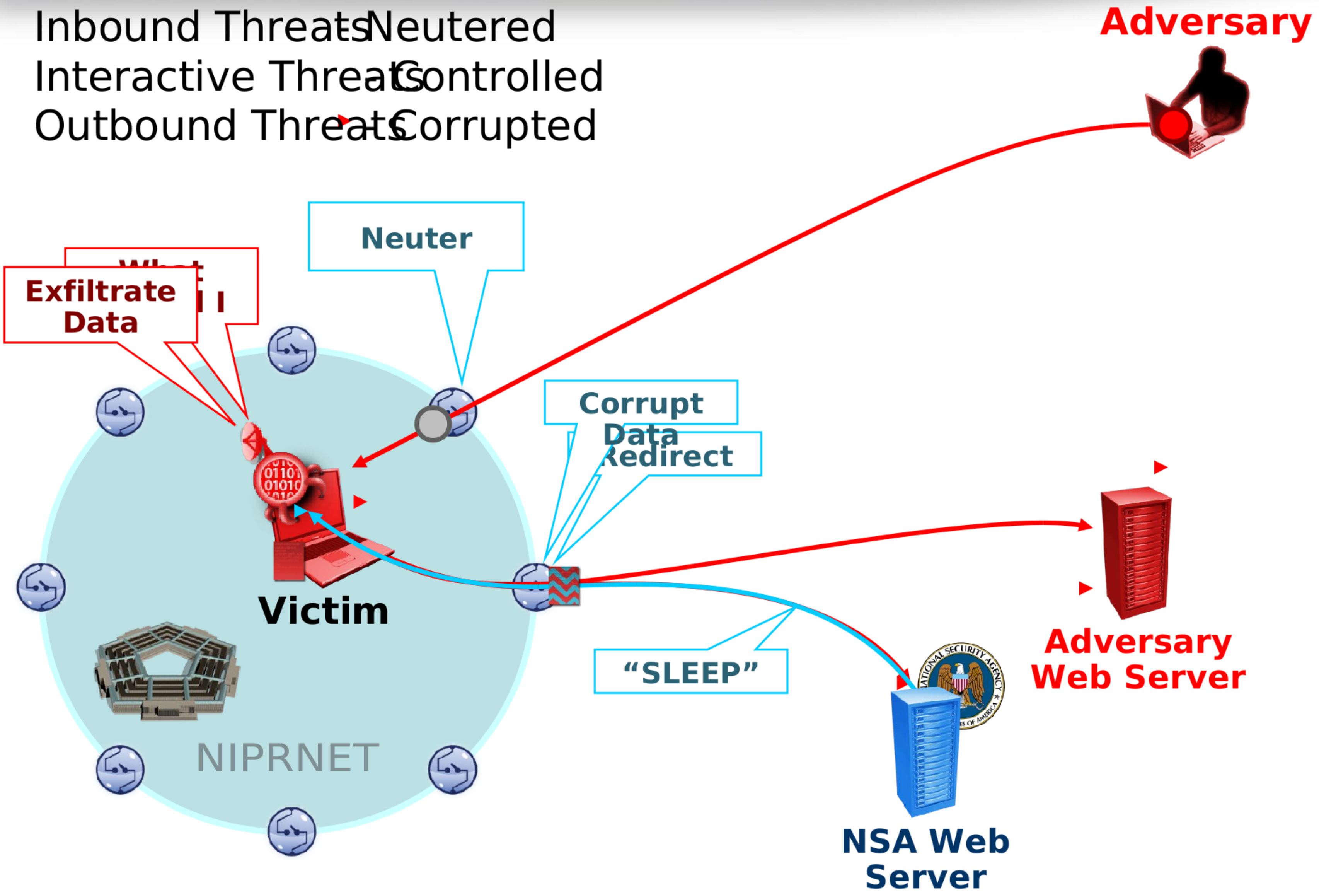
Case Studies of Integrated Cyber Operation Techniques

[redacted]

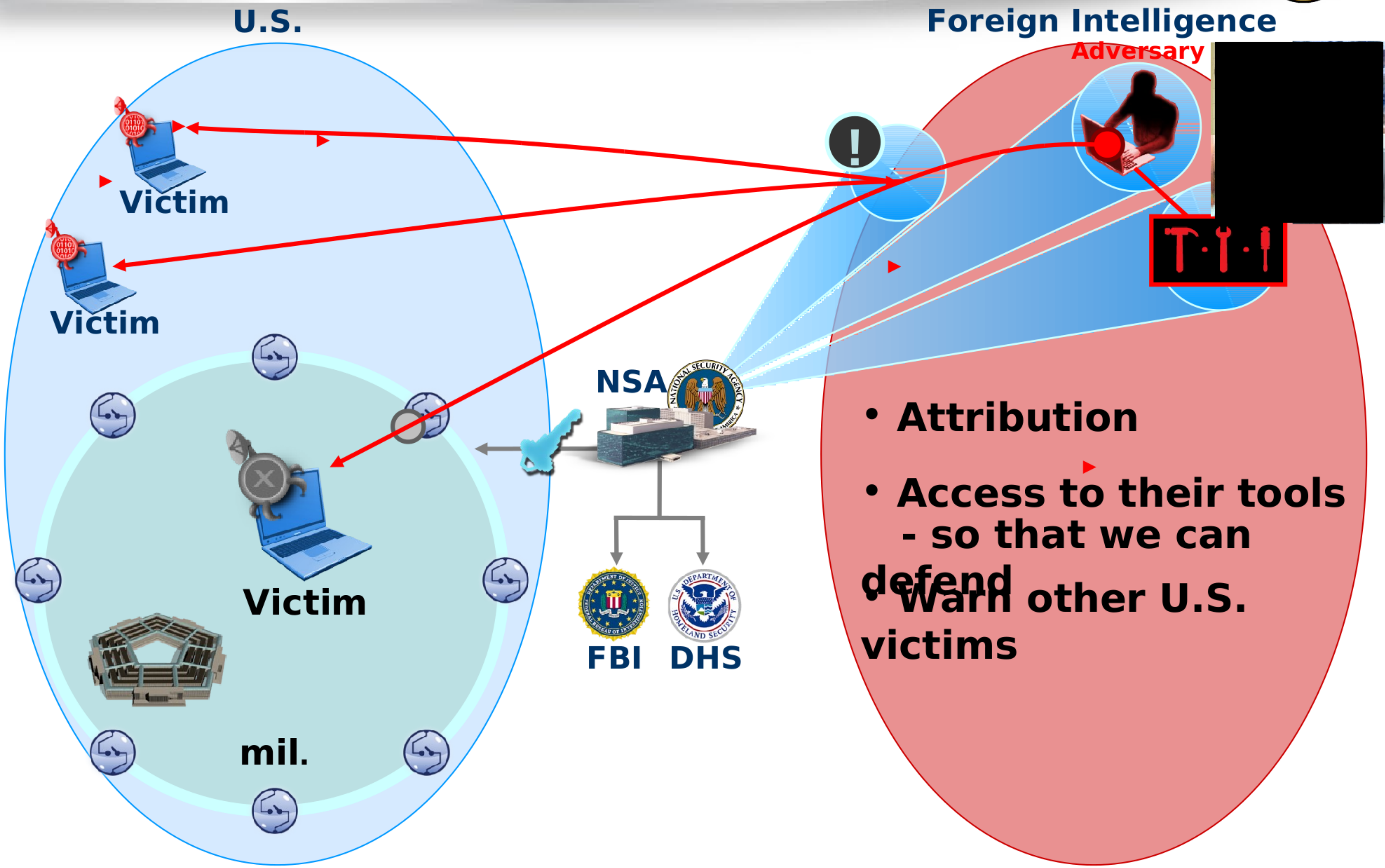
NSA/CSS Threat Operations Center
VS

(U//FOUO) TUTELAGE: Dynamic Defense

Inbound Threats - Neutered
Interactive Threats - Controlled
Outbound Threats - Corrupted



