



# Case Studies of Integrated Cyber Operation Techniques



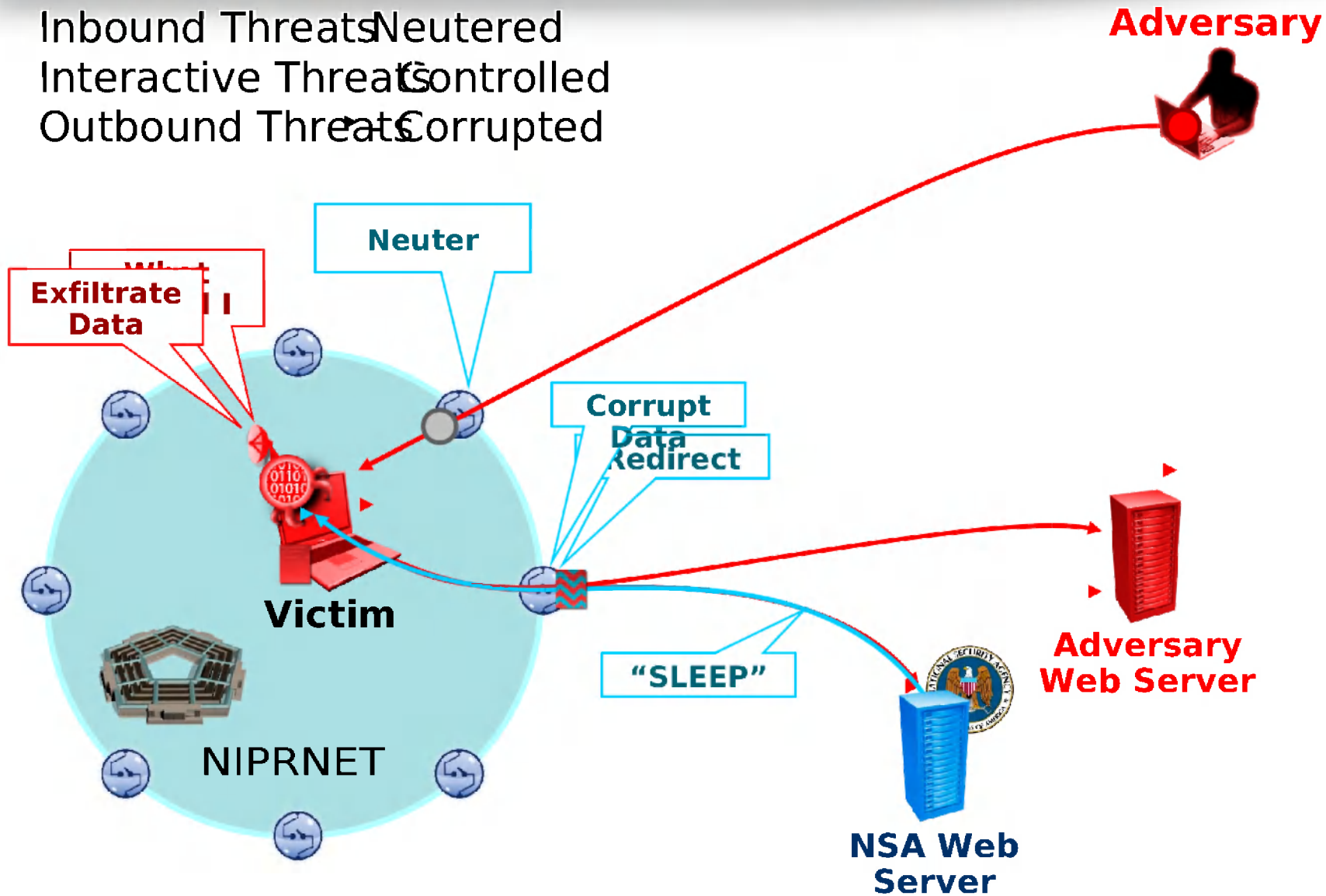
NSA/CSS Threat Operations Center  
VS

# (U//FOUO) TUTELEGE. Dynamic Defense

TOP SECRET//COMINT//REL USA, FVEY

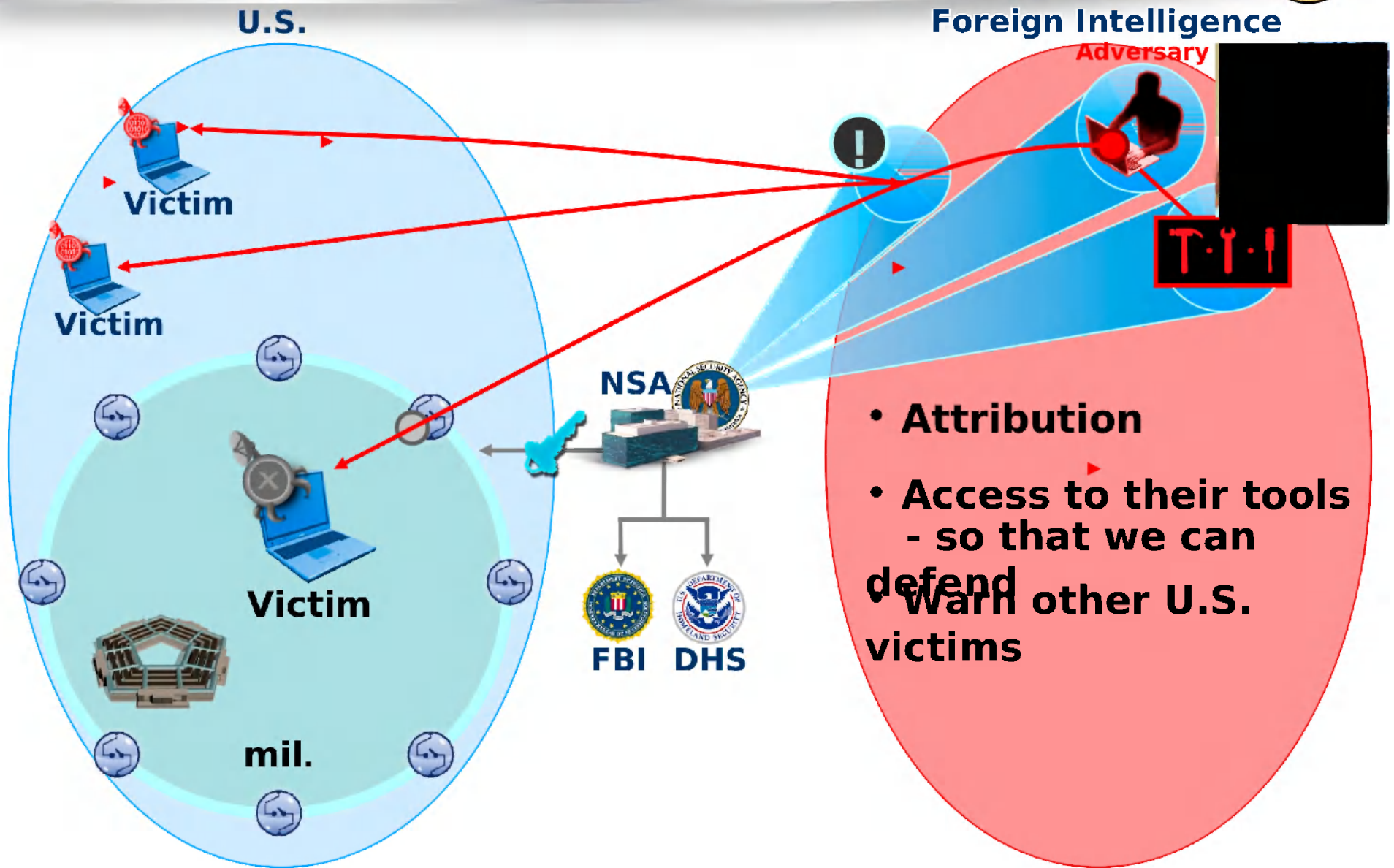


Inbound Threats Neutered  
Interactive Threats Controlled  
Outbound Threats Corrupted



