CYBER THREAT TO THE UNITED STATES

Homeland Security

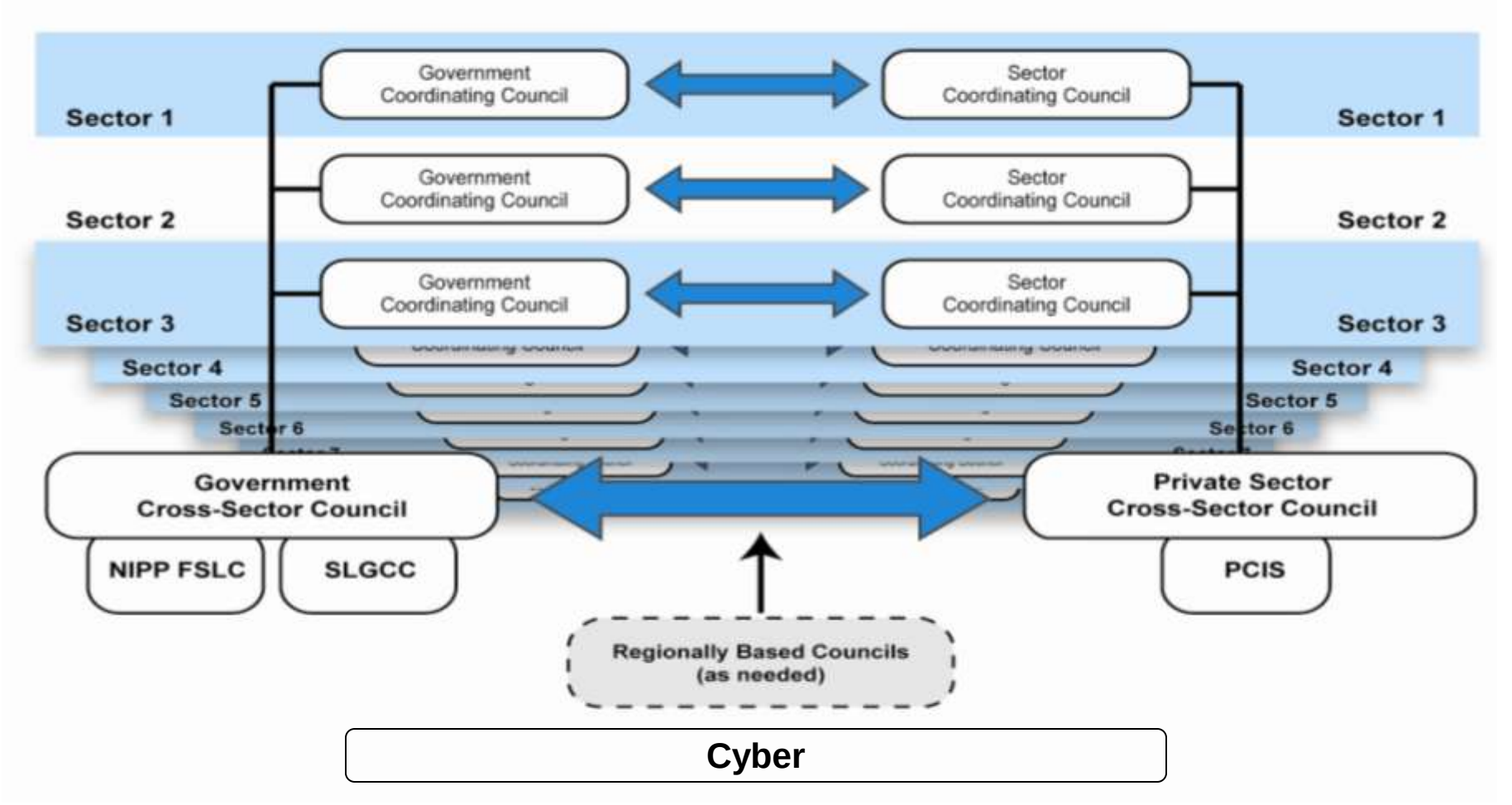
DHS Office of Intelligence and Analysis
Domestic Threat Analysis Division (DTA)
Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

Agenda

- **DHS organization: Cyber Threat Branch**
  - **Mission**
  - **Role**
  - **Responsibilities**
  - **Requirements**
  - **Focus areas**
- **The cyber threat environment**
- **Cyber threats to control systems**

U.S. Intelligence Community

DHS I&A and the Private Sector



DHS I&A will work to *understand and* to *assist* in the detection of and protection from adversary cyber threats to improve the integrity of the national information infrastructure.