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



[redacted]

- Attribution
- Access to their tools
  - so that we can defend
- Warn other U.S. victims

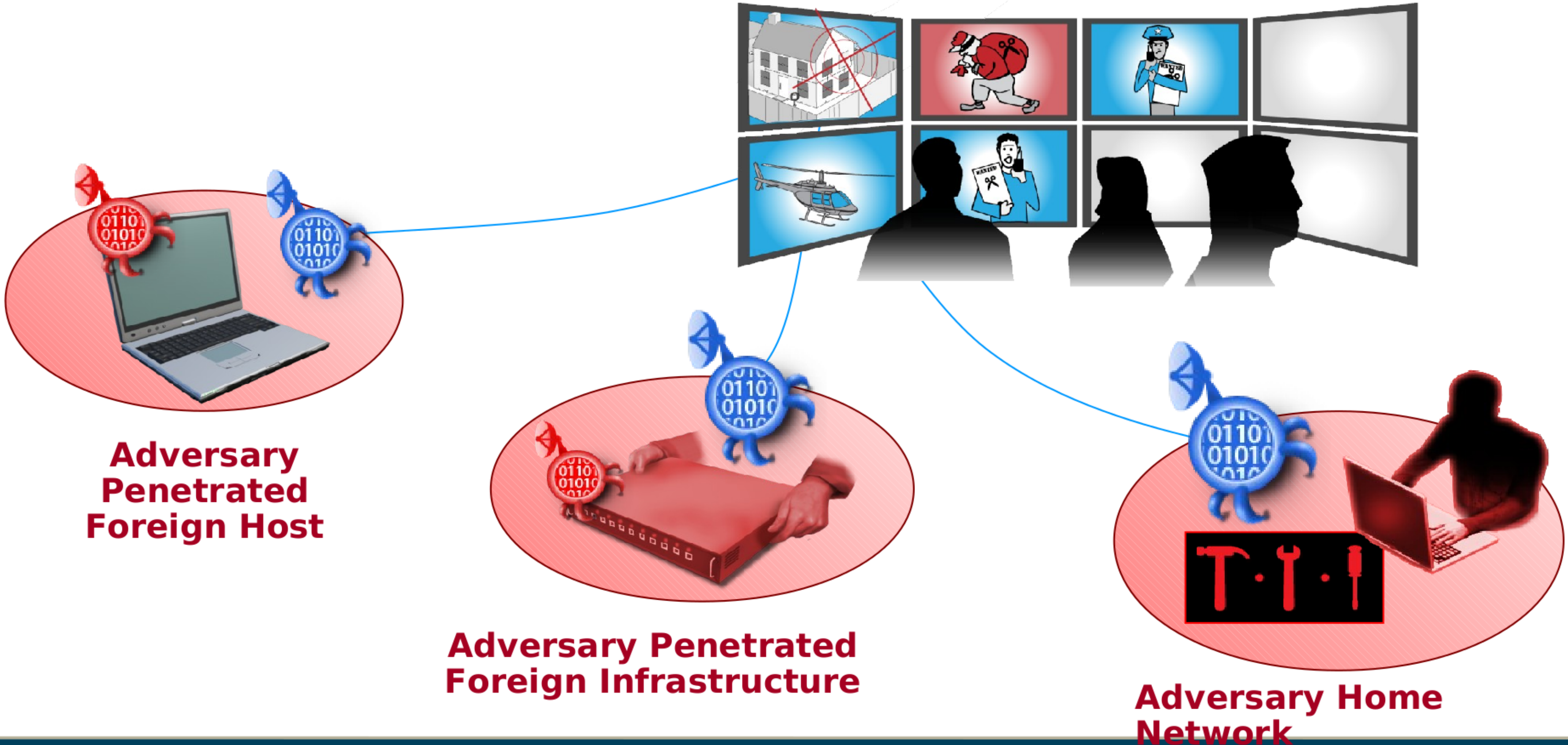
(U//FOUO) Counter-CNE: Support to CND

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

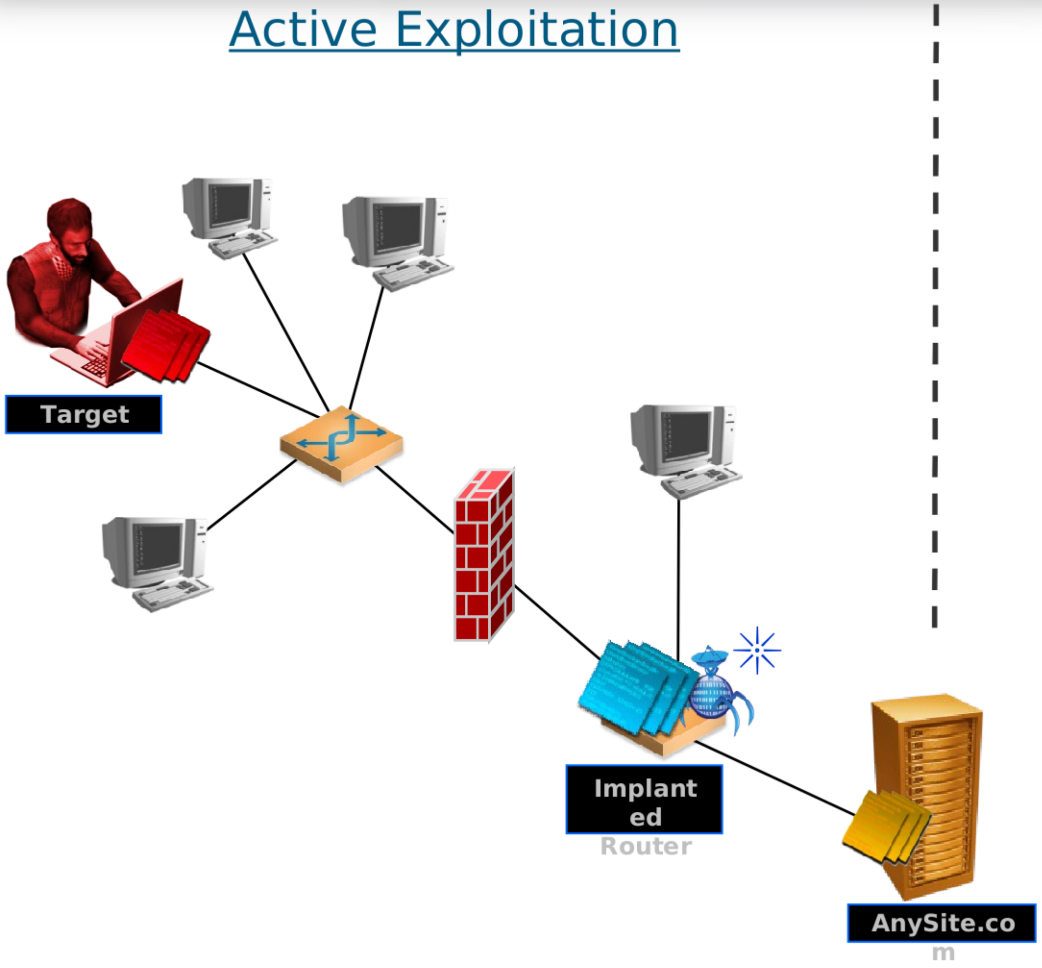

Adversary Penetrated Foreign Host

