American Spies

Surveillance versus Security

NSA Crypto History

- DES
- Public Key Crypto
- NSF
- ITAR
- Invention Secrecy Act of 1951

Clipper Chip & Crypto Wars

CALEA & lawful intercept

- Surveillance Friendly POTS network

Skype


FAA702 Operations
Two Types of Collection
PRISM
Upstream
• Collection of communications on fiber cables and infrastructure as data flows past.
(FAIRVIEW, [redacted], BLARNEY, [redacted])
You Should Use Both
PRISM
• Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

Lavabit

Pen Register/Trap & Trace

"a provider … shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services"

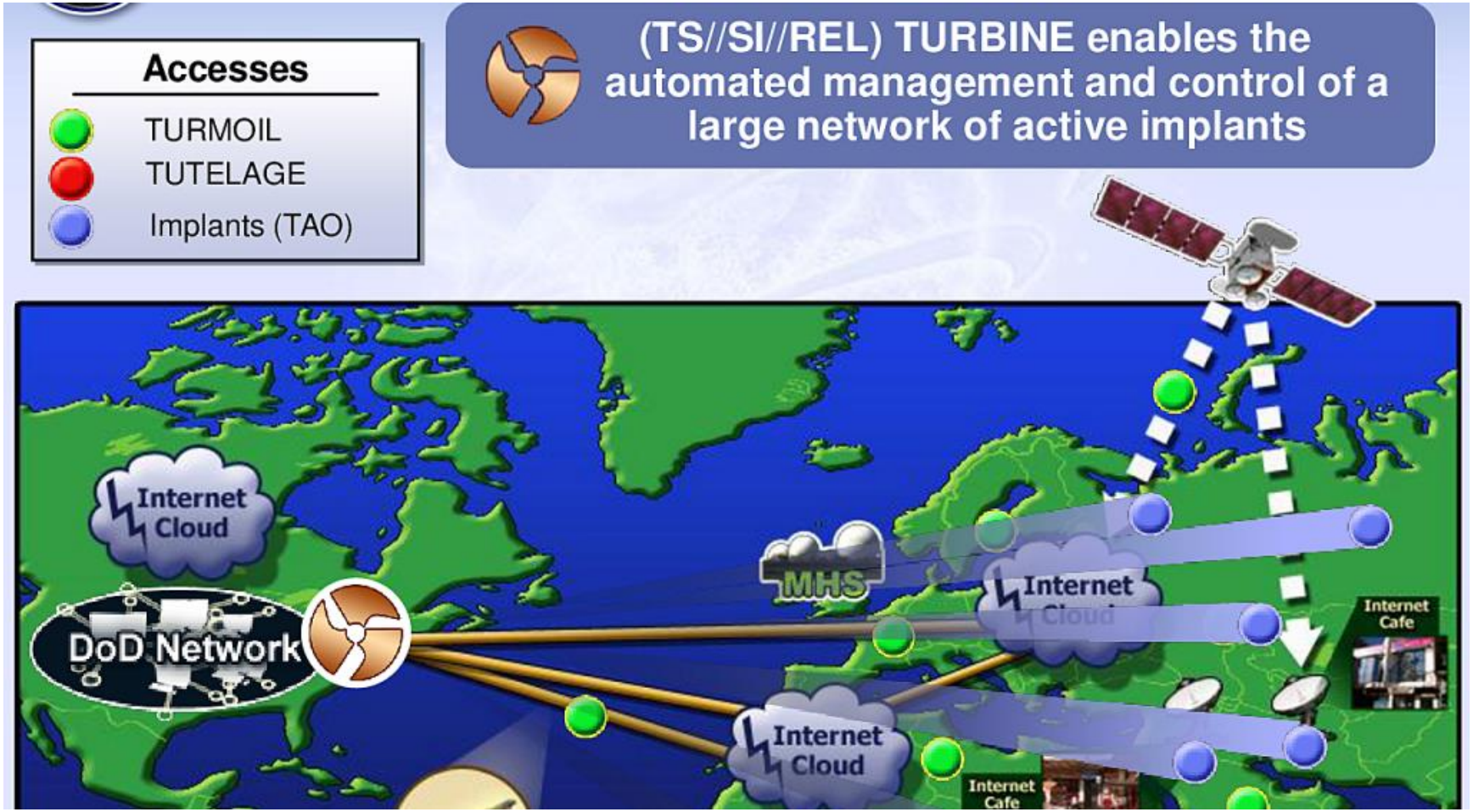
Apple Phone Encryption

All Writs Act (1789)

The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

BULLRUN

Botnets


Accesses
TURMOIL
TUTELAGE
Implants (TAO)
(TS//SI//REL) TURBINE enables the automated management and control of a large network of active implants
Internet Cloud
DoD Network
MHS
Internet Cloud
Internet Cloud
Internet Cafe
Internet Cafe

Router Hacking

0day

- How much is the vulnerable system used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
- Does the vulnerability, if left unpatched, impose significant risk?
- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- How likely is it that we would know if someone else was exploiting it?
- How badly do we need the intelligence we think we can get from exploiting the vulnerability?
- Are there other ways we can get it?
- Could we utilize the vulnerability for a short period of time before we disclose it?
- How likely is it that someone else will discover the vulnerability?
- Can the vulnerability be patched or otherwise mitigated?

Oversight

- Judges?
- Congress?
- Agencies?
- Legal authority?