Cyber Threat Branch Organization

Team E-mail:
cyber@hq.dhs.gov

DHS
Office of Intelligence and Analysis
Domestic Threat Analysis Division

Cyber Threat Branch
George Bamford
202-447-3129
george.bamford@dhs.gov

National Cybersecurity and Communications Integration Center Support

Strategic Analysis Section

Plans, Programs, and Mission Support Section

The Cyber Threat Branch mission is to identify, monitor, and evaluate cyber and other threats to information technology and telecommunication assets and to provide federal civilian government elements, state, local, and tribal authorities, and homeland critical infrastructure/key resources owners and operators with timely, accurate, and actionable intelligence they can use to protect their assets. The Cyber Threat Branch also serves as the DHS enterprise designee to Intelligence Community efforts related to the cyber domain.

Cyber Threat Branch Responsibilities

- **Execute the responsibilities created by the Homeland Security Act of 2002:**
  - Access, receive, and analyze law enforcement, intelligence, and other information from federal, state, and local agencies and private sector entities to:
    - Identify and assess the nature and scope of terrorist threats
    - Detect and identify threats to the United States
    - Understand threats in light of actual and potential vulnerabilities
  - Carry out comprehensive assessments to determine the risk posed by terrorist attacks
- **Outreach plays a critical role in the mission**
  - The CTB provides threat briefings and teleconferences to:
    - Sector Coordinating Councils
    - Government Coordinating Councils
    - Key industry associations
    - State and local officials, including fusion centers

The Cyber Threat Branch works closely with colleagues in the Critical Infrastructure Branch and HITRAC.

Cyber Threat Branch Requirements

Three primary mission requirements as outlined by HSPD-7, the Homeland Security Act of 2002, the Comprehensive National Cybersecurity Initiative, the National Infrastructure Protection Plan, and the I&A Strategic Plan:

- **Provide intelligence support for the DHS National Protection and Programs Directorate and the federal civilian domain.**
- **Provide intelligence analysis regarding cyber threats and threats to information technology and communication assets to homeland critical infrastructure/key resources owners and operators and federal, state, local, tribal, law enforcement, and private sector partners**
- **Serve as the DHS enterprise designee to Intelligence Community efforts related to the cyber domain:**
  - **National Cyber Study Group**
  - **National Intelligence Estimates**
  - **Intelligence Community Assessments**
  - **National Intelligence Priorities Framework**

Cyber Threat Branch Focus Areas

- Adversarial capabilities
- Industrial control systems
- Telecommunications
- Critical infrastructure and key resources
- Information technology
- Interdependencies

Remote Cyber Threats: Three Levels

Threat Level 1
"Garden Variety"

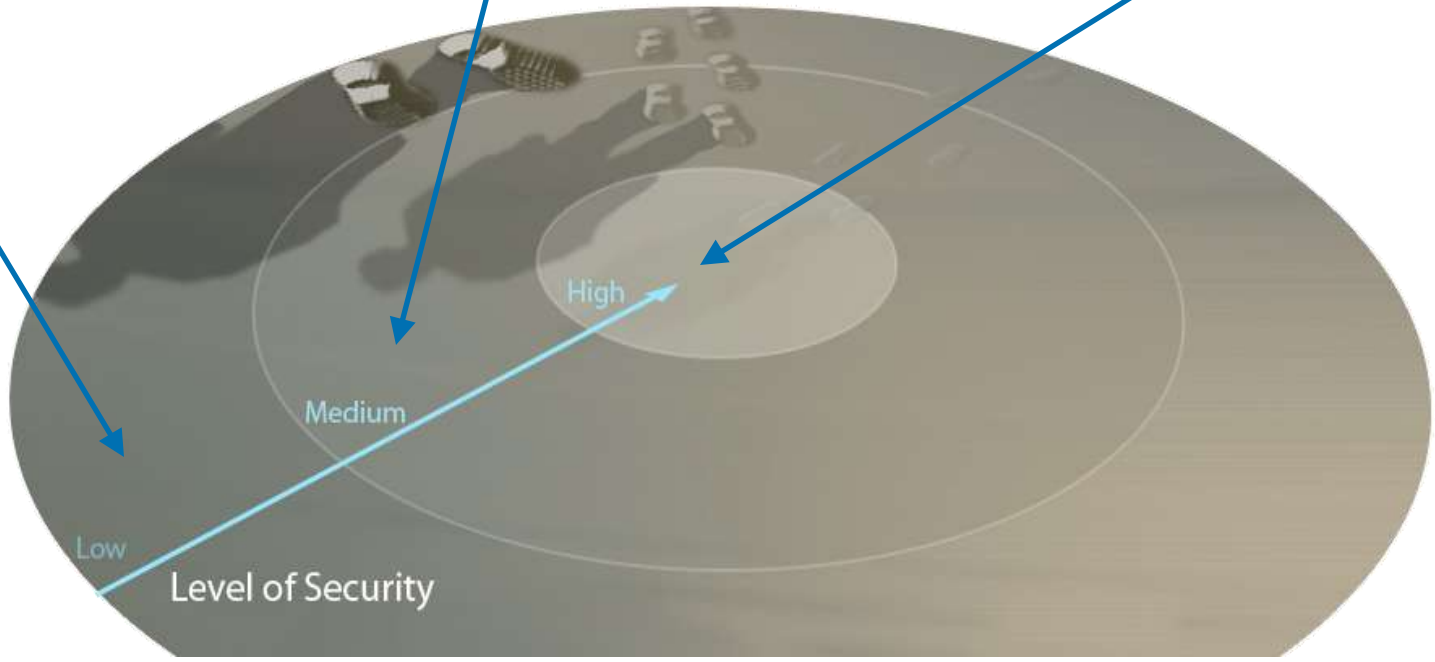
- Inexperienced
- Limited funding
- Opportunistic behavior
- Target known vulnerabilities
- Use viruses, worms, rudimentary trojans, bots
- Acting for thrills, bragging rights
- Easily detected

