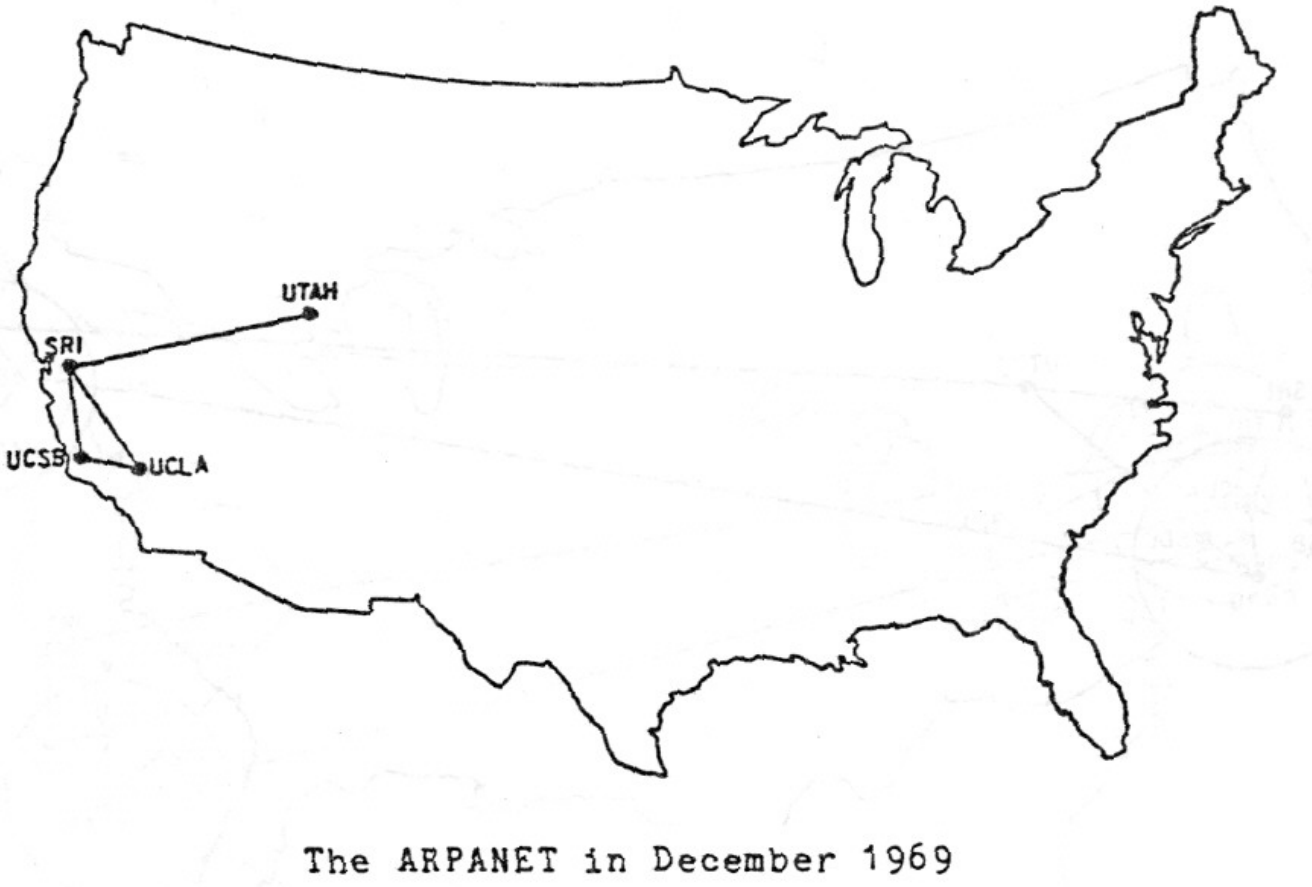
NEW YORK STATE BAR ASSOCIATION

Threats to Critical Infrastructure **Jay F. Kramer, Lewis Brisbois Bisgaard & Smith LLP**