Adversary Penetrated Foreign Infrastructure

Adversary Home Network

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

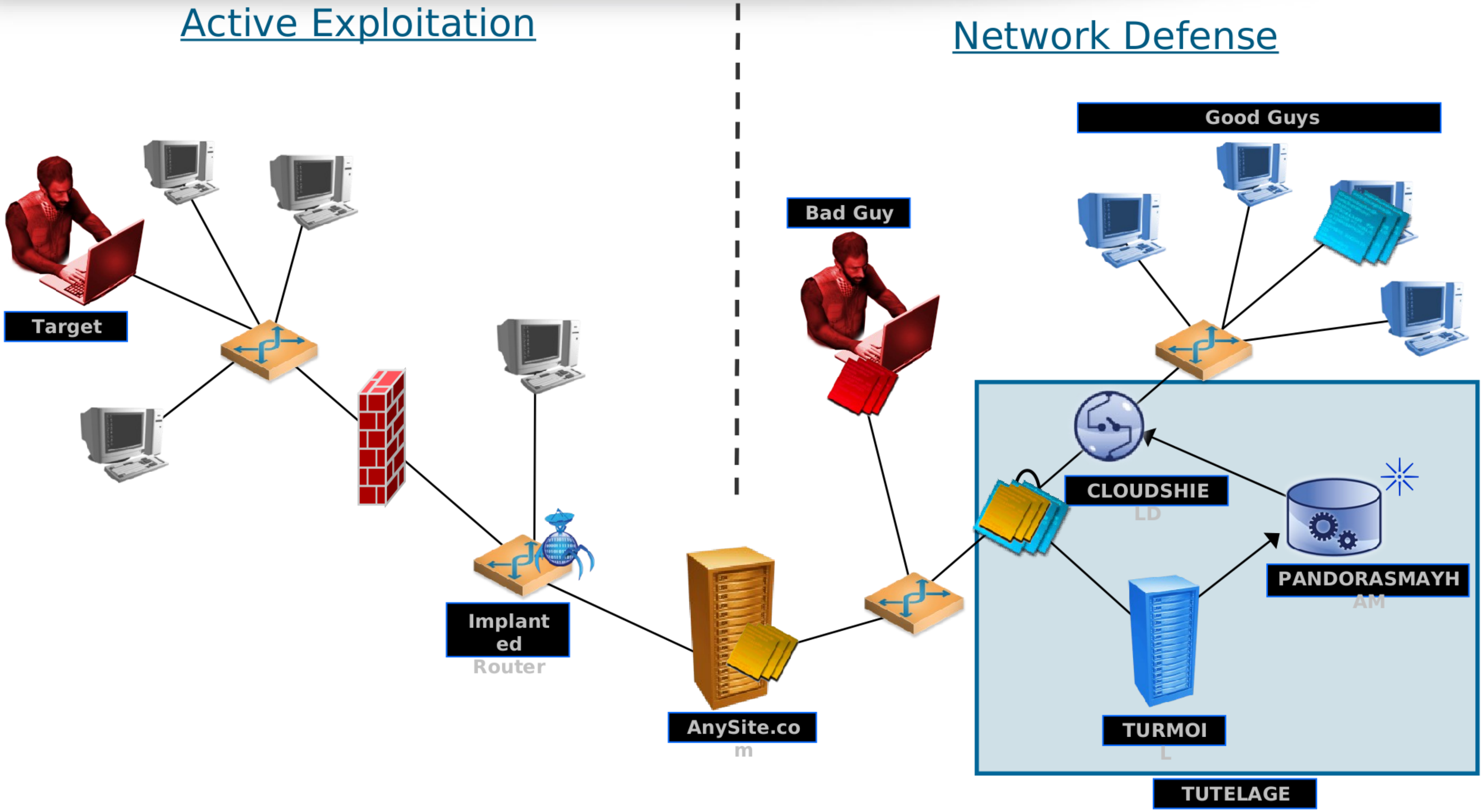
Active Exploitation



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

Active Exploitation

Network Defense



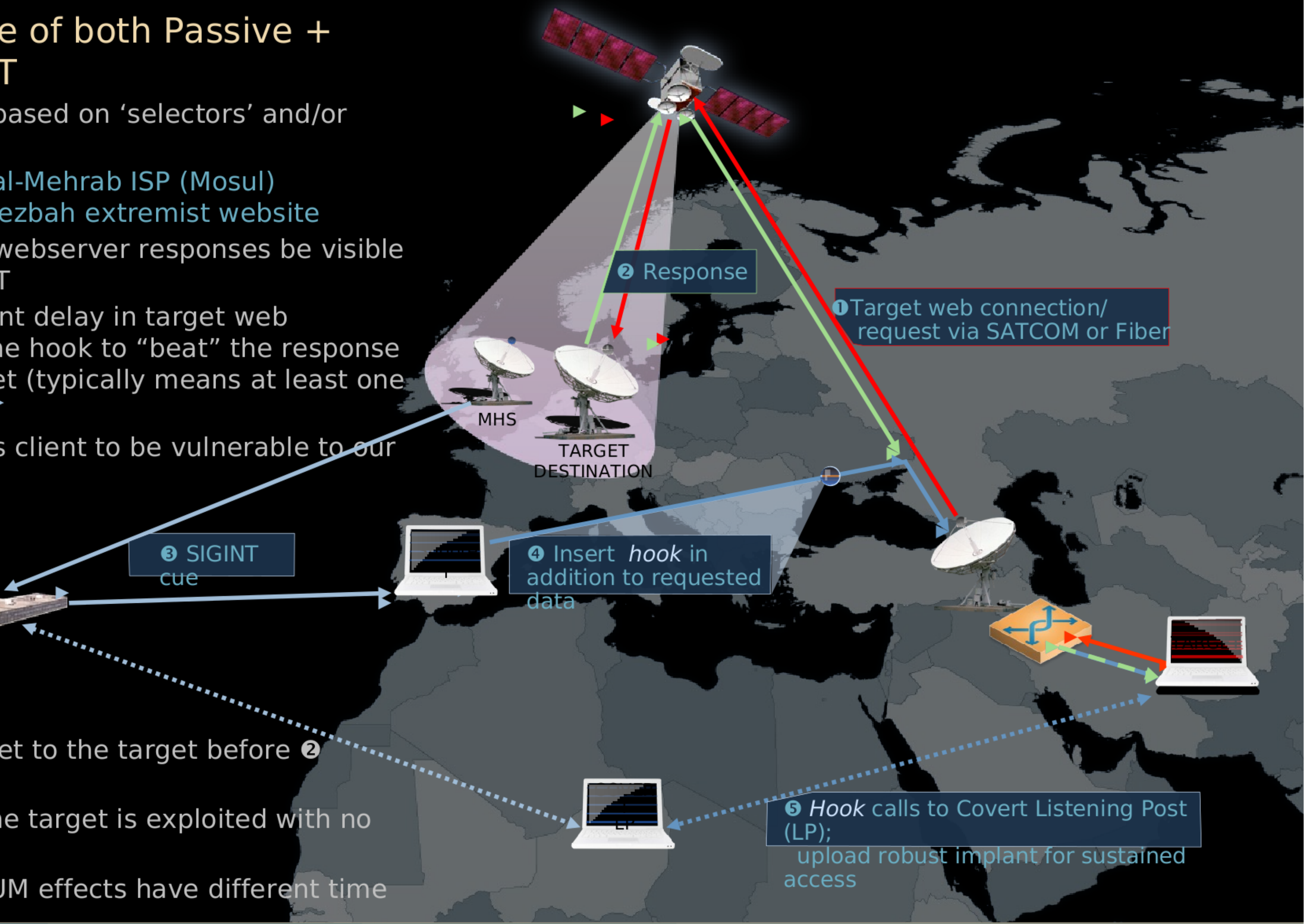
S//REL) TUTELAGE is a man-in-the-middle technique