TOP SECRET//COMINT//REL USA, FVEY

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





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

TOP SECRET//COMINT//REL USA, FVEY

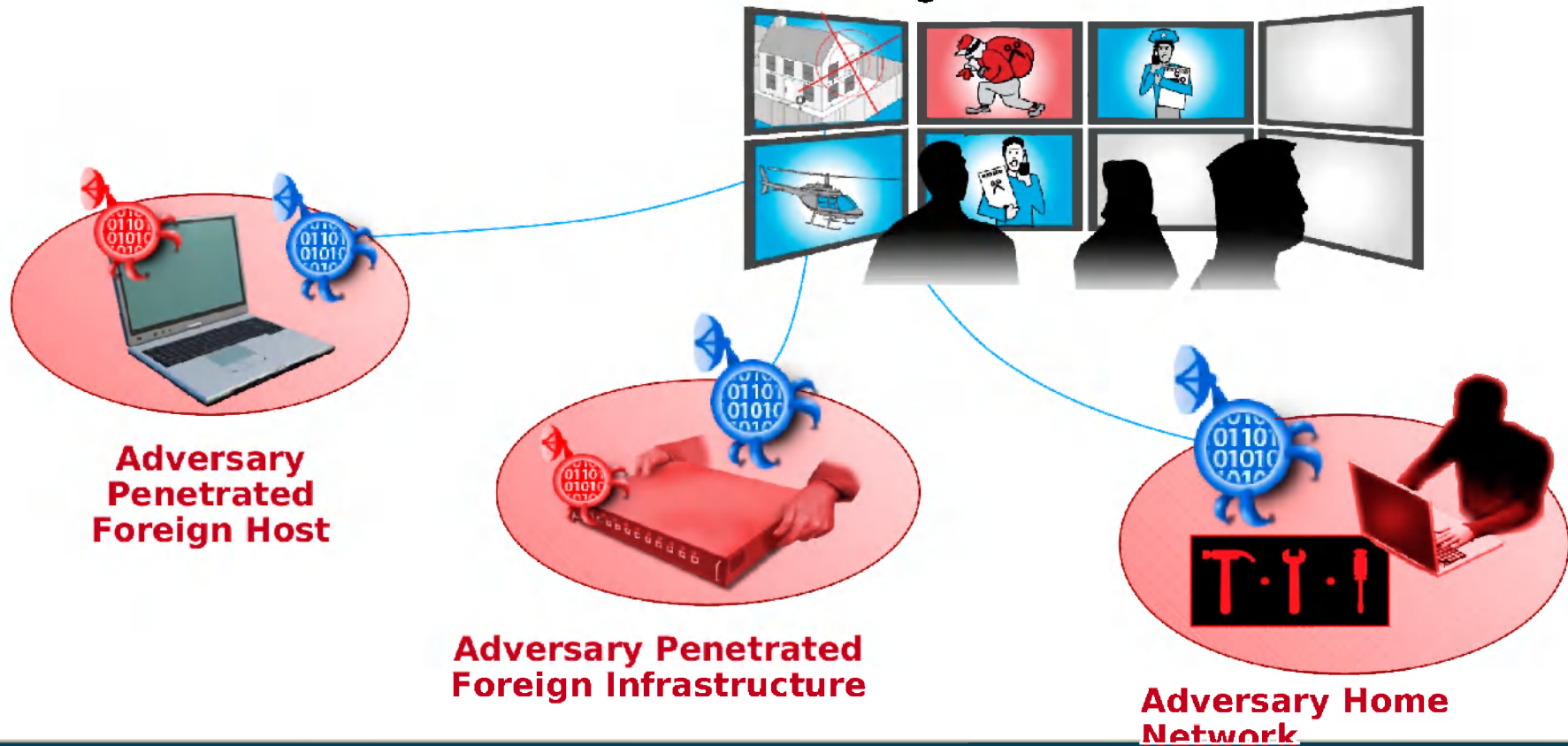


S//REL) Use CNE to penetrate the operations of foreign cyber actors

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

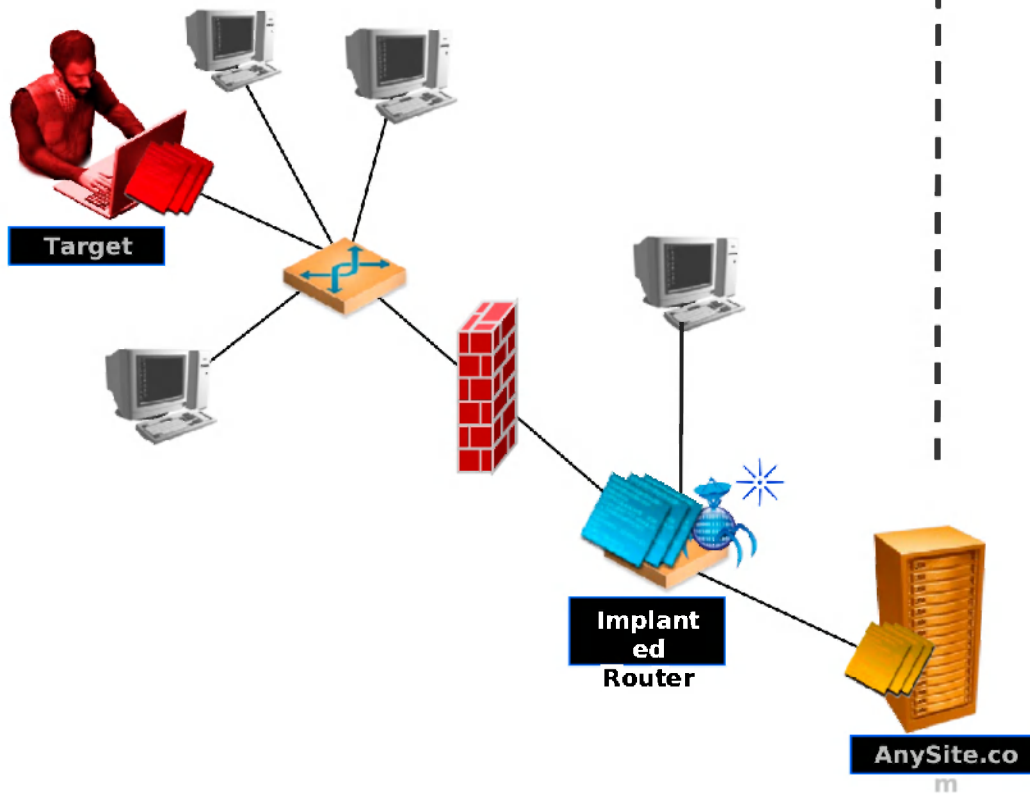


TOP SECRET//COMINT//REL USA, FVEY

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



## Active Exploitation

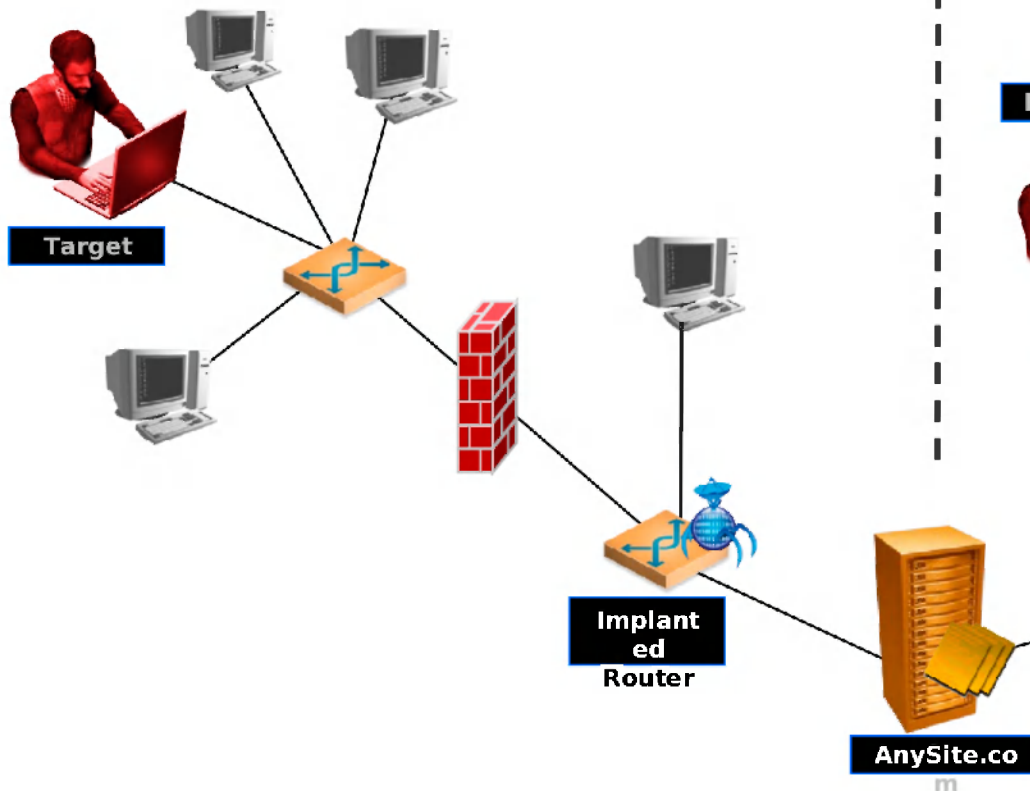