Discussion Points and Goals

- Introduction and overview
- Critical infrastructure – definition
- Threat brief - what is motivating these attacks?
- Examples of infrastructure attacks
- Federal Government response
- Development of a national plan – the “NCIRP”
- NIAC guidance on protecting critical infrastructure
- *Self help*: how the NIST CSF and Critical Security Controls can reduce risk
- Questions

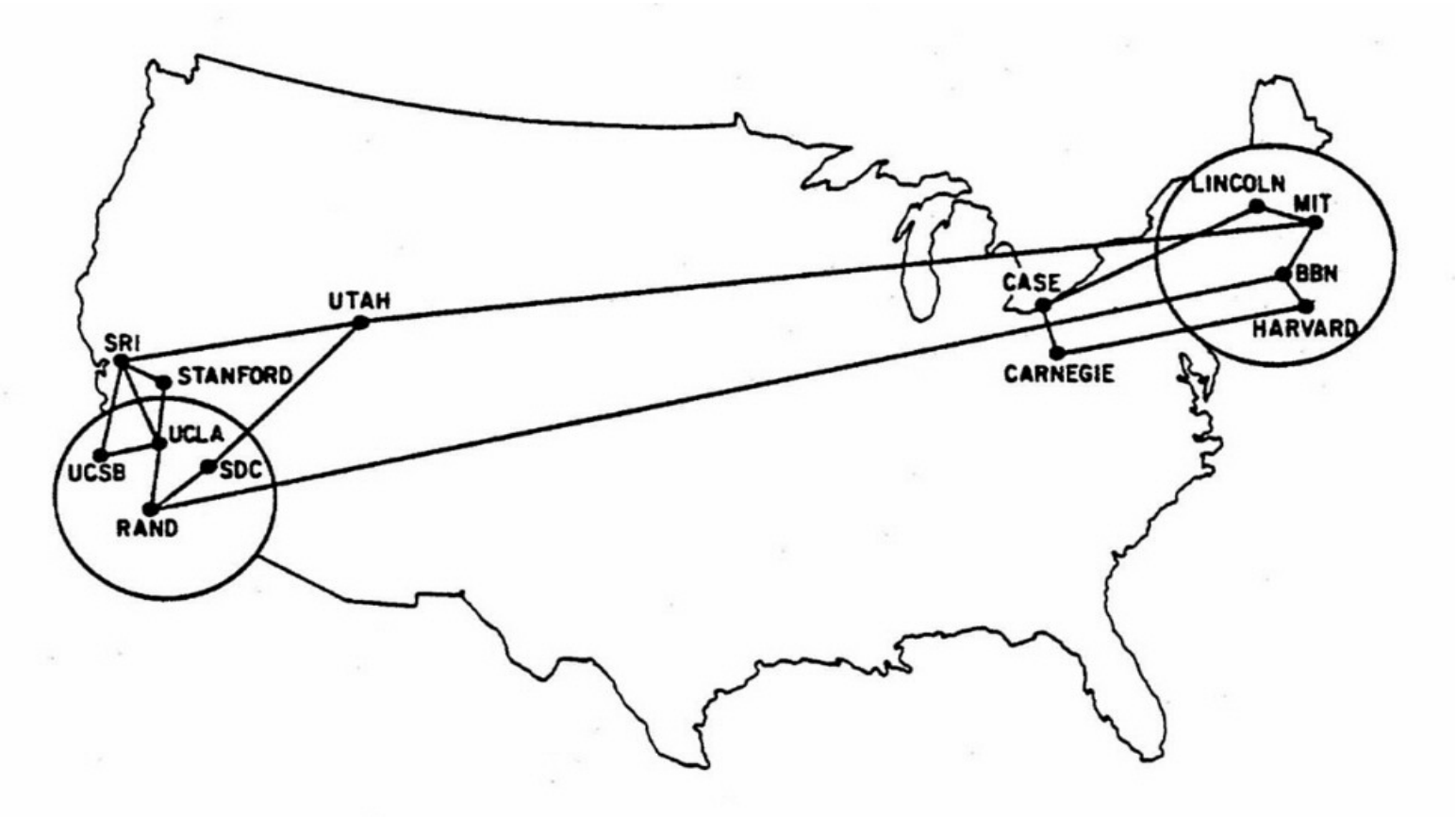
The Evolution of Internet Infrastructure



