Cyber Threats: Applying the Law to Malicious Cyber Activity by States

Texas Bar Military and Veterans Law Section

January 15, 2021

Todd Huntley

Director, National Security Law Program

Georgetown University Law Center

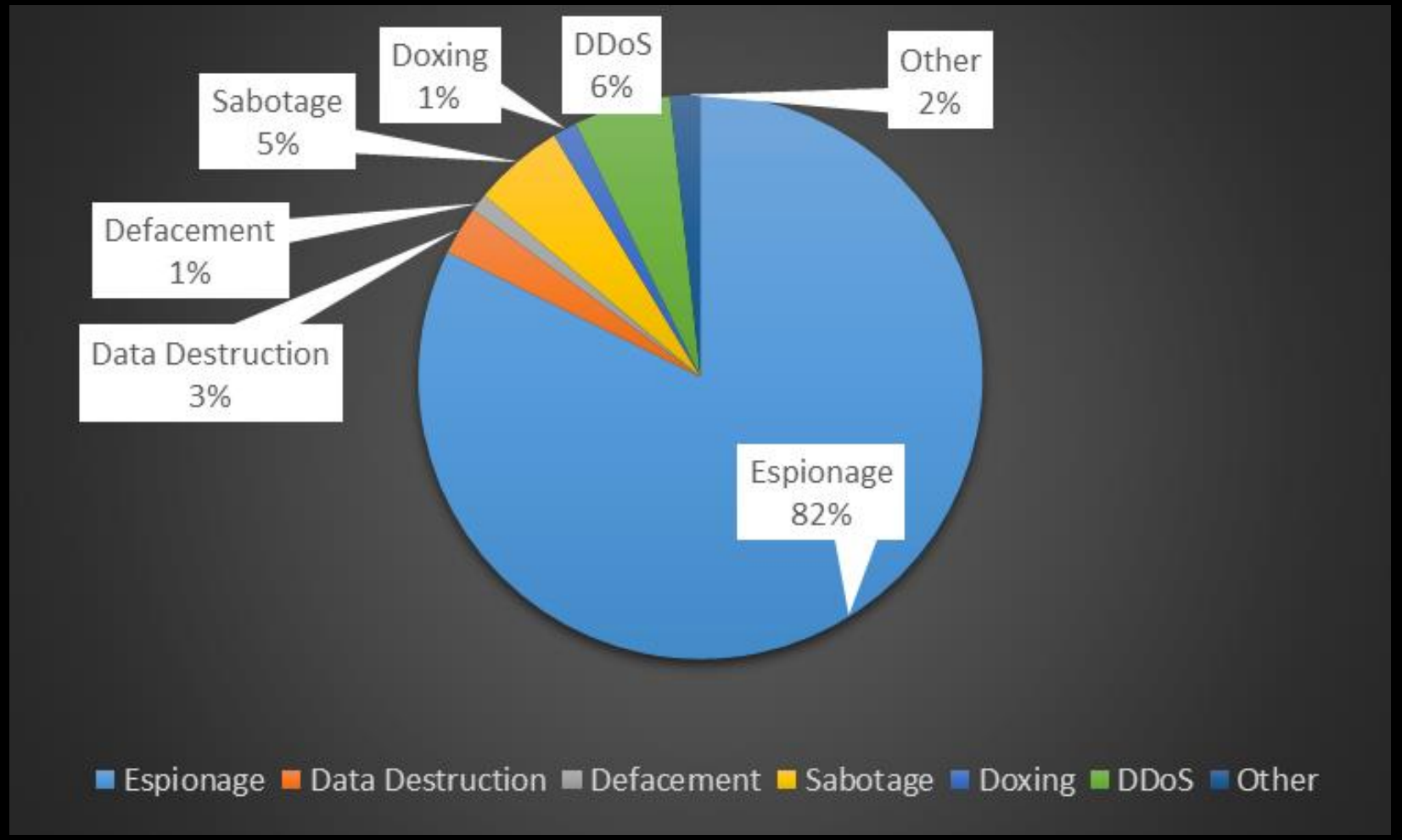
What is the threat?

"The good news is that there are only three things you can do to a computer: steal its data, misuse credentials, and hijack resources."

- Cybersecurity and Cyberwar, Singer and Friedman, p. 39.