# (U) Man-in-the-Middle has Multiple Uses

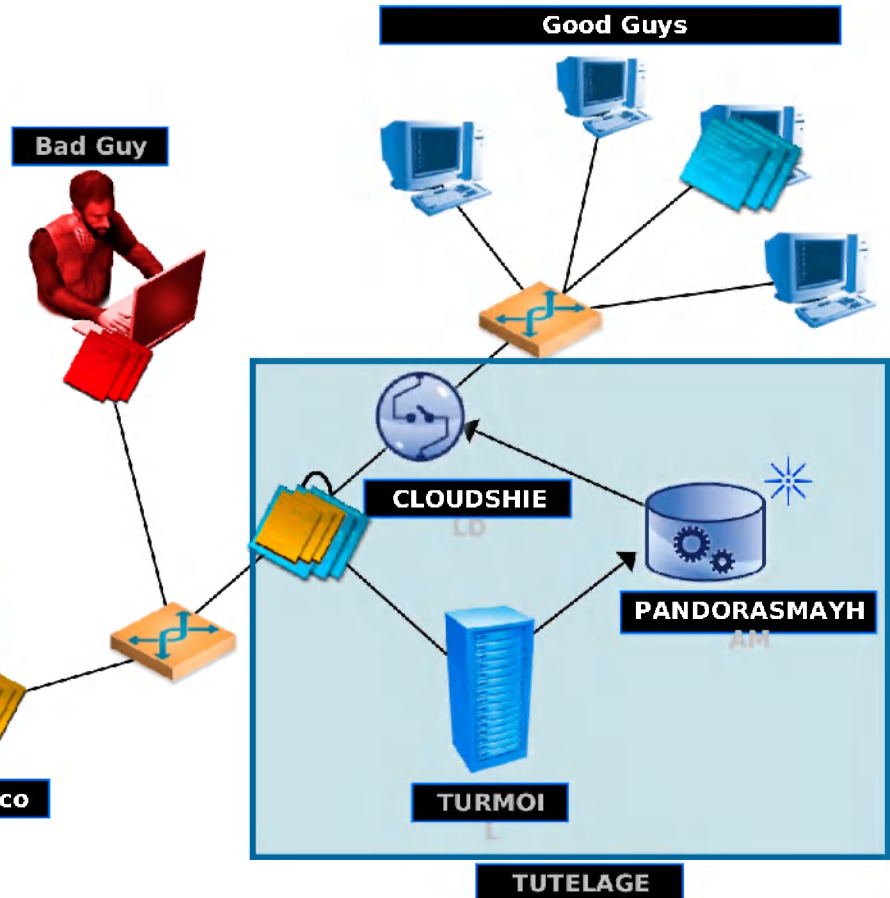
TOP SECRET//COMINT//REL//SI, FROTH



## 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) QUANTUM THEORY: Man-on-the-Side Active Exploitation

TOP SECRET//COMINT//REL USA, FVEY



## 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

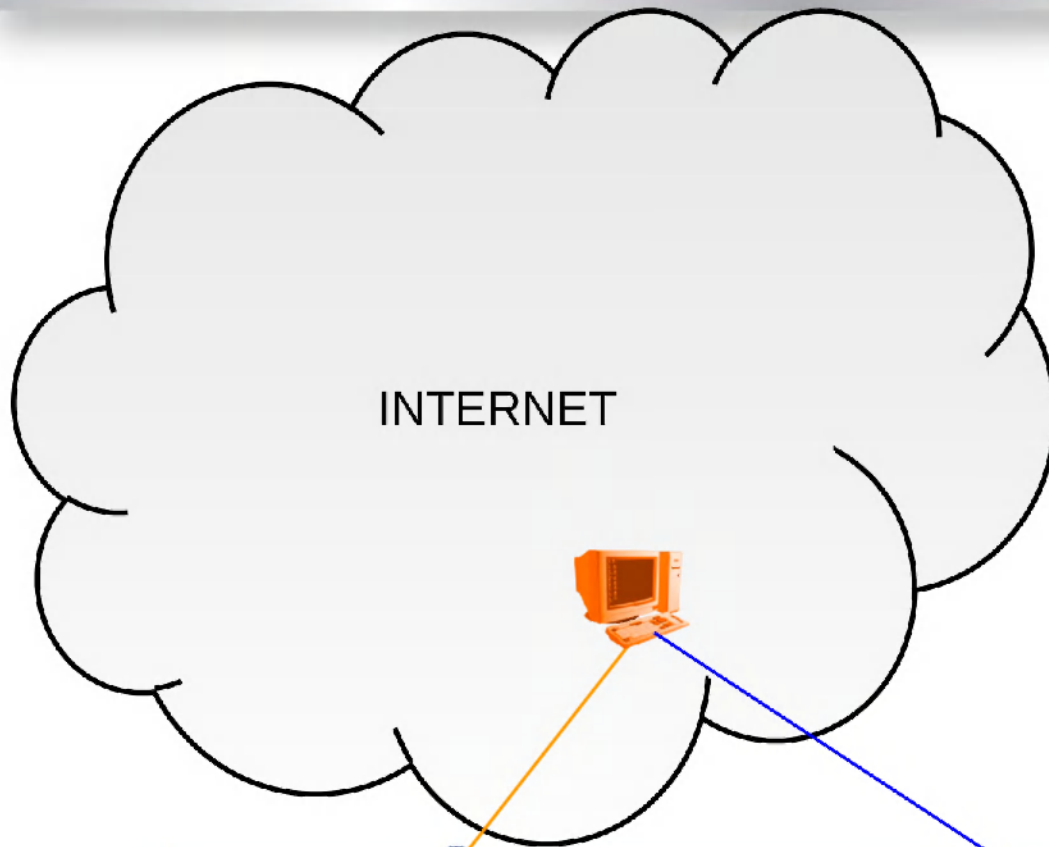


- Cycle ③④ must get to the target before ② occurs
- Once 'hooked,' the target is exploited with no time constraints
- Different QUANTUM effects have different time constraints.