The ARPANET in December 1969

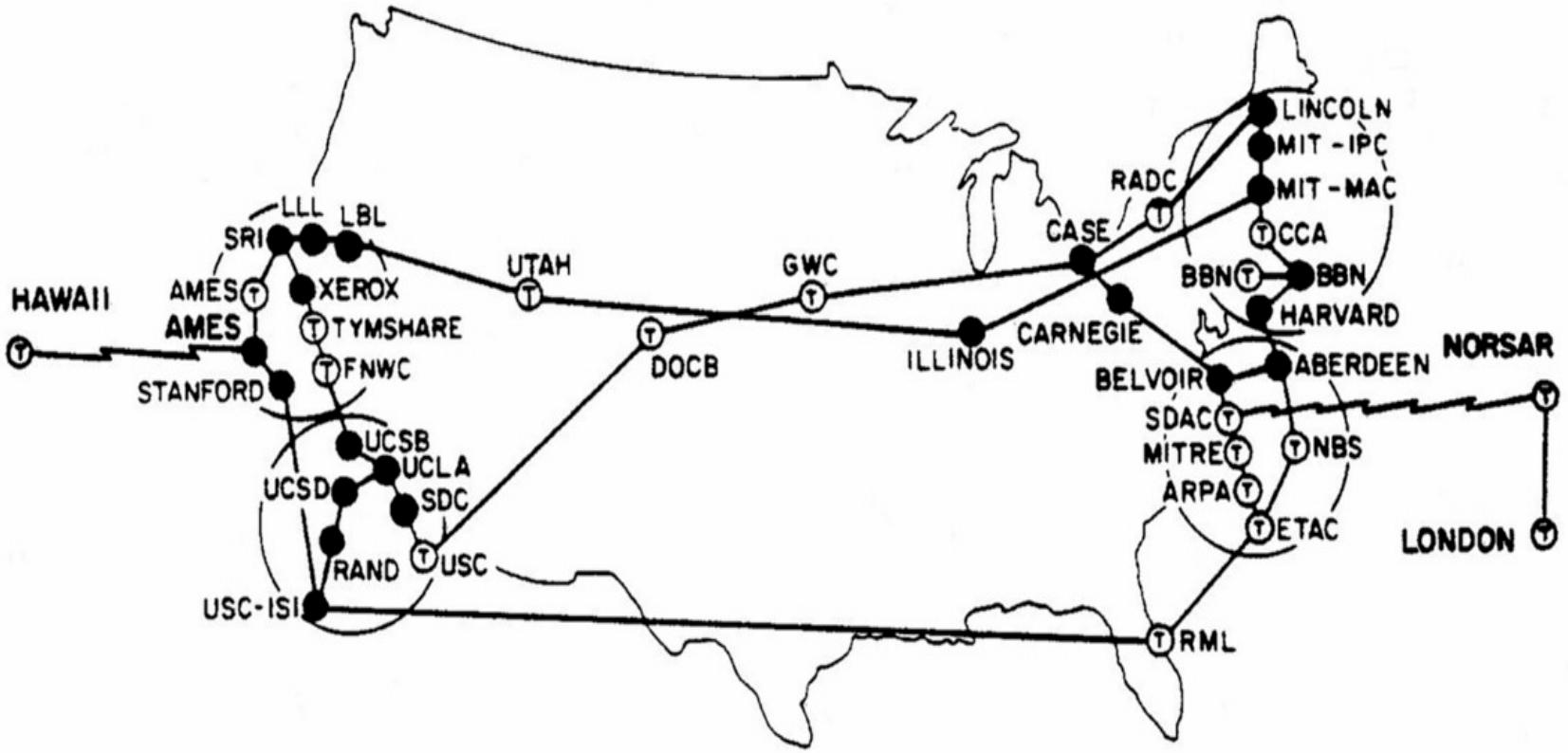
Source: vox.com

1970 – ARPANET