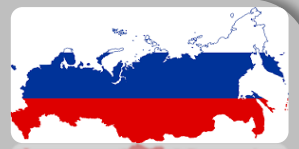
Operational Environment – Threats

- **Types of CO**
  - Espionage
  - DDoS
  - Sabotage
  - Destruction
  - Doxing
  - Defacement



Threat Actors

Russia



- Most Sophisticated/Covert
- Large Cyber Crime Nexus
- DDoS - Estonia (2007), Georgia (2008)
- Energy Sector - Ukraine (2015), U.S. (2017)
- Political Influence Activity - Western gov'ts (2016 – present)

China

- Very Active
- Increasingly Sophisticated
- IP Theft
- Increasing Influence Activity (COVID)

Hacktivists

- Website Defacements
- Counter-narrative
- DDoS Attacks

Cyber Crime

- Identity Theft
- Financial Motivation

North Korea

- Active Propaganda
- Offensive Capabilities
- Sony (2014)

Iran

- Rapid Development
- Persistent Presence
- Saudi Aramco (2012)

Gov & Mil Networks

Weapon Systems - R&D

Top Threat Vectors
Socially Engineered Email
Public Websites
Common Vulnerabilities
Non-patched software
Poor user security

Energy Sector

Intellectual Property

Banks & Finance

Cyber Ops Legal and Authority Issues

Application and analysis of law and authorities to cyberspace operations is fact dependent

- Domestic and International Law apply to cyberspace operations
- The Law of Armed Conflict applies to cyberspace operations that rise to the level of an armed conflict
- The difficulty is in applying the law to new capabilities and factual situations

Must identify

- What is purpose of activity?
- What is the effect of the activity?
- Where will activity take place?
- Where will effects manifest?
- Will the activity be conducted with the consent of, or notice to, the relevant State(s)?

What is Cyberspace?

- Three Interrelated Layers (JP 3-12)
  1. Physical
     - Computers/servers/routers/wires & waves
     - Hardware
     - Geography matters!
  2. Logical
     - Data – 1s & 0s
     - Software / Apps
     - Who owns it? Can we “attack” it?
  3. Cyber-Persona
     - Users
     - Users ≠ People
     - The Attribution Problem