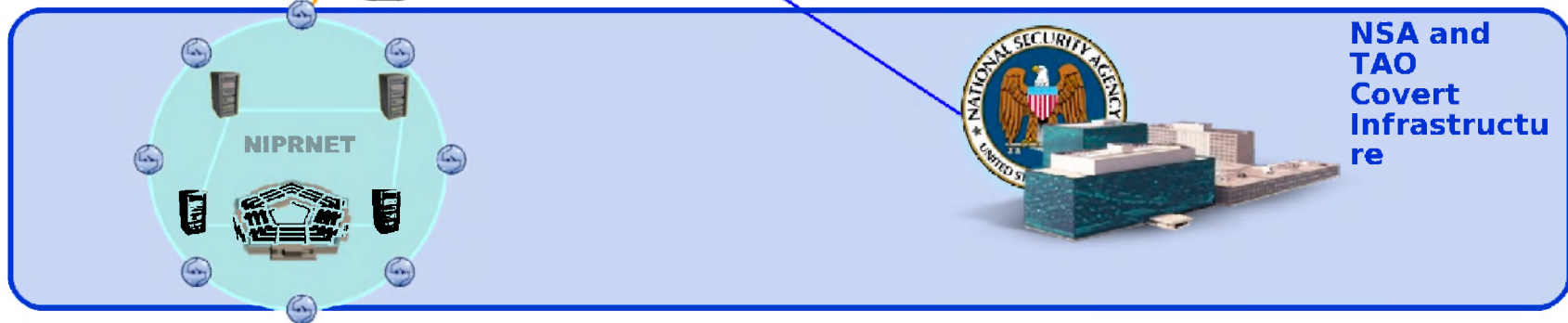
TOP SECRET//COMINT//REL USA, FVEY



# (U//FOUO) BOXINGGRUMBLE Case Study

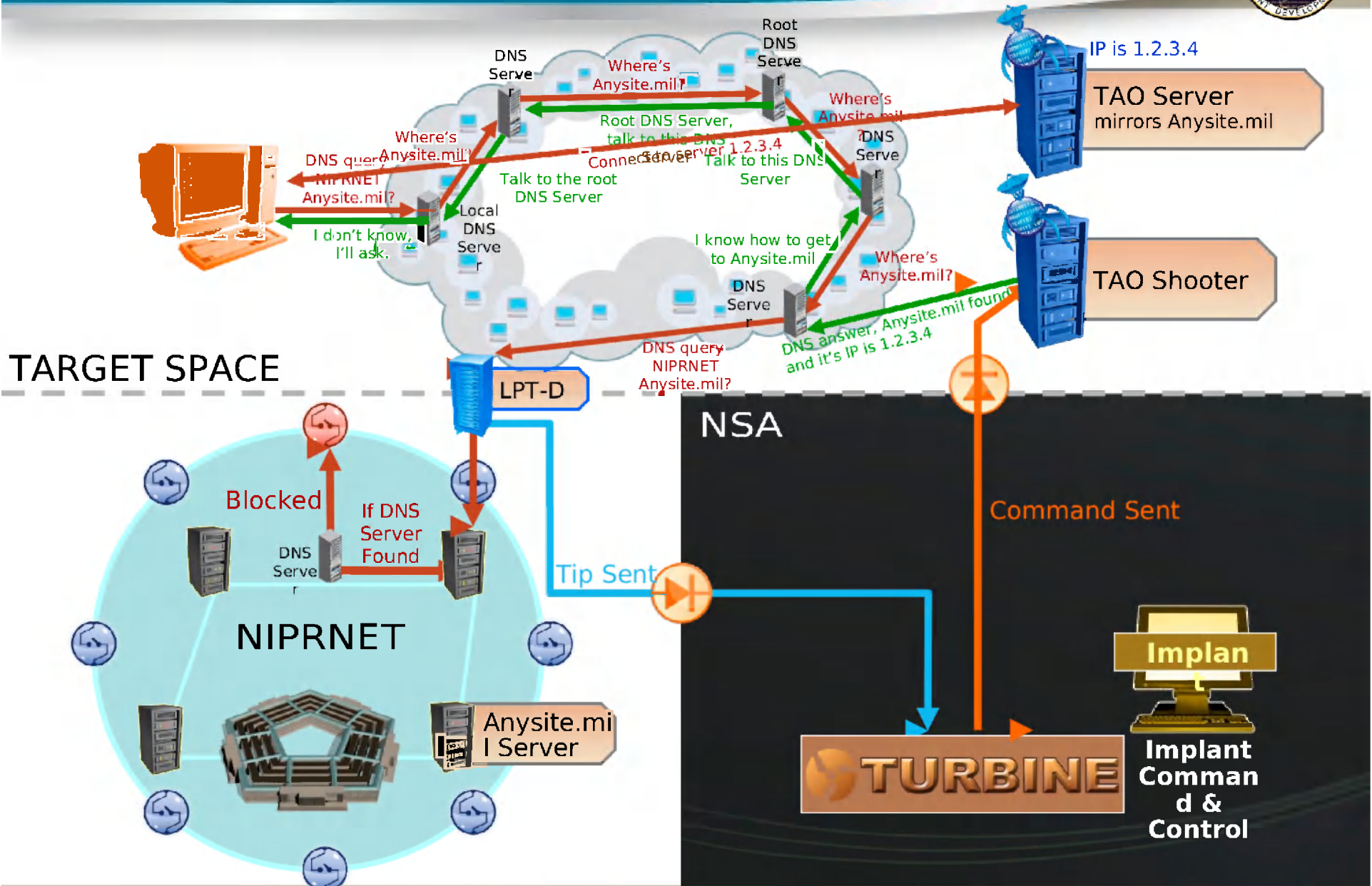


- (S//REL) DNS requests entering NIPRnet domain
  - (S//REL) Destination IP not a NIPRnet DNS server
  - (S//REL) Domain name not within NIPRnet
- (S//REL) DNS behavior of host is suspicious but not dangerous
- (TS//SI//REL) TAO uses QUANTUMDNS to redirect the requesting host