(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



❶Target web connection/ request via SATCOM or Fiber

❷ Response

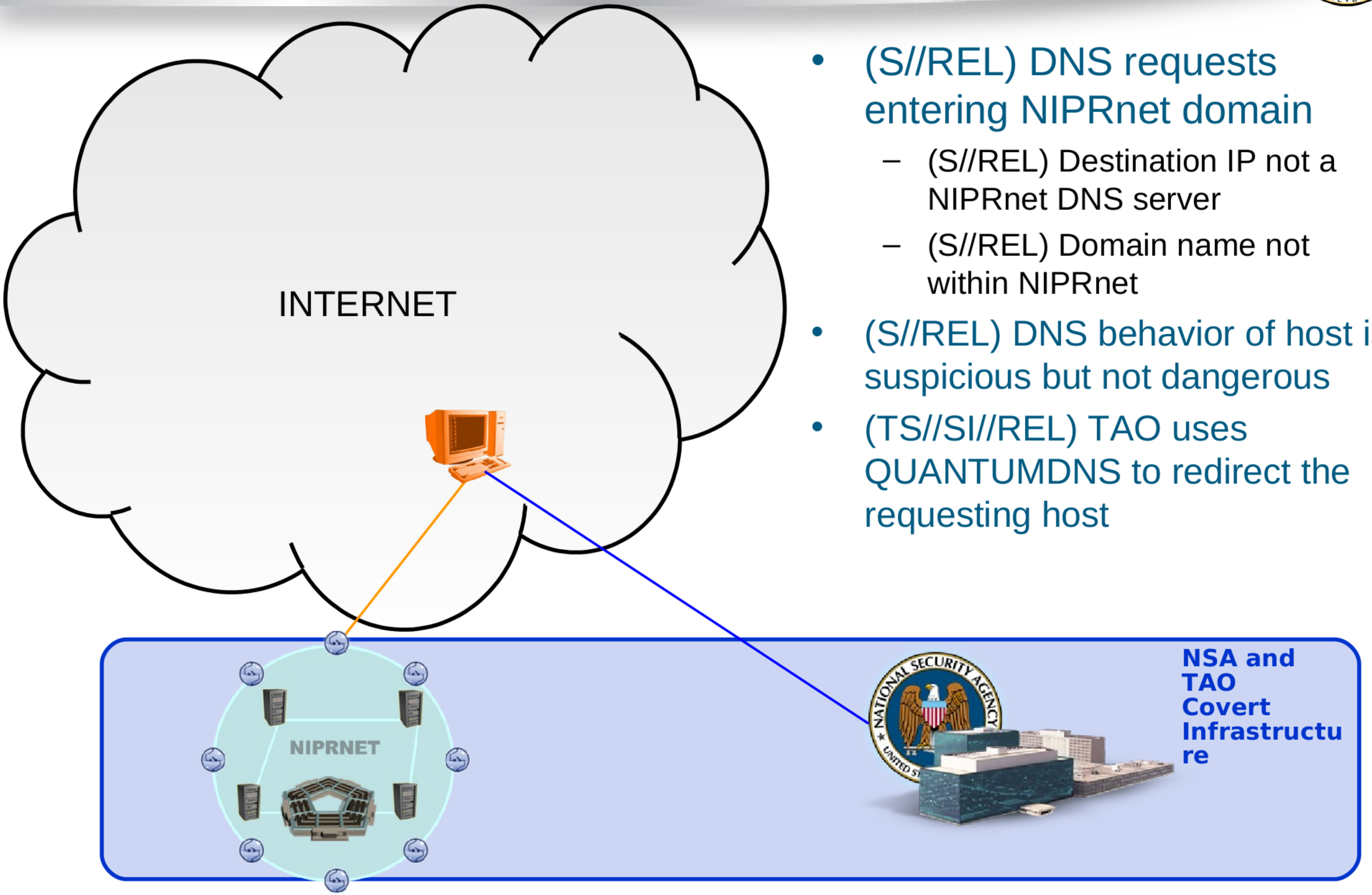
❸ SIGINT cue

❹ Insert *hook* in addition to requested data

❺ *Hook* calls to Covert Listening Post (LP); upload robust implant for sustained access

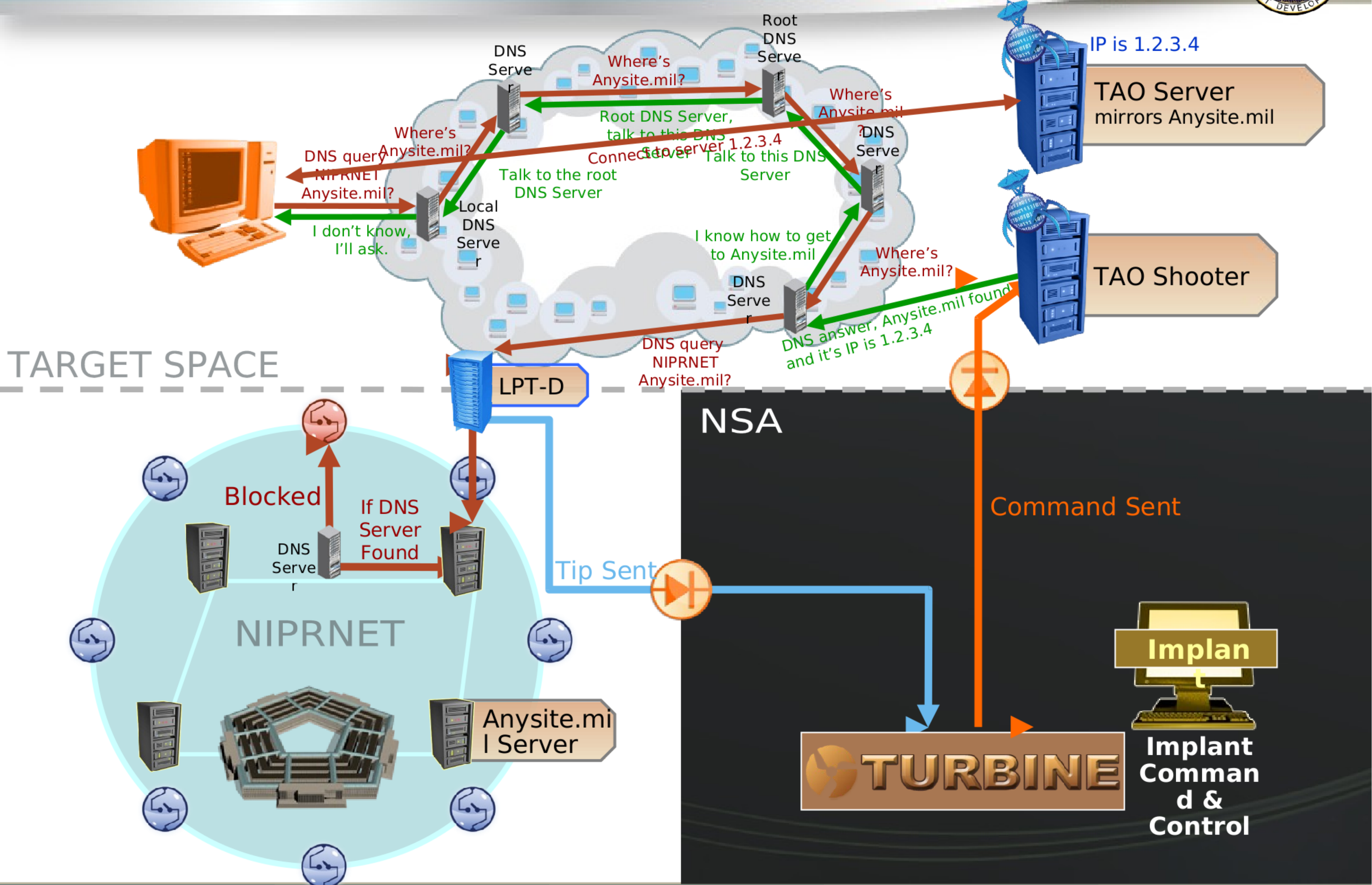
- Cycle ❸❹ must get to the target before ❷ occurs
- Once 'hooked,' the target is exploited with no time constraints
- Different QUANTUM effects have different time constraints.