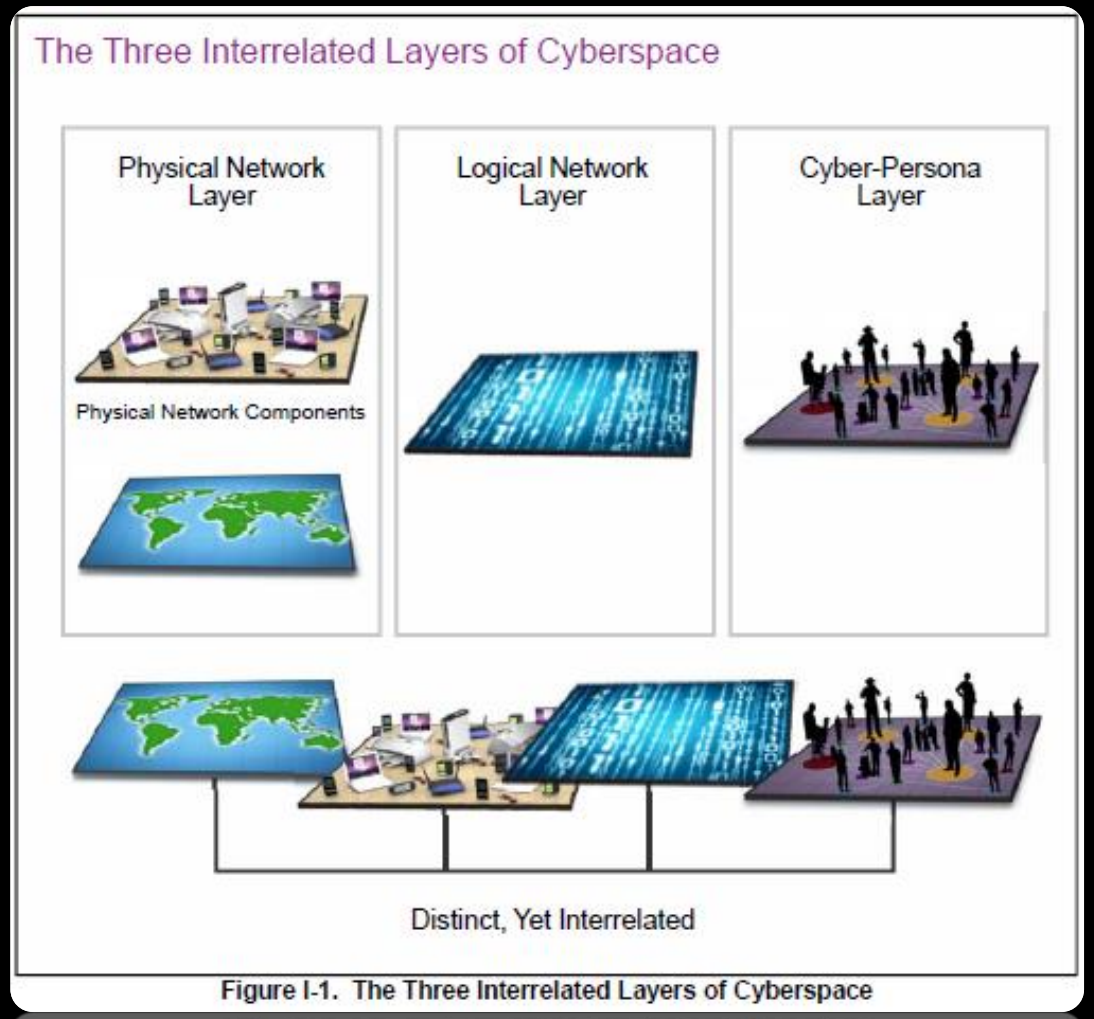
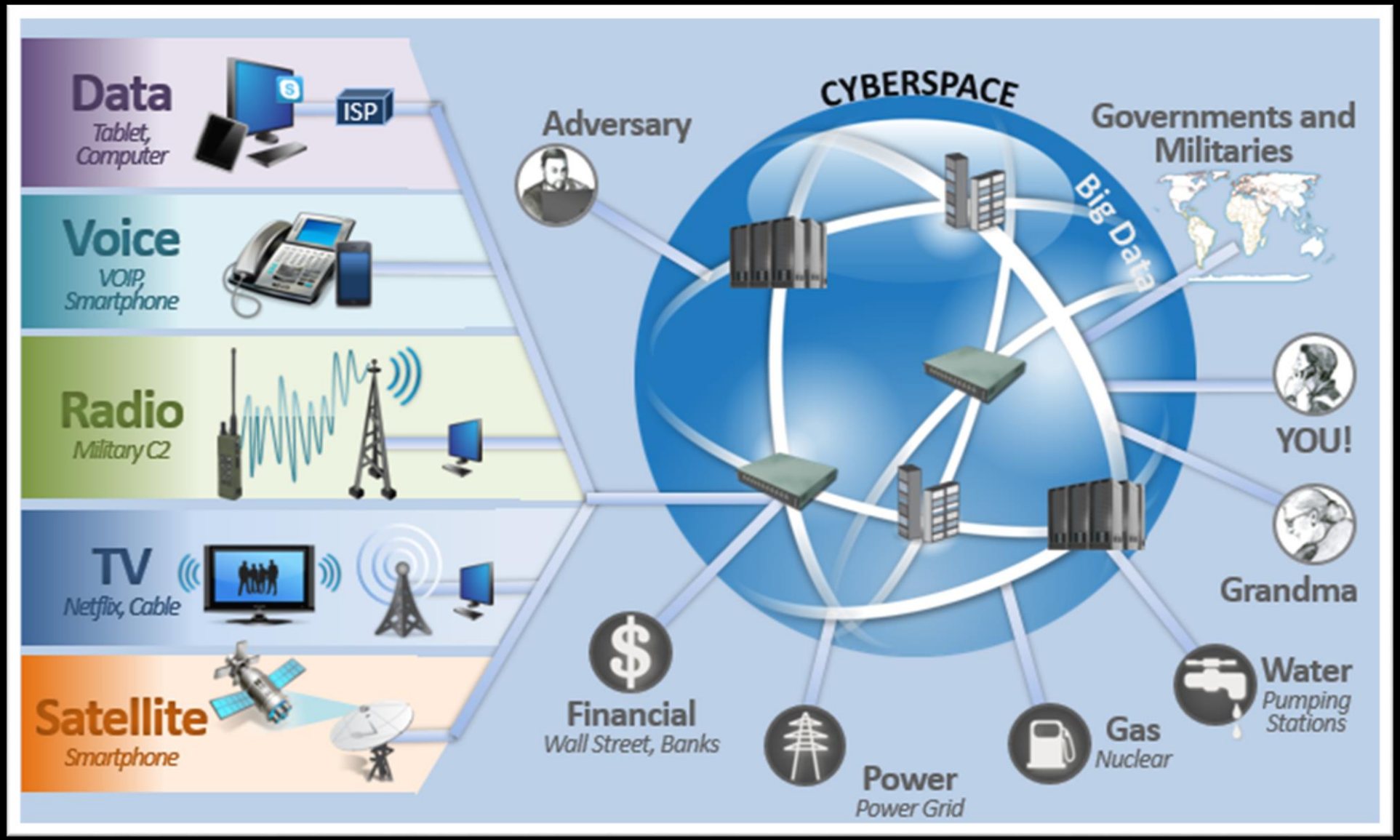