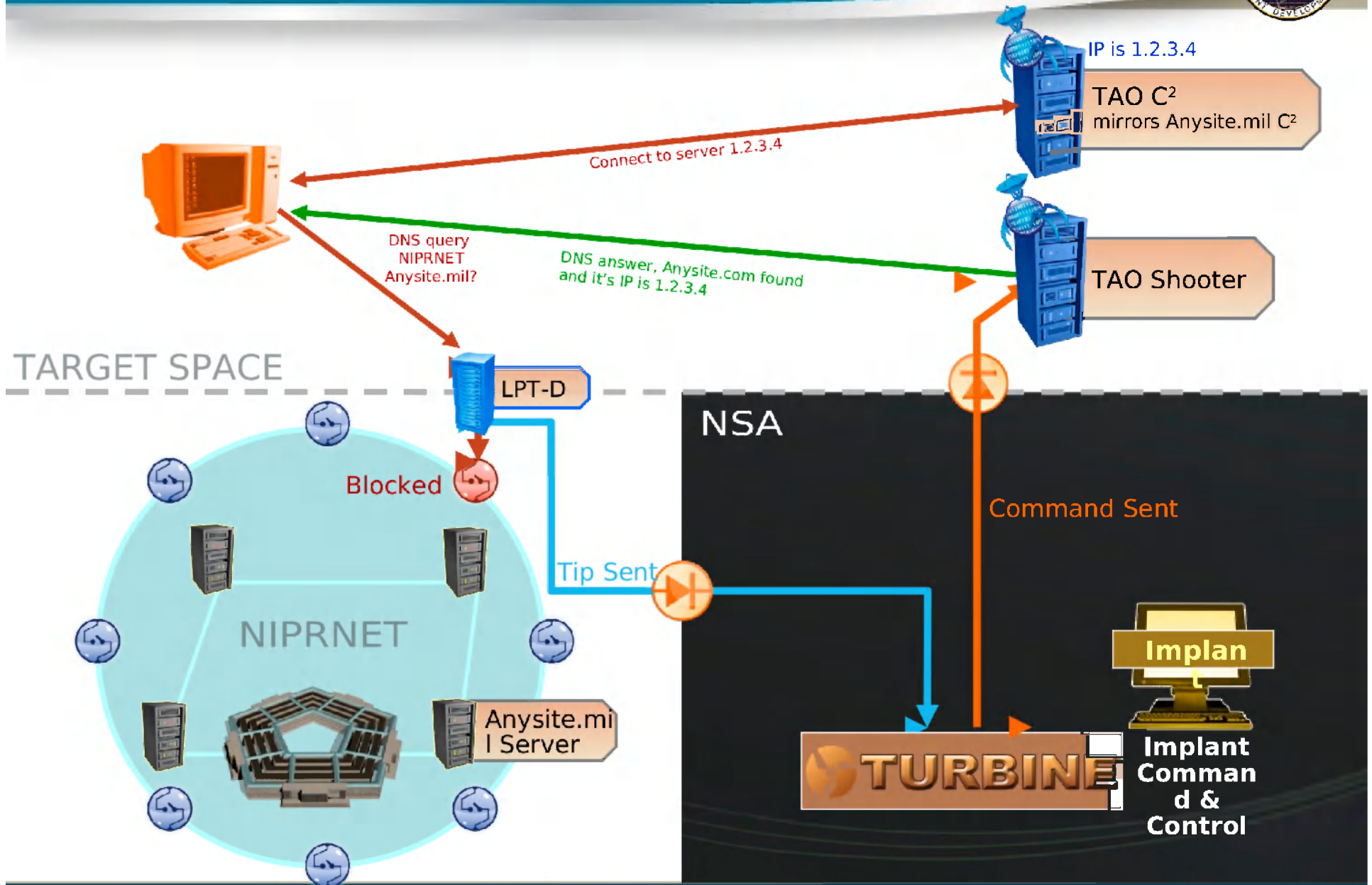




# (S//REL) QUANTUMDNS: An Integrated Cyber Operation

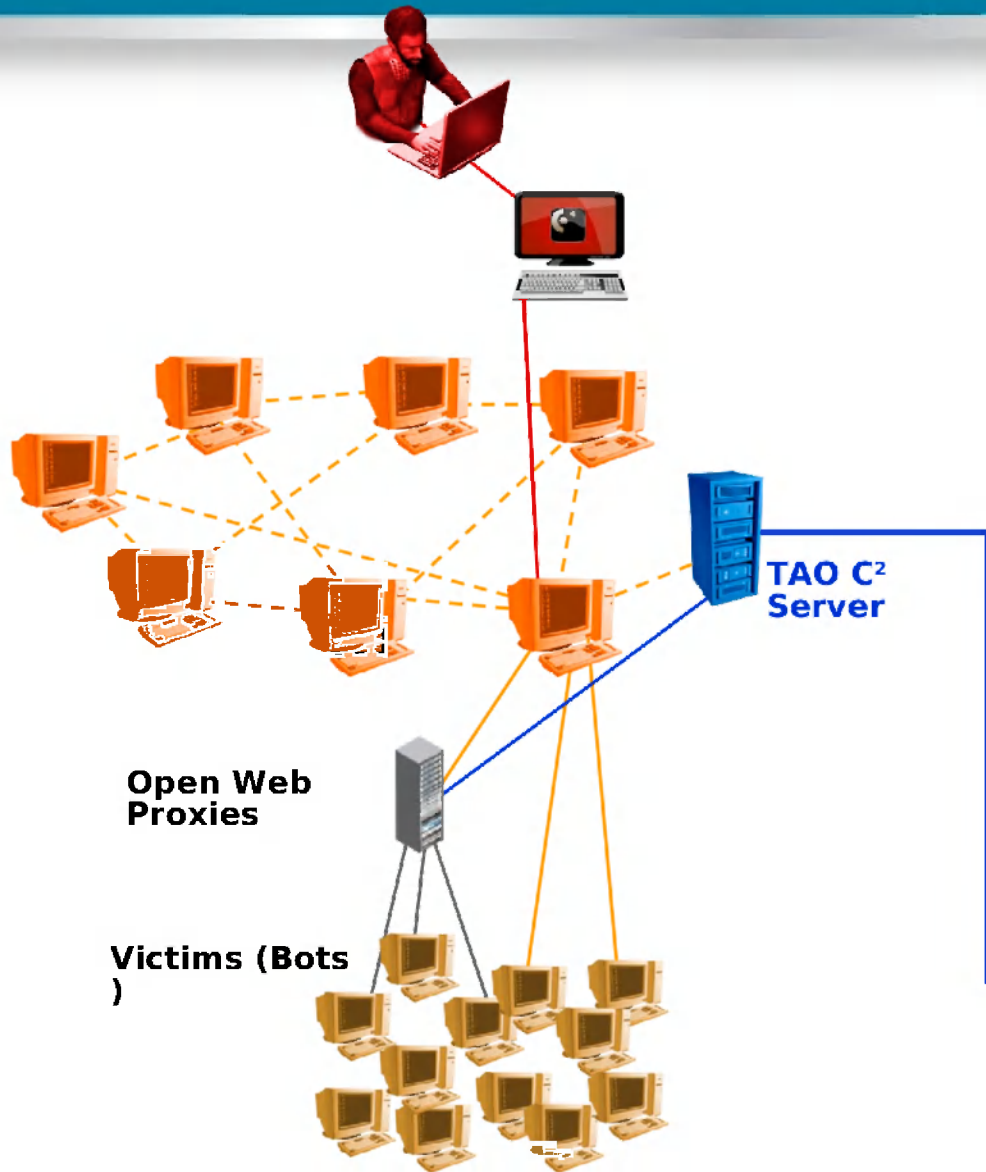


# (S//REL) QUANTUMDNS: As Used Against BOXINGRUMBLE





# (U//FOUO) BOXINGGRUMBLE Case Study

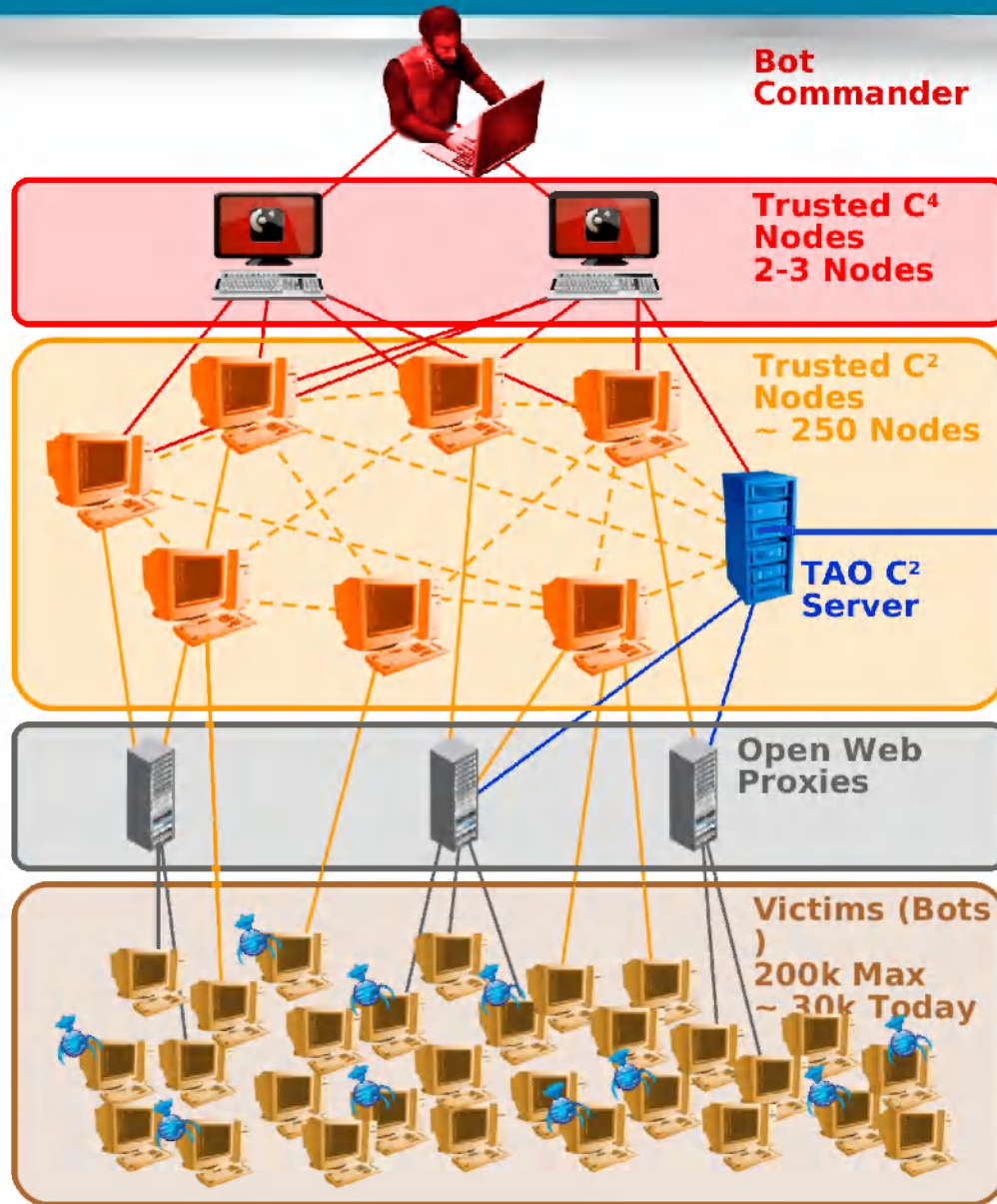


- (TS//SI//REL) TAO establishes itself as a trusted C2 node
- (U//FOUO) Captured traffic indicates the existence of a bot net
  - (S//REL) Command and control split into two layers (C2 and C4)
  - (S//REL) C2 layer has a peer-to-peer mesh network topology with direct connection to a C4 node
- (S//REL)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

NSA and TAO Covert Infrastructure

DEFIANTWARRIOR Implant

The block contains the NSA seal and a 3D rendering of a server rack. A blue line connects the TAO C<sup>2</sup> Server from the main diagram to this block.