(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



Root DNS Serve r

DNS Serve r

Where's Anysite.mil?

Root DNS Server, talk to this DNS Server

Connect to server 1.2.3.4

Where's Anysite.mil?

DNS Serve r

Talk to this DNS Server

Where's Anysite.mil?

Talk to the root DNS Server

DNS query NIPRNET Anysite.mil?

Local DNS Serve r

I don't know, I'll ask.

I know how to get to Anysite.mil

DNS Serve r

Where's Anysite.mil?

DNS answer, Anysite.mil found and it's IP is 1.2.3.4

DNS query NIPRNET Anysite.mil?

IP is 1.2.3.4

TAO Server mirrors Anysite.mil

TAO Shooter

TARGET SPACE

LPT-D

NSA

Blocked

If DNS Server Found

DNS Serve r

NIPRNET

Anysite.mi l Server

Tip Sent

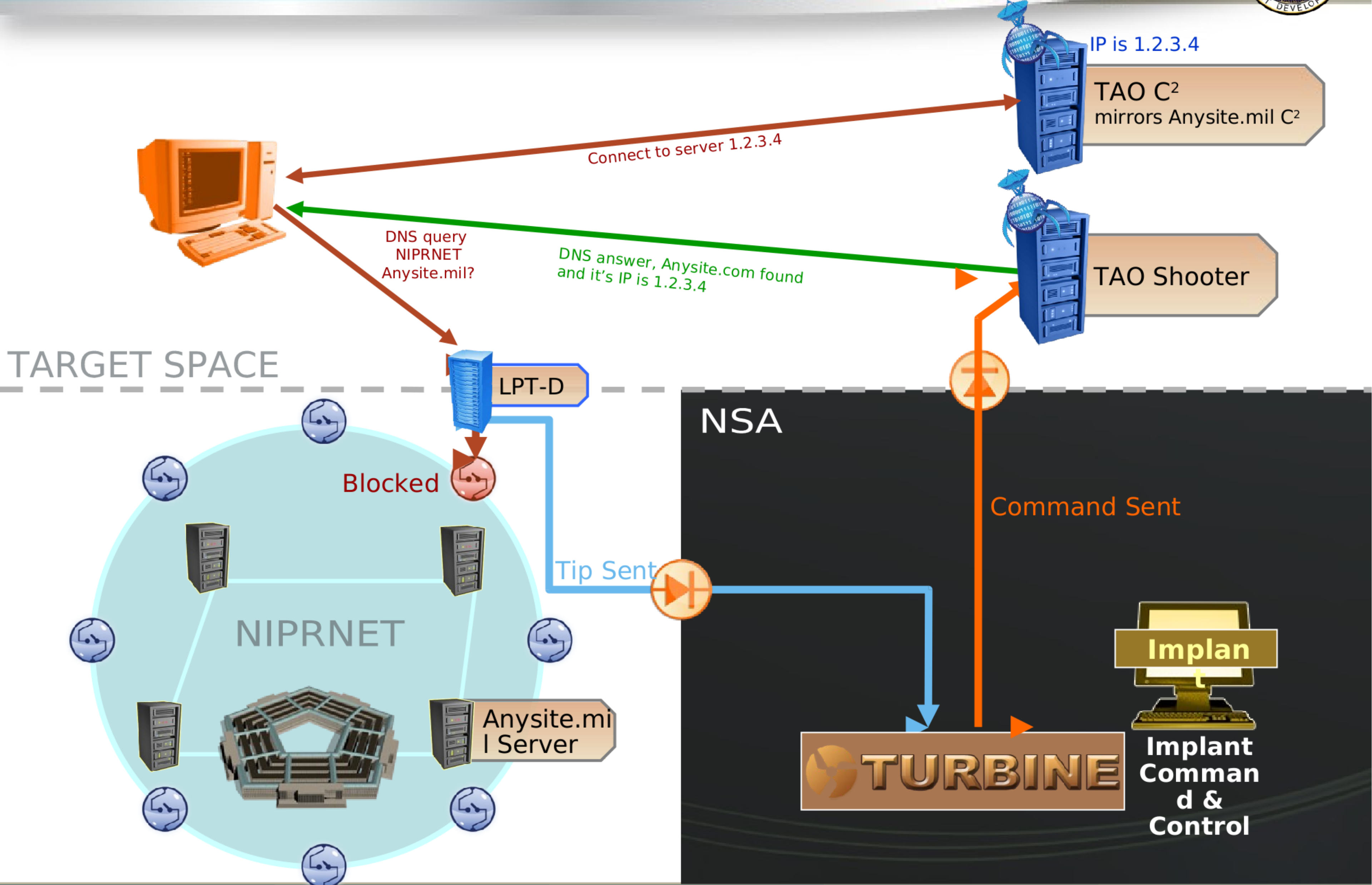
Command Sent

TURBINE

Implan t

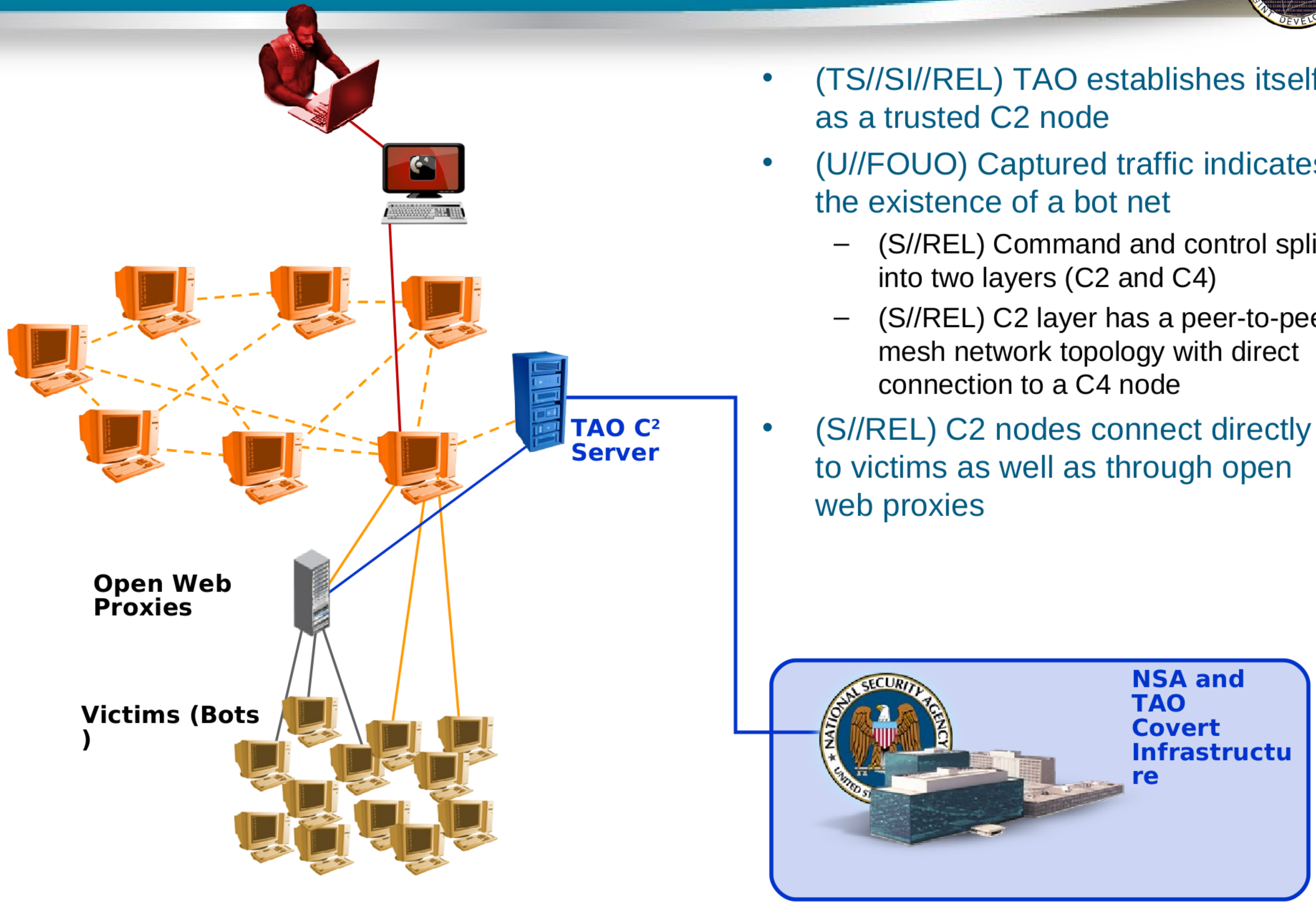
Implant Comman d & Control

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

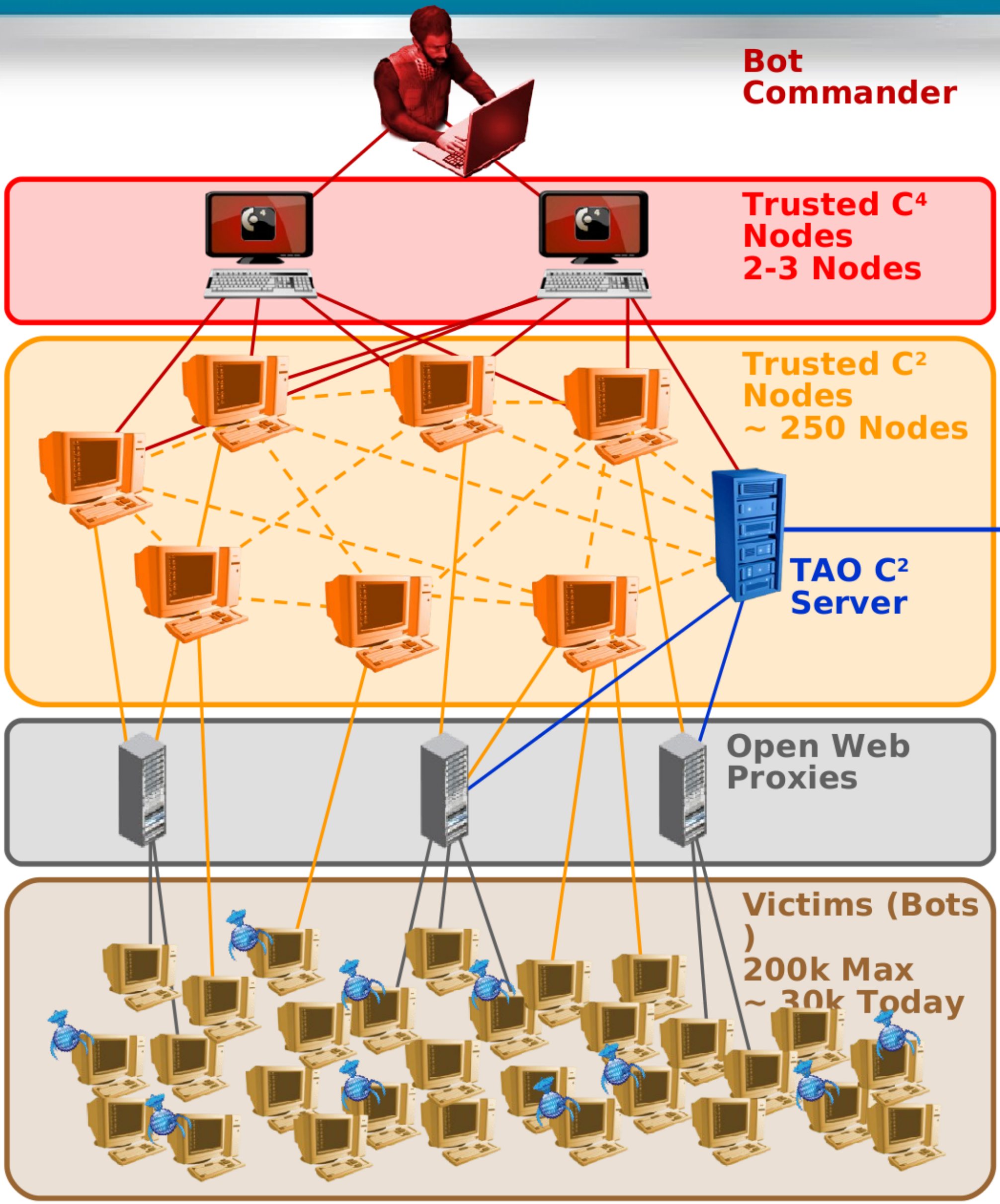


(U//FOUO) BOXINGRUMBLE Case Study

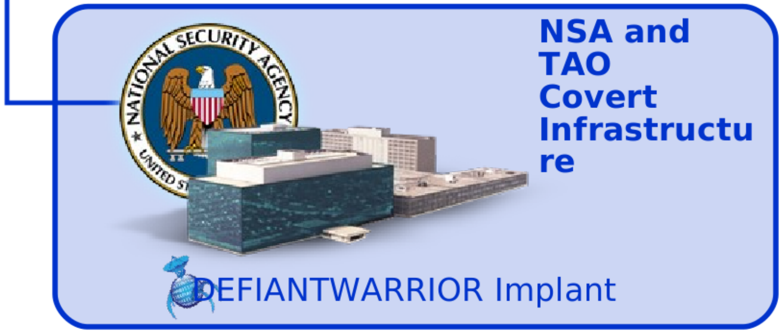
- (TS//SI//REL) TAO establishes itself as a trusted C2 node
- (U//FOUO) Captured traffic indicates the existence of a bot net
  - (S//REL) Command and control split into two layers (C2 and C4)
  - (S//REL) C2 layer has a peer-to-peer mesh network topology with direct connection to a C4 node
- (S//REL)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