Threat Level 2
"Mercenary"

- Higher-order skills
- Well-financed
- Targeted activity
- Target known vulnerabilities
- Use viruses, worms, trojans, bots as means to introduce more sophisticated tools
- Target and exploit valuable data
- Detectable, but hard to attribute

Threat Level 3
"Nation State"

- Very sophisticated tradecraft
- Foreign intel agencies
- Very well financed
- Target technology as well as info
- Use wide range of tradecraft
- Establish covert presence on sensitive networks
- Difficult to detect
- Supply Interdiction/hardware implants



Adversarial Characterization

- We assess state and non-state threat actors have technical capabilities to target and disrupt elements of U.S. cyber infrastructure as well as collect intelligence
- Reporting indicates that violent Islamic extremist groups--al-Qa‘ida, Hamas, Hizballah--are acquiring better cyber skills
  - Cyberspace is used for propaganda, recruitment, training, fundraising, communications, and target reconnaissance
  - Highest levels of al-Qa‘ida leadership are aware of the West’s reliance on cyber capability and connectivity
  - Physical attacks remain the preferred method of terrorist attack
- Criminal elements continue to show growing sophistication in technical capability and targeting
  - Will offer illicit cyber capabilities and services to anyone willing to pay

The Cyber Threat Environment

- **Malicious cyber activity routinely is directed at the U.S. Government, private sector, and academia**
  - **Growing more sophisticated, targeted, and prevalent**
  - **Nature and source of the threat is diverse**
  - **Designed to**
    - **Exploit data gathered from information systems or networks (computer network exploitation)**
    - **Disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves (computer network attack)**
- **We have limited insight on intrusions into private sector networks, but are becoming more aware of U.S. information infrastructure vulnerabilities to cyber attacks**
  - **Key factors: dynamic business environment, reliance on open systems and COTS, management/enterprise networks' Internet connections**