(U) There is More Than One Way to

QUANTUM

TOP SECRET//COMINT//REL USA//EYES



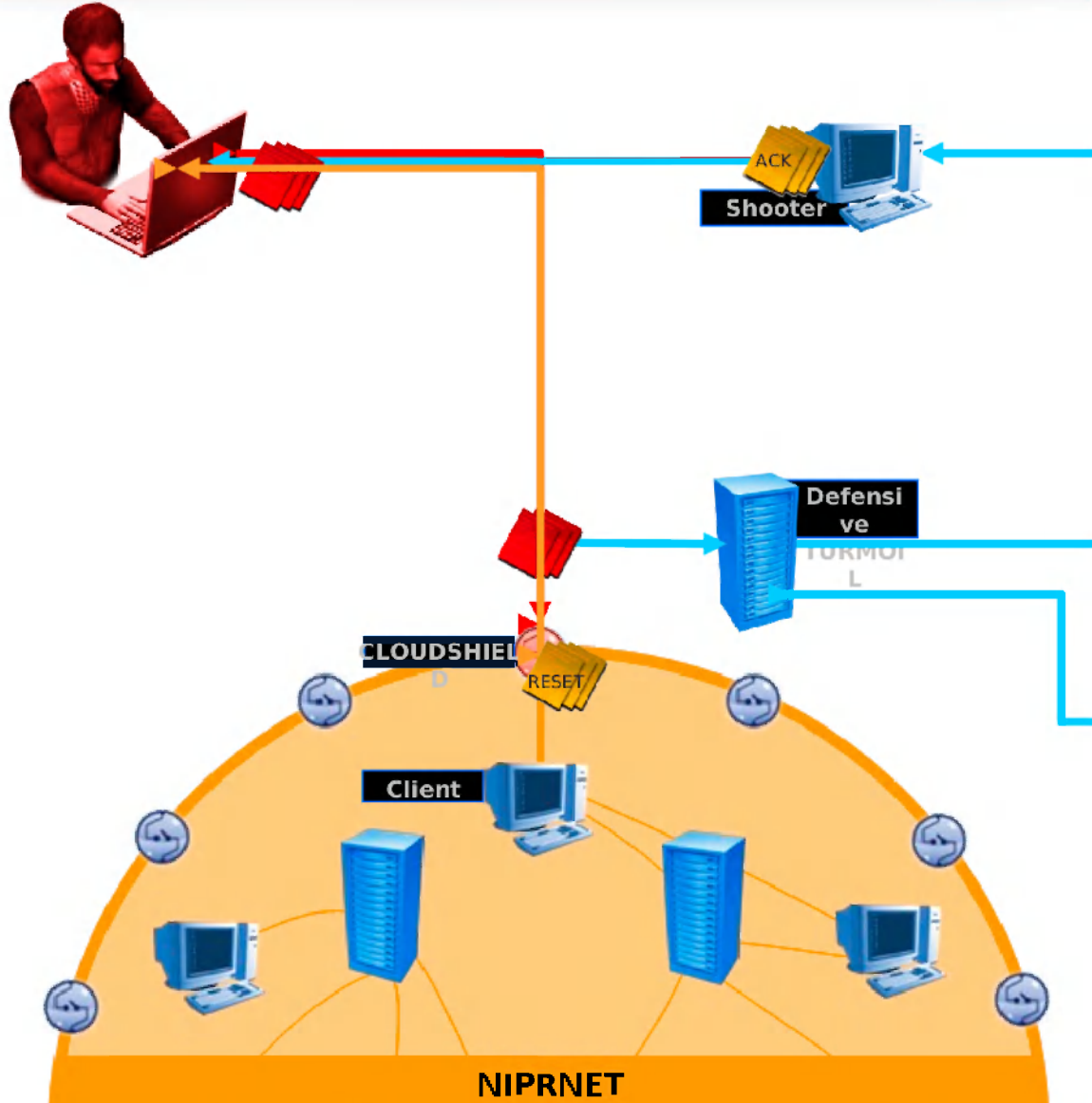
TS//SI//REL

Name	Description	Inception Date	Status	Operational Success
<b>CNE</b>				
<b>QUANTUMINSERT</b>	<ul style="list-style-type: none"> <li>• Man-on-the-Side technique</li> <li>• Briefly hi-jacks connections to a terrorist website</li> <li>• Re-directs the target to a TAO server (FOXACID) for implantation</li> </ul>	2005	Operational	<b>Highly Successful</b> (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
<b>QUANTUMBOT</b>	<ul style="list-style-type: none"> <li>• Takes control of idle IRC bots</li> <li>• Finds computers belonging to botnets, and hijacks the command and control channel</li> </ul>	Aug 2007	Operational	<b>Highly Successful</b> (over 140,000 bots co-opted)
<b>QUANTUMBISCUIT</b>	<ul style="list-style-type: none"> <li>• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation</li> <li>• Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.</li> </ul>	Dec 2007	Operational	<b>Limited success at NSA</b> due to high latency on passive access (GCHQ uses technique for 80% of CNE accesses)
<b>QUANTUMDNS</b>	<ul style="list-style-type: none"> <li>• DNS injection/redirection based off of A Record queries.</li> <li>• Targets single hosts or caching name servers.</li> </ul>	Dec 2008	Operational	<b>Successful</b> (High priority CCI target exploited)
<b>QUANTUMHAND</b>	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	<b>Successful</b>
<b>QUANTUMPHANTOM</b>	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	<b>N/A</b>
<b>CNA</b>				
<b>QUANTUMSKY</b>	Denies access to a webpage through RST packet spoofing.	2004	Operational	<b>Successful</b>
<b>QUANTUMCOPPER</b>	File download/upload disruption and corruption.	Dec 2008	Live	<b>N/A</b>

