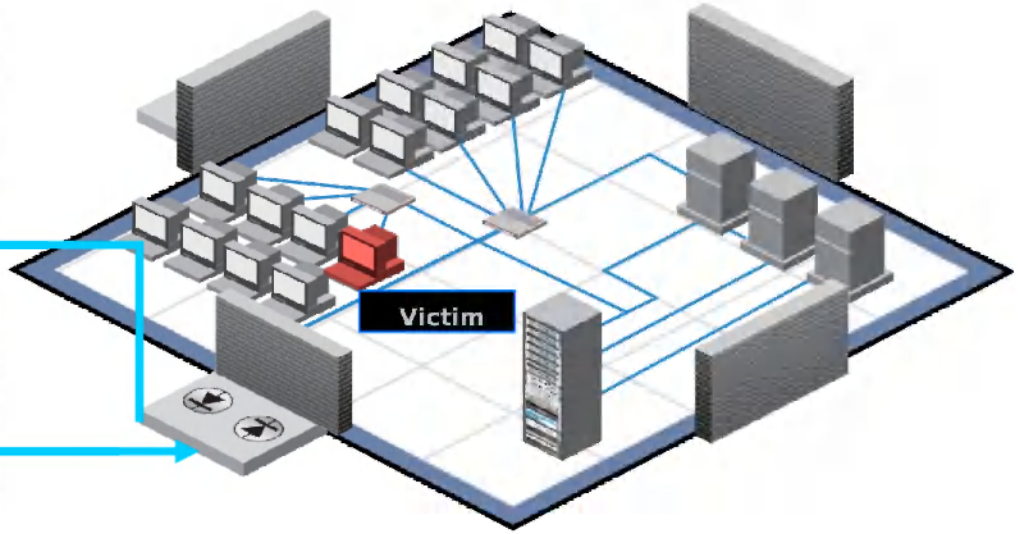
Internet

NSA Space

ure Malware Test Environm

- Take captured malware and execute in controlled environment.
- Allow communication through QUANTUM technique with outside world
- Will be able to see tasking, get later st
disinfo





(U) Future Work

- (U//FOUO) Develop lower latency guards
- (S//REL) Use TUTELAGE inline devices as our "shooter"
- (U//FOUO) Push decision logic to the edge

- (U//FOUO) Identify more mission opportunities
- (U//FOUO) Continue developing and deploying additional QUANTUM capabilities

(U) There is More Than One Way to QUANTUM

TS//SI//REL

Name	Description	Inception Date	Status	Operational Success
	CNE			
QUANTUMINSERT	• Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation	2005	Operational	**Highly Successful** (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
QUANTUMBOT	• Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel	Aug 2007	Operational	**Highly Successful** (over 140,000 bots co-opted)
QUANTUMBISCUIT	• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.	Dec 2007	Operational	**Limited success at NSAW due to high latency on passive access** (GCHQ uses technique for 80% of CNE accesses)
QUANTUMDNS	• DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers.	Dec 2008	Operational	**Successful** (High priority CCI target exploited)
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	**Successful**
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	**N/A**
	CNA			
QUANTUMSKY	Denies access to a webpage through RST packet spoofing.	2004	Operational	**Successful**
QUANTUMCOPPER	File download/upload disruption and corruption.	Dec 2008	Live	**N/A**

TS//SI//REL

(U) QUESTIONS?

For more information, please contact:

- TUTELAGE – [redacted], **VS** ([redacted])
- QUANTUM – [redacted], **S32X** ([redacted])
- TURBINE – [redacted], T1412 ([redacted])
- BOXINGRUMBLE – [redacted], **F22** ([redacted])