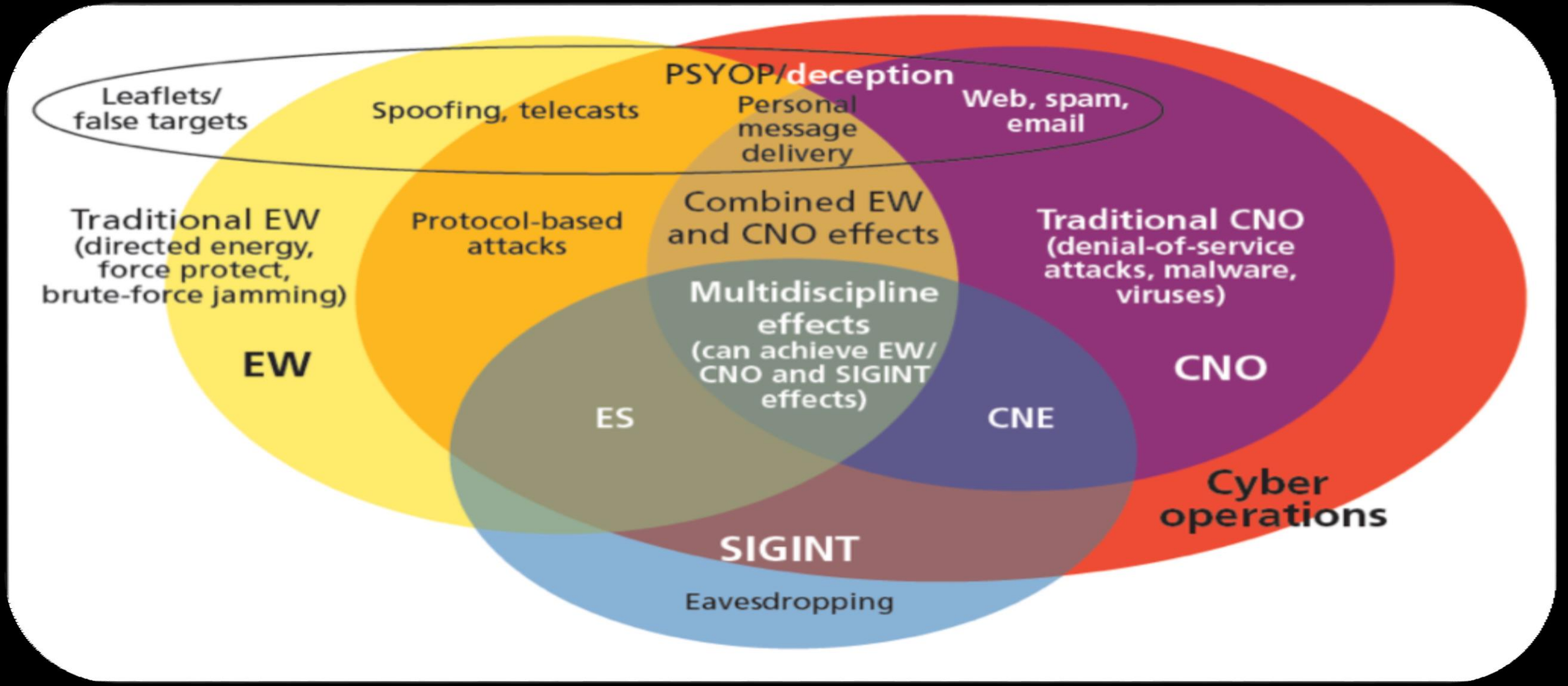