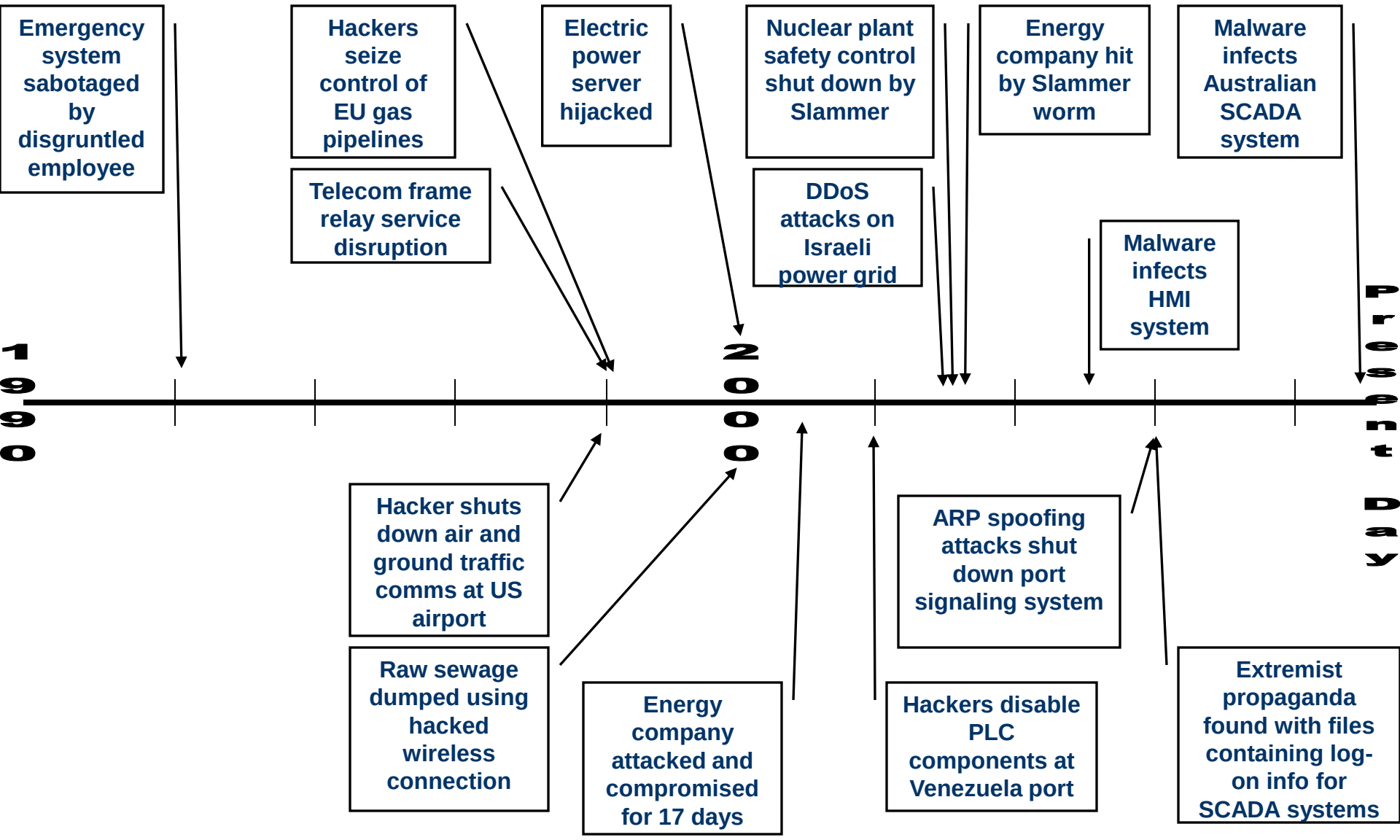
Commonality in Systems

- **Worldwide, power, chemical, water systems, and manufacturing companies have similar control systems**
- **Six vendors of process management systems are used in over 75 percent of U.S. domestic systems***
  - **This commonality in systems suggests that an adversary would not require a great deal of time to develop tools for new attacks or possibly could move rapidly from target to target**

These same vendors also supply systems overseas, allowing potential adversaries insights into U.S. process control systems

* Idaho National Engineering and Environmental Laboratory, *Review of Supervisory Control and Data Acquisition (SCADA) Systems*, January 2004.

Timeline of Worldwide SCADA Cyber Events



Cyber Threats – Control Systems

- The Intelligence Community has information from multiple regions outside the U.S. of cyber intrusions into utilities, followed by extortion demands
  - We suspect but cannot confirm that some of these attackers had the benefit of inside knowledge
- Separately, cyber attacks have been used to disrupt power equipment in several regions outside the U.S.
  - In at least one case the disruption caused a power outage affecting multiple cities
  - We do not know who executed these attacks or why, but all involved intrusions through the Internet
- The majority of control system networks are owned and operated by the private sector

The Evolving Control Systems Threat

- **Embedded Computing**
  - **Smart Grid Technology**
    - **IP-based networks leave door open to cyber attacks**
    - **Up to 17 million homes with smart meters installed in near term**
- **Wireless Technologies**
  - **Global Positioning System (GPS)**

1-Watt GPS Jammer

If a system is connected to the Internet or operating on a wireless frequency, it *can* and *will* be exploited.

GPS Timing and Synchronization Uses

- Global fiber networks
  - SDH, SONET
- Global wireless networks
  - PCS, GSM, TDMA, CDMA
- Transportation and public safety
  - National airspace system (VDL, NEXCOM, UAT)
  - Land, rail, marine
- GPS features
  - Low cost, high reliability and performance
  - Big asset for synchronization of digital networks
  - GPS (and Cesium, Loran-C) – Stratum 1

Intelligence Cycle