TS//SI//REL

TOP SECRET//COMINT//REL US  
(U//FOUO) QUANTUMSMA

Internet



TOP SECRET//COMINT//REL US

# A, FVEY CKDOWN



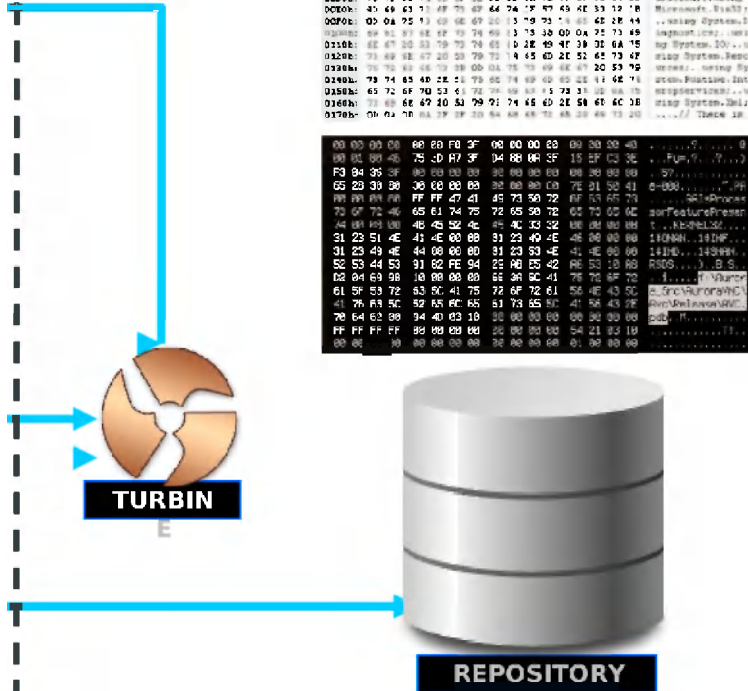
## NSA Space

```

0020: 71 69 8E 87 20 51 79 73 74 85 80 22 43 8F 8C 8C  ....System.Conn
0020: 61 61 74 69 67 41 73 28 87 69 88 63 74 69 43 28  ..ctions-Generi
0020: 00 0A 75 73 69 41 67 2C 23 79 73 71 65 50 2E 43  ..LLING States.C
0040: 67 60 70 67 4E 41 62 74 80 6F 66 61 6C 78 00 0A  ..caAccountCode
0060: 71 71 69 4E 47 21 83 76 73 74 46 60 21 64 61 74  ..velus System-Stat
0080: 41 20 80 8A 70 70 69 8E 87 20 30 79 73 74 69 60  ..a...ating System
0100: 20 44 20 43 77 69 8E 41 78 20 0A 73 71 69 4E 67  ..Drawings...ating
0120: 20 51 79 73 74 65 80 2E 54 45 70 71 31 20 0A 75  ..System-Exec...
0140: 71 69 8E 87 20 51 79 73 74 43 80 21 57 69 4E 44  ..Atto System-Exec
0160: 67 71 73 2C 14 6F 73 4E 72 39 00 0A 75 70 69 6E  ..User-Process...
0180: 67 60 70 67 4E 47 67 71 6F 44 74 21 57 69 4E 44  ..User-Process-Exec
0200: 67 71 71 4F 6F 60 69 66 65 2E 43 67 50 66 69 67  ..oneBolt.c-COACTC
0220: 73 71 51 71 6F 6F 62 3E 00 0A 75 73 69 6F 67 20  ..ventions...ating
0240: 41 69 63 71 6F 70 66 74 79 47 43 4E 43 13 74  ..Management-Stat
0260: 00 0A 75 71 69 6F 60 61 71 70 71 71 69 4E 44  .....ating System-Stat
0280: 6E 61 67 6E 6F 73 74 69 63 73 30 00 0A 71 73 69  ..Management-Stat
0300: 4E 67 20 53 79 73 74 65 10 2E 49 4F 38 3E 6A 75  ..ng System-Stat
0320: 71 69 8E 87 20 23 79 73 74 45 60 2E 52 45 73 4F  ..Atto System-Exec
0340: 71 73 69 6E 72 39 00 0A 75 70 69 4E 44  ..User-Process-Exec
0360: 73 74 65 40 2E 11 73 60 74 69 49 60 2E 41 4E 71  ..User-Process-Stat
0380: 63 72 6F 70 53 41 70 70 69 66 71 72 31 20 0A 70  ..Management-Stat
0400: 71 69 8E 87 10 51 70 71 74 4E 40 2E 58 60 4C 2B  ..Atto System-Stat
0420: 0A 70 70 6A 79 3F 55 6A 68 49 70 6B 20 68 73 20  ...../..Trace-Stat
    
```

```

00 00 00 00 60 20 F0 3F 00 00 00 00 00 00 00 00  ..F...
00 00 00 40 75 20 F7 3F 04 80 80 3F 15 2F C3 3C  ..F...
F3 84 36 3F 80 00 00 00 00 00 00 00 00 00 00 00  ..F...
55 23 30 30 30 00 00 00 00 00 00 00 7E 01 50 41  ..5...
70 6F 6F 6F 6F 6F 6F 41 45 73 50 72 6F 53 65 73  ..F...
70 6F 72 46 65 61 74 75 72 65 30 72 05 70 00 4C  ..F...
44 8F 80 00 4B 40 32 4C 4C 4C 33 32 80 00 80 88  ..F...
31 23 51 4E 41 4E 00 88 31 23 40 4E 4E 00 00 88  ..F...
31 23 49 4E 44 00 00 80 31 23 53 4E 41 4E 00 00  ..F...
55 20 44 53 31 02 7E 04 25 40 52 42 8E 50 10 80  ..F...
02 04 69 98 10 00 00 80 2E 30 5C 41 70 6E 6F 70  ..F...
61 5F 53 72 63 5C 41 75 2F 6F 72 61 5E 4F 43 5C  ..F...
41 76 63 5C 52 65 6C 65 51 73 85 67 41 58 43 2E  ..F...
70 64 63 80 34 40 63 10 30 00 00 00 00 00 00 00  ..F...
FF FF FF FF 82 00 80 00 20 00 00 00 54 21 83 18  ..F...
00 60 70 60 00 00 30 80 80 60 01 90 80 80  ..F...
    
```



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) 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

TOP SECRET//COMINT//REL USA//EYES



TS//SI//REL

Name	Description	Inception Date	Status	Operational Success
<b>CNE</b>				
<b>QUANTUMINSERT</b>	<ul style="list-style-type: none"> <li>• Man-on-the-Side technique</li> <li>• Briefly hi-jacks connections to a terrorist website</li> <li>• Re-directs the target to a TAO server (FOXACID) for implantation</li> </ul>	2005	Operational	<b>Highly Successful</b> (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
<b>QUANTUMBOT</b>	<ul style="list-style-type: none"> <li>• Takes control of idle IRC bots</li> <li>• Finds computers belonging to botnets, and hijacks the command and control channel</li> </ul>	Aug 2007	Operational	<b>Highly Successful</b> (over 140,000 bots co-opted)
<b>QUANTUMBISCUIT</b>	<ul style="list-style-type: none"> <li>• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation</li> <li>• Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.</li> </ul>	Dec 2007	Operational	<b>Limited success at NSA</b> due to high latency on passive access (GCHQ uses technique for 80% of CNE accesses)
<b>QUANTUMDNS</b>	<ul style="list-style-type: none"> <li>• DNS injection/redirection based off of A Record queries.</li> <li>• Targets single hosts or caching name servers.</li> </ul>	Dec 2008	Operational	<b>Successful</b> (High priority CCI target exploited)
<b>QUANTUMHAND</b>	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	<b>Successful</b>
<b>QUANTUMPHANTOM</b>	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	<b>N/A</b>
<b>CNA</b>				
<b>QUANTUMSKY</b>	Denies access to a webpage through RST packet spoofing.	2004	Operational	<b>Successful</b>
<b>QUANTUMCOPPER</b>	File download/upload disruption and corruption.	Dec 2008	Live	<b>N/A</b>

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])