(U//FOUO) BOXINGRUMBLE Case Study


Bot Commander
Trusted C⁴ Nodes 2-3 Nodes
Trusted C² Nodes ~ 250 Nodes
TAO C² Server
Open Web Proxies
Victims (Bots) 200k Max ~ 30k Today

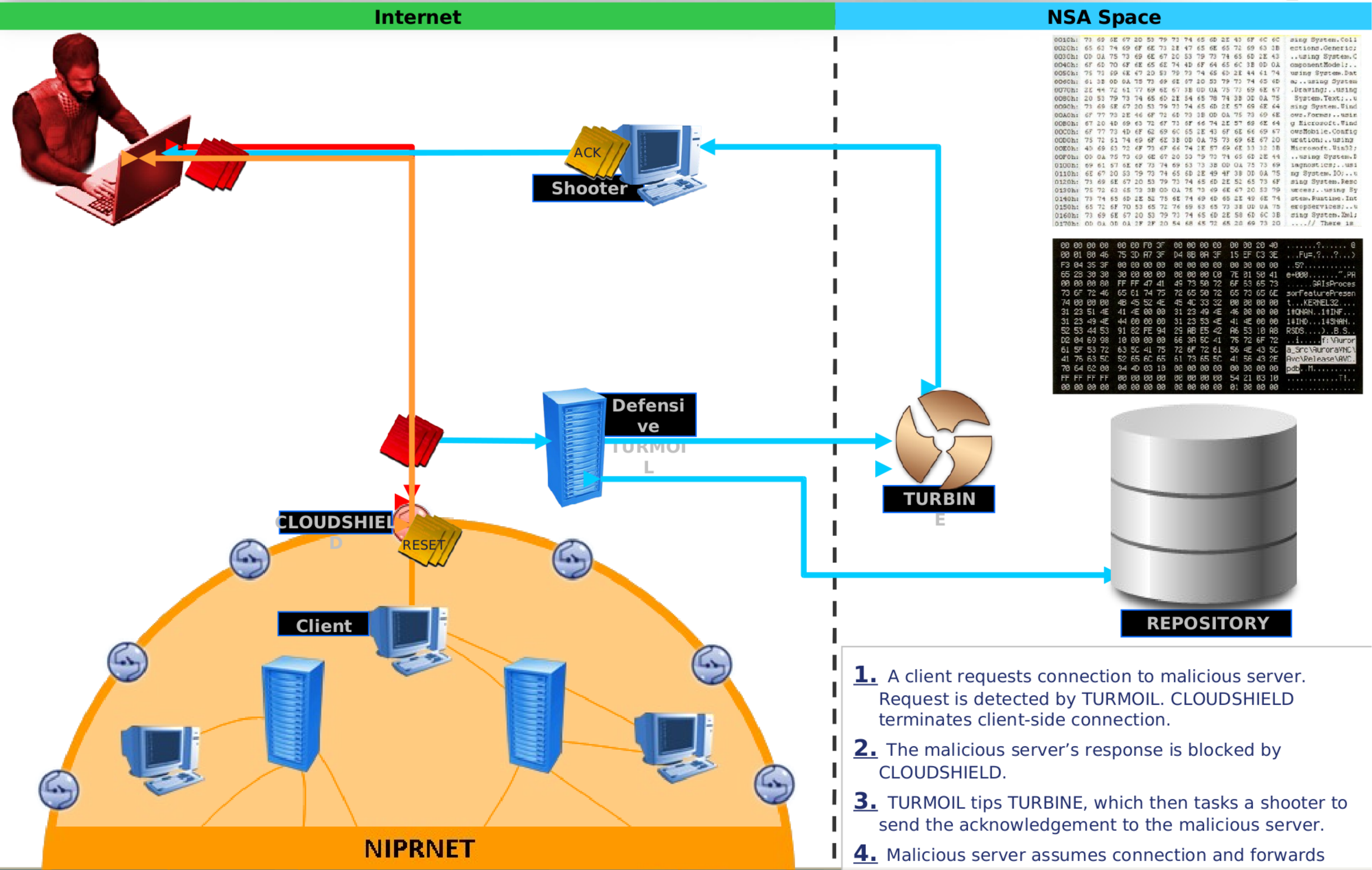
- (TS//SI//REL)TAO C2 server can see all bot tasking
- (TS//SI//REL) TAO C2 server can push tasking
- (S//REL) BOXINGRUMBLE bots
  - (S//REL) ~ 45% Vietnamese dissidents
  - (S//REL) ~45% Chinese dissidents
  - (S//REL) ~10% Other
- (TS//SI//REL) Adding BOXINGRUMBLE bots to DEFIANTWARRIOR



