(U//FOUO) QUANTUMTHEORY

(U//FOUO) name redacted S32X

(U) Classification of Presentation

- This presentation is classified:

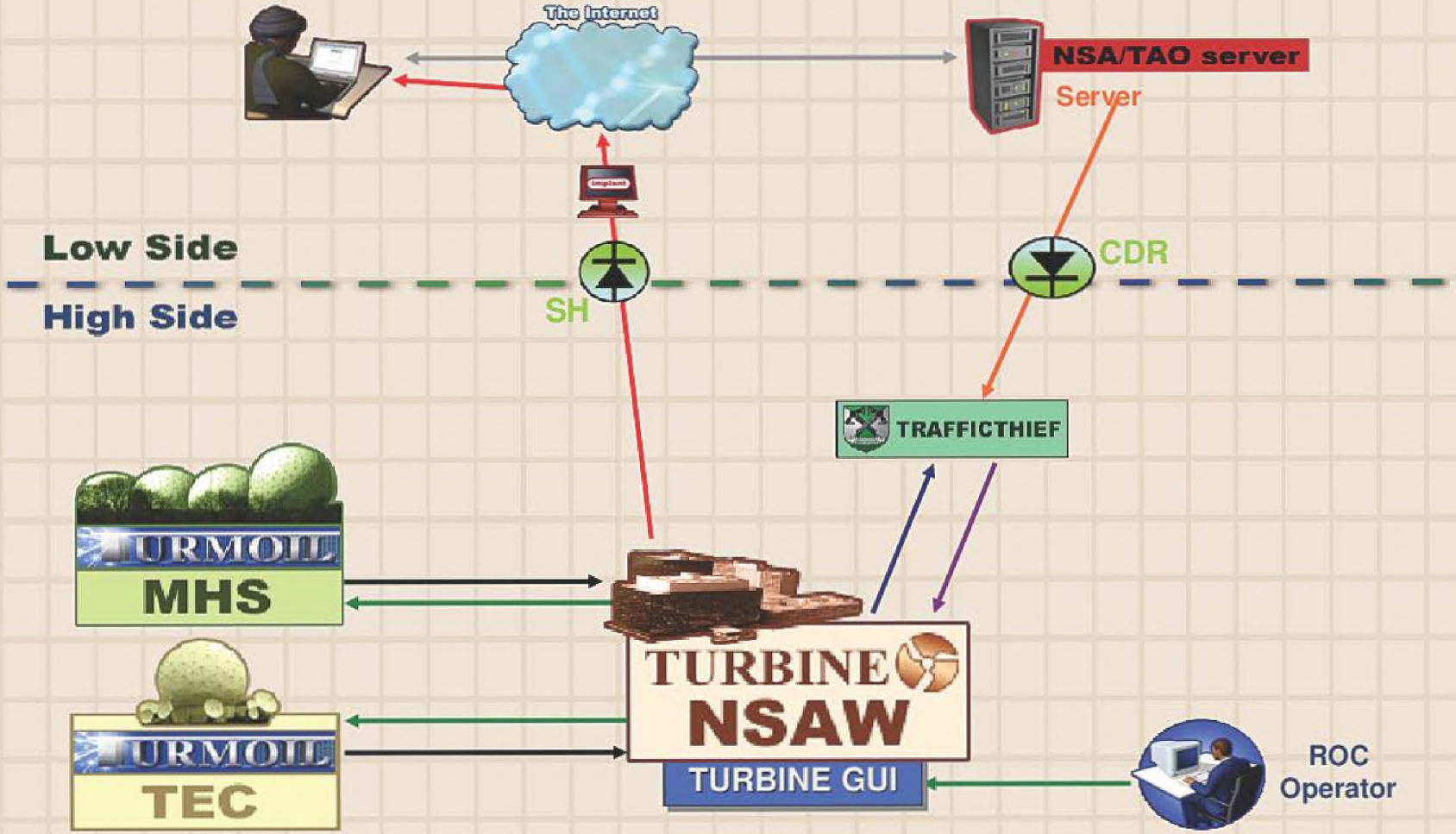
TOP SECRET // COMINT // REL TO USA, FVEY // 20320108

(U) What is QUANTUMTHEORY

- (U//FOUO) Nothing to do with "Quantum Computing"
- (S//SI//REL) Protocol injection technique
  - Passive
  - Active
- (S//REL) Not Man-in-the-Middle
  - But can be used to gain that position
- (S//REL) Man-on-the-Side
- (S//REL) Mostly Low Latency… mostly



(U) Man on the Side?



(C) Components of QUANTUM Architecture

- (S//REL) TURMOIL
  - (or LPT, LPT-D, what else can you kludge for tipping… cough.. NINJANIC)
  - Passive Sensor
- (S//REL) TURBINE
  - Active Mission Logic of Remote Agents
- (C//REL) ISLANDTRANSPORT
  - Messaging Fabric
- (S//REL) SURPLUSHANGER
  - High->Low diodes
- (S//REL) STRAIGHTBIZARRE or DAREDEVIL
  - Implant / Shooter



(C) Legacy QUANTUMTHEORY techniques

- (TS//SI//REL) QUANTUMINSERT
  - HTML Redirection
- (TS//SI//REL) QUANTUMSKY
  - HTML/TCP resets
- (TS//SI//REL) QUANTUMBOT
  - IRC botnet hijacking


(U) New Hotness

- (TS//SI//REL) QUANTUMBISCUIT
  - Redirection based on keywork
  - Mostly HTML Cookie Values
- (TS//SI//REL) QUANTUMDNS
  - DNS Hijacking
  - Caching Nameservers
- (TS//SI//REL) QUANTUMBOT2
  - Combination of Q-BOT/Q-BISCUIT for web based Command and controlled botnets

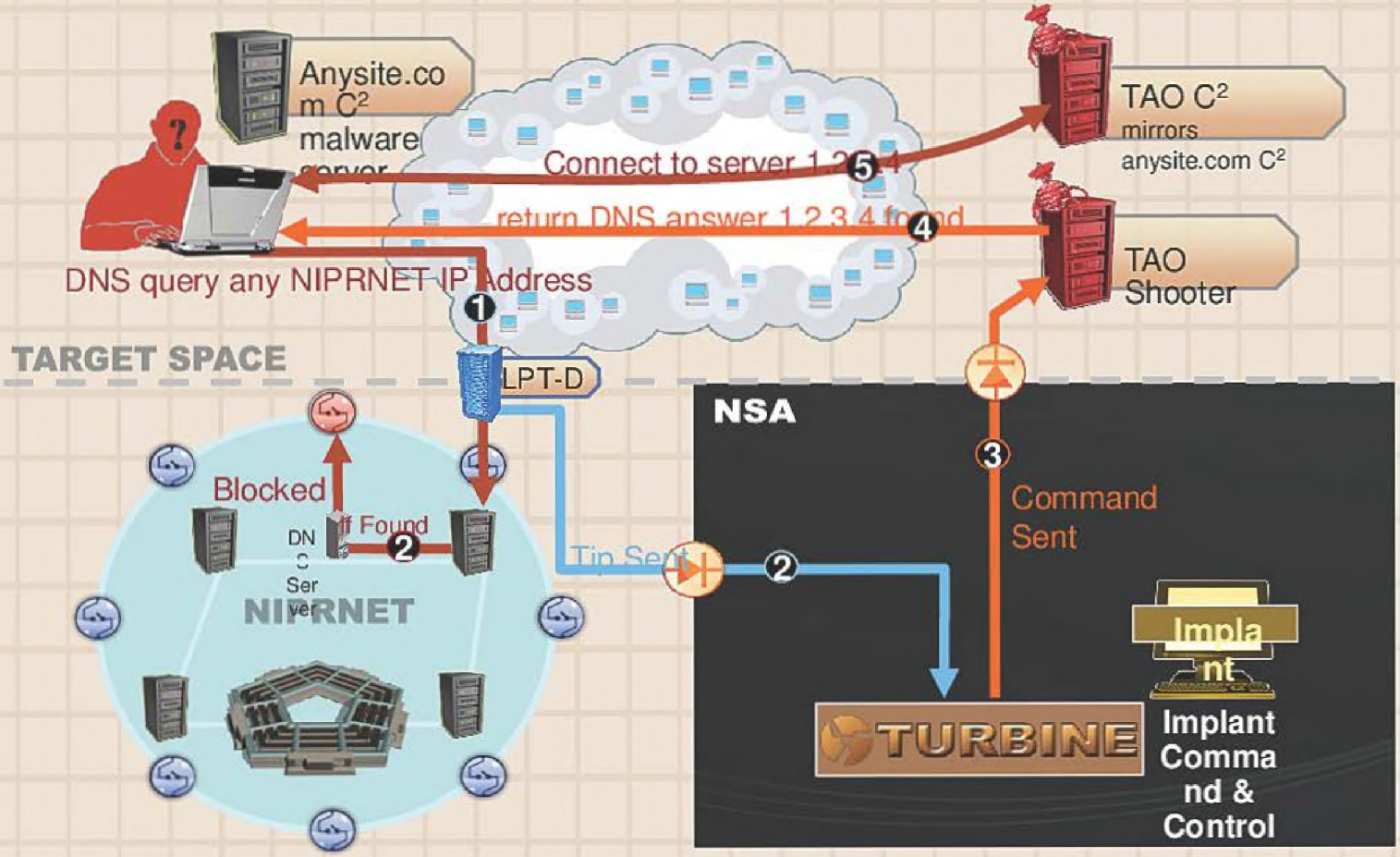


(U) Experimental

- (TS//SI//REL) QUANTUMCOPPER
  - File download disruption
- (TS//SI//REL) QUANTUMMMUSH
  - Virtual HUFFMUSH / Targeted Spam Exploitation
- (TS//SI//REL) QUANTUMSPIM
  - Instant Messaging (MSN chat, XMPP)
- (TS//SI//REL) QUANTUMSQUEEL
  - Injection into MySQL persistent database connections
- (TS//SI//REL) QUANTUMSQUIRREL
  - Truly covert infrastructure, be any IP in the world



(U//FOUO) QUANTUMDEFENSE



(C) Where/What can you QUANTUM

- (S//SI//REL) Menwith Hill Station (USJ-759, USJ-759A,…)
  - Operational: Q-INSERT, Q-SKY, Q-DNS, Q-BISCUIT, Q-BOT
  - Tested: Q-COPPER, Q-SQUIRREL, Q-BOT2
- (S//SI//REL) Misawa AFB (USF-799,…)
  - Operational: Q-INSERT
- (S//SI//REL) INCENSOR (DS-300) – with help from GCHQ
  - Operational: Q-BOT, Q-BISQUIT, Q-INSERT
  - Tested: Q-SQUEEL, Q-SPIM
- (TS//SI//REL) NIPRNET Gateways
  - Operational: Q-DNS
- (S//SI//REL) Coming Soon….
  - SMOKEYSINK
  - SARATOGA


Questions?

contact info redacted