Figure I-1. The Three Interrelated Layers of Cyberspace

But, What is Cyberspace, Really?



Cyber or Something Else?

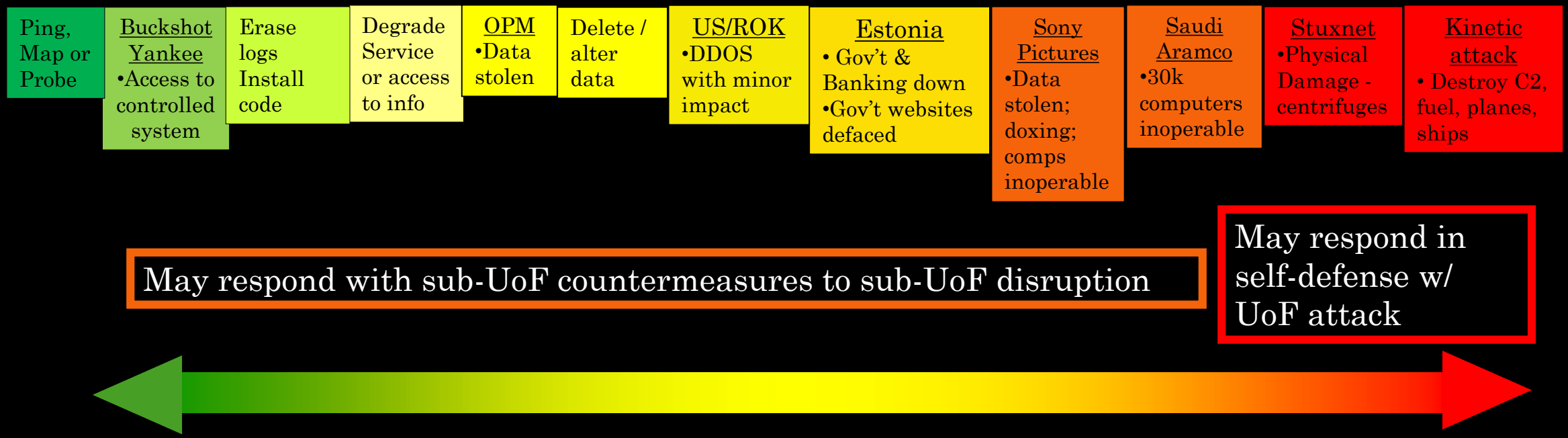


What is the threat?

"The good news is that there are only three things you can do to a computer: steal its data, misuse credentials, and hijack resources."

- Cybersecurity and Cyberwar, Singer and Friedman, p. 39.

Spectrum of Cyber Operations



Access Operations
Digital intelligence (e.g., stealthy implant)

Cyber Disruption
Interrupt the flow of information or function of information systems without physical damage or injury

Cyber Attack
Physical damage to property or injury to persons

Cyber Ops Legal and Authority Issues

Application and analysis of law and authorities to cyberspace operations is fact dependent

- Domestic and International Law apply to cyberspace operations
- The Law of Armed Conflict applies to cyberspace operations that rise to the level of an armed conflict
- The difficulty is in applying the law to new capabilities and factual situations

Must identify

- What is purpose of activity?
- What is the effect of the activity?
- Where will activity take place?
- Where will effects manifest?
- Will the activity be conducted with the consent of, or notice to, the relevant State(s)?

International Wrongful Acts & State Responses

Violation of Sovereignty	Violation of Principle of Non-Intervention	Use of Force	Armed Attack
Violation of diplomatic facilities, airspace, waters Exercise of law enforcement authority	Interference in election Support to internal opposition groups Coercion affecting political, economic, social, & cultural systems Coercion affecting foreign policy	Border incursions Support to armed groups/UW	Kinetic military force Support to armed groups/UW

- Retorsion
- Counter-measures
- Domestic legal measures

Use of force in self-defense – art. 51
- *Jus ad bellum*
- LOAC

DoD Cyber Operations Spectrum

DODIN

- Inside DOD/Friendly Network
- Network focused; Threat Agnostic
- E.g., Anti-Virus Software / Network construction

DCO-IDM (CPTs)

- Inside DOD/Friendly Network
- Specific Threat
- E.g., Seeking/Removing Insider Threat

DCO-RA (NMTs)

- Outside DOD/Friendly Network
- W/o permission of the owner / operator of the network
- Specific Threat
- E.g., Stopping attack before it happens

OCO

- Outside DOD/Friendly Network
- Specific Threat
- E.g., Shutting down enemy network prior to attack

LEGAL CONSIDERATIONS/AUTHORITIES

US Government Departments and Agencies

Global Cyberspace

DOJ/FBI

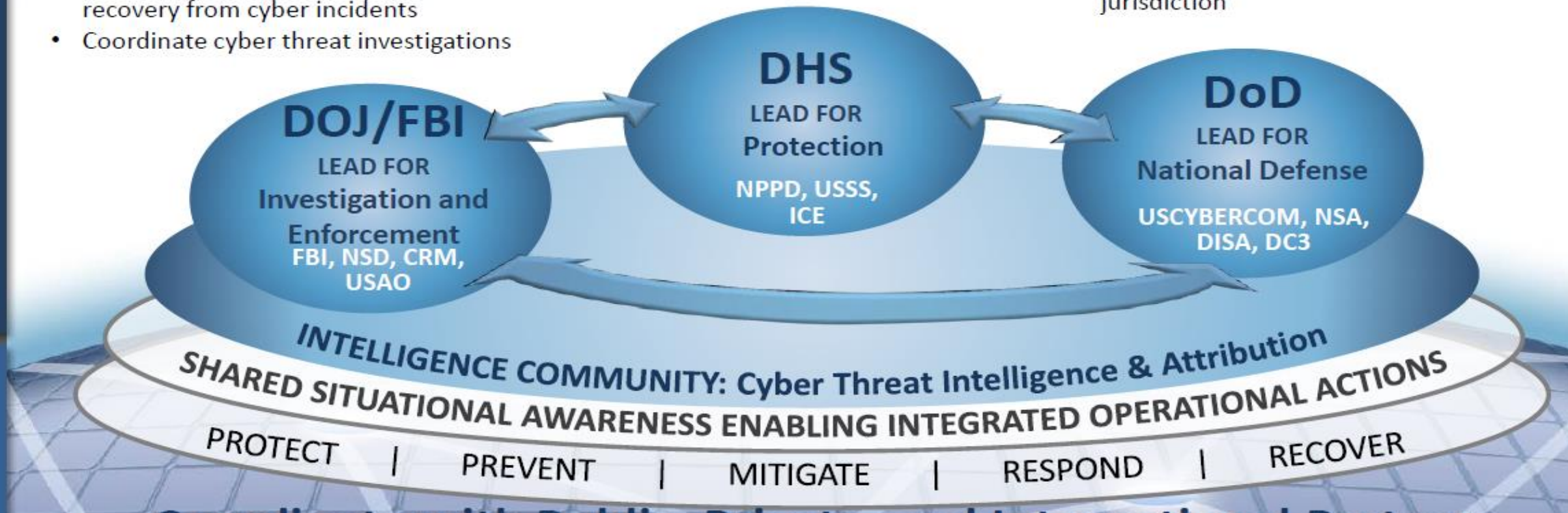
- Investigate, attribute, disrupt and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

DHS

- Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS's jurisdiction

DoD

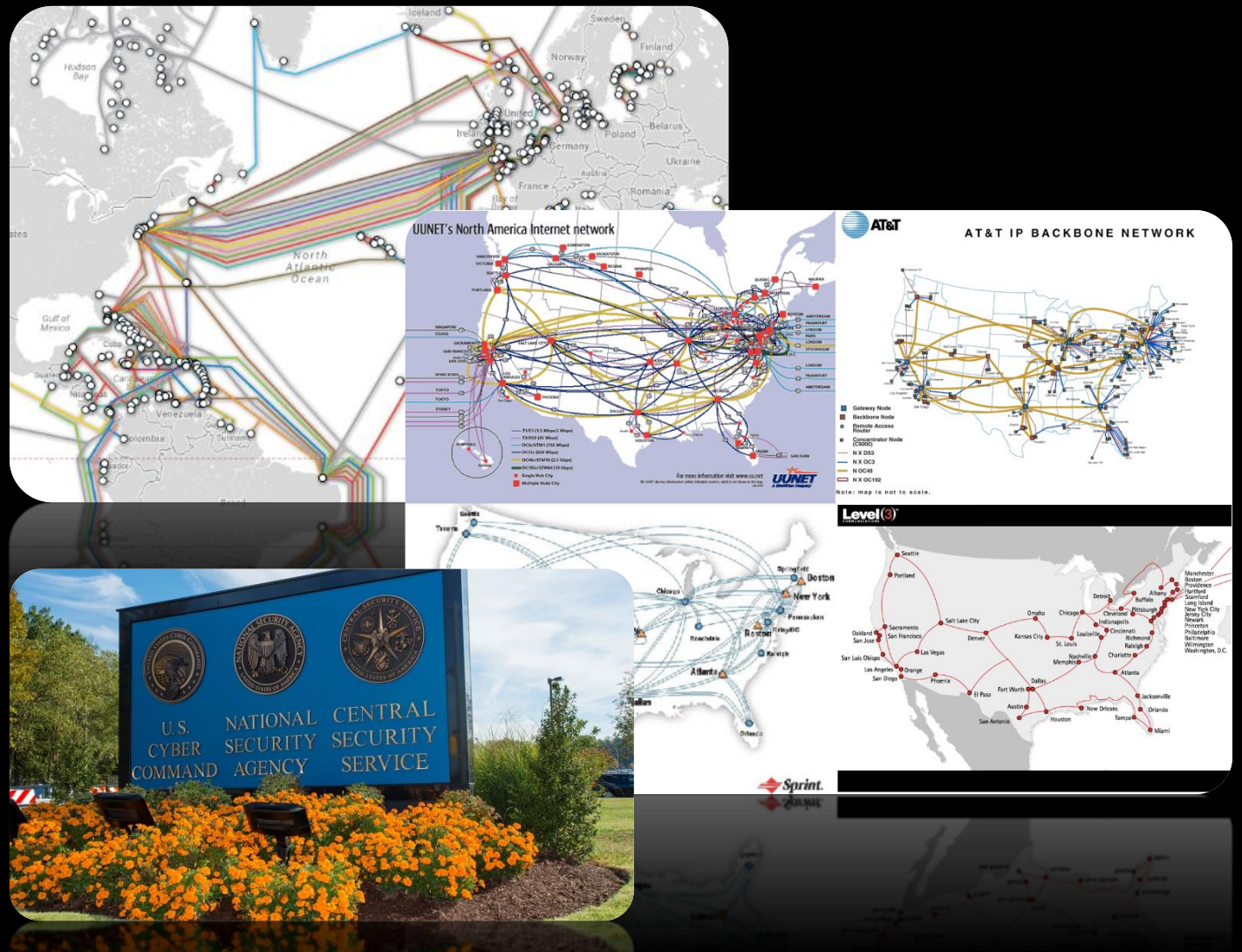
- Defend the nation from attack
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction



Coordinate with Public, Private, and International Partners

** Note: Nothing in this chart alters existing DOJ, DHS, and DoD roles, responsibilities, or authorities*

Why Can't the Government Just Do It?



1. Limited by geographic territory
2. Limited by control/ownership
   "98 percent of U.S. government communications, including classified communications, travel over civilian-owned-and-operated networks and systems."
   – C&C, pg 196
3. Limited by Purpose/Priority

What is the Private Sector's Role?

- Who are we talking about?
  - IT companies
    - ISPs
    - Cybersecurity companies
    - Facebook/Twitter etc?
  - Non-IT companies
    - Banking
    - Electricity
    - Other critical infrastructure sectors
- What Responsibility?
  - Product development
    - Make secure products
    - Make products to make insure things more secure
  - Information Sharing

Cyber Ops Legal and Authority Issues

Application and analysis of law and authorities to cyberspace operations is fact dependent

- Domestic and International Law apply to cyberspace operations
- The Law of Armed Conflict applies to cyberspace operations that rise to the level of an armed conflict
- The difficulty is in applying the law to new capabilities and factual situations

Must identify

- What is purpose of activity?
- What is the effect of the activity?
- Where will activity take place?
- Where will effects manifest?
- Will the activity be conducted with the consent of, or notice to, the relevant State(s)?