(U) There is More Than One Way to QUANTUM

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**

(U//FOUO) QUANTUMSMACKDOWN



```
0010h: 73 69 6E 67 20 53 79 73 74 65 6D 2E 43 6F 6C 6C  sing System.Coll
0020h: 65 63 74 69 6F 6E 73 2E 47 65 6E 65 72 69 63 3B  ections.Generic;
0030h: 0D 0A 75 73 69 6E 67 20 53 79 73 74 65 6D 2E 43  ..using System.C
0040h: 6F 6D 70 6F 6E 65 6E 74 4D 6F 64 65 6C 3B 0D 0A  omponentModel;..
0050h: 75 73 69 6E 67 20 53 79 73 74 65 6D 2E 44 61 74  using System.Dat
0060h: 61 3B 0D 0A 75 73 69 6E 67 20 53 79 73 74 65 6D  a;..using System
0070h: 2E 44 72 61 77 69 6E 67 3B 0D 0A 75 73 69 6E 67  .Drawing;..using
0080h: 20 53 79 73 74 65 6D 2E 54 65 78 74 3B 0D 0A 75   System.Text;..u
0090h: 73 69 6E 67 20 53 79 73 74 65 6D 2E 57 69 6E 64  sing System.Wind
00A0h: 6F 77 73 2E 46 6F 72 6D 73 3B 0D 0A 75 73 69 6E  ows.Forms;..usin
00B0h: 67 20 4D 69 63 72 6F 73 6F 66 74 2E 57 69 6E 64  g Microsoft.Wind
00C0h: 6F 77 73 4D 6F 62 69 6C 65 2E 43 6F 6E 66 69 67  owsMobile.Config
00D0h: 75 72 61 74 69 6F 6E 3B 0D 0A 75 73 69 6E 67 20  uration;..using 
00E0h: 4D 69 63 72 6F 73 6F 66 74 2E 57 69 6E 33 32 3B  Microsoft.Win32;
00F0h: 0D 0A 75 73 69 6E 67 20 53 79 73 74 65 6D 2E 44  ..using System.D
0100h: 69 61 67 6E 6F 73 74 69 63 73 3B 0D 0A 75 73 69  iagnostics;..usi
0110h: 6E 67 20 53 79 73 74 65 6D 2E 49 4F 3B 0D 0A 75  ng System.IO;..u
0120h: 73 69 6E 67 20 53 79 73 74 65 6D 2E 52 65 73 6F  sing System.Reso
0130h: 75 72 63 65 73 3B 0D 0A 75 73 69 6E 67 20 53 79  urces;..using Sy
0140h: 73 74 65 6D 2E 52 75 6E 74 69 6D 65 2E 49 6E 74  stem.Runtime.Int
0150h: 65 72 6F 70 53 65 72 76 69 63 65 73 3B 0D 0A 75  eropServices;..u
0160h: 73 69 6E 67 20 53 79 73 74 65 6D 2E 58 6D 6C 3B  sing System.Xml;
0170h: 0D 0A 0D 0A 2F 2F 20 54 68 65 72 65 20 69 73 20  ....// There is 
```

```
00 00 00 00  00 00 F0 3F  00 00 00 00  00 00 20 40  .......?...... @
00 01 80 46  75 3D A7 3F  D4 8B 0A 3F  15 EF C3 3E  ...Fu=.?...?...>
F3 04 35 3F  00 00 00 00  00 00 00 00  00 00 00 00  ..5?............
65 2B 30 30  30 00 00 00  00 00 00 C0  7E 01 50 41  e+000.......~.PA
00 00 00 80  FF FF 47 41  49 73 50 72  6F 63 65 73  ......GAIsProces
73 6F 72 46  65 61 74 75  72 65 50 72  65 73 65 6E  sorFeaturePresen
74 00 00 00  4B 45 52 4E  45 4C 33 32  00 00 00 00  t...KERNEL32....
31 23 51 4E  41 4E 00 00  31 23 49 4E  46 00 00 00  1#QNAN..1#INF...
31 23 49 4E  44 00 00 00  31 23 53 4E  41 4E 00 00  1#IND...1#SNAN..
52 53 44 53  91 82 FE 94  29 AB E5 42  A6 53 10 A8  RSDS....)..B.S..
D2 04 69 98  10 00 00 00  66 3A 5C 41  75 72 6F 72  ..i.....f:\Auror
61 5F 53 72  63 5C 41 75  72 6F 72 61  56 4E 43 5C  a_Src\AuroraVNC\
41 76 63 5C  52 65 6C 65  61 73 65 5C  41 56 43 2E  Avc\Release\AVC.
70 64 62 00  94 4D 03 10  00 00 00 00  00 00 00 00  pdb..M..........
FF FF FF FF  00 00 00 00  00 00 00 00  54 21 03 10  ............T!..
00 00 00 00  00 00 00 00  00 00 00 00  01 00 00 00  ................
```

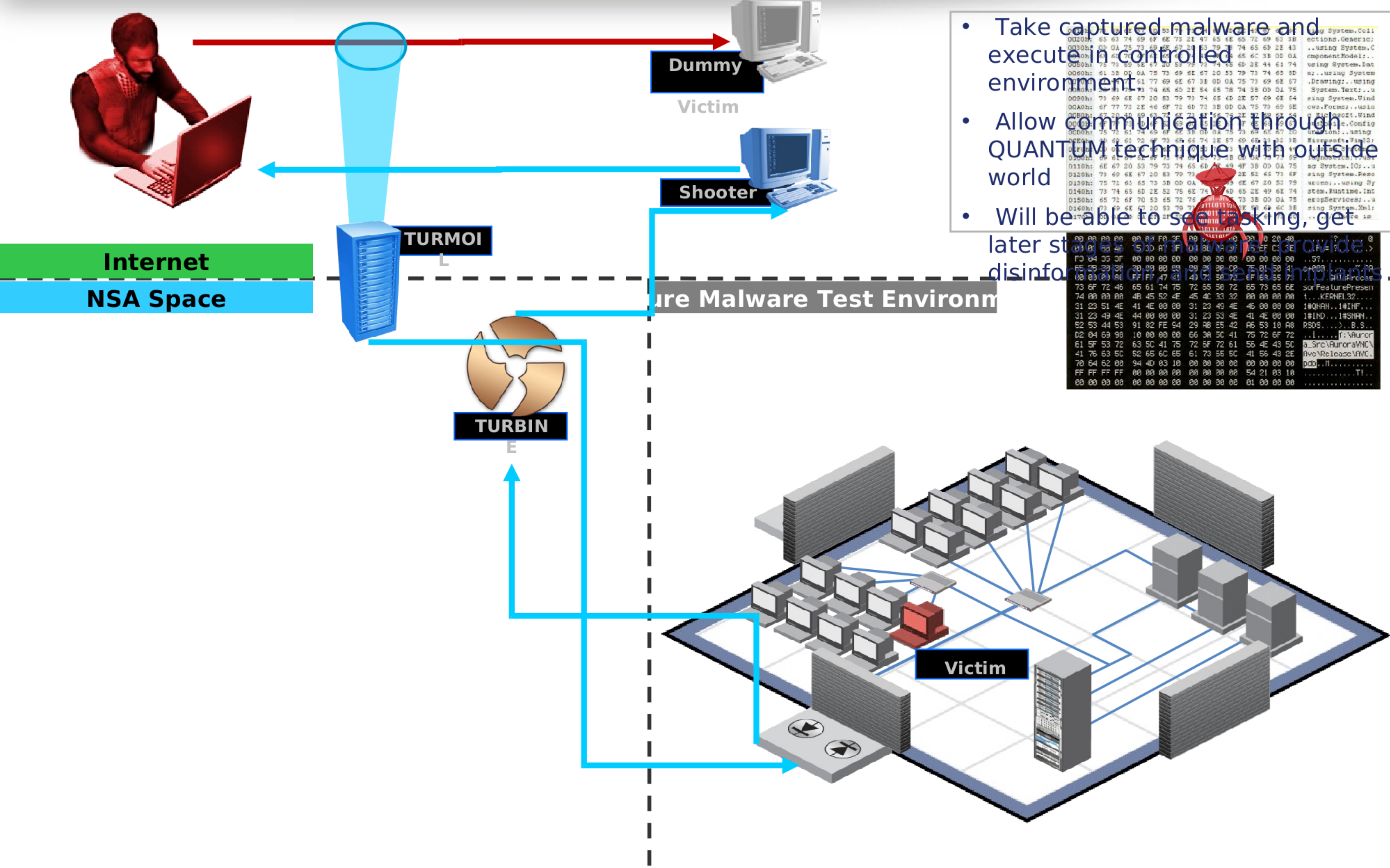
1. A client requests connection to malicious server. Request is detected by TURMOIL. CLOUDSHIELD terminates client-side connection.

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



- Take captured malware and execute in controlled environment.
- Allow communication through QUANTUM technique with outside world
- Will be able to see tasking, get later stages of malware, provide disinformation, and send implants.

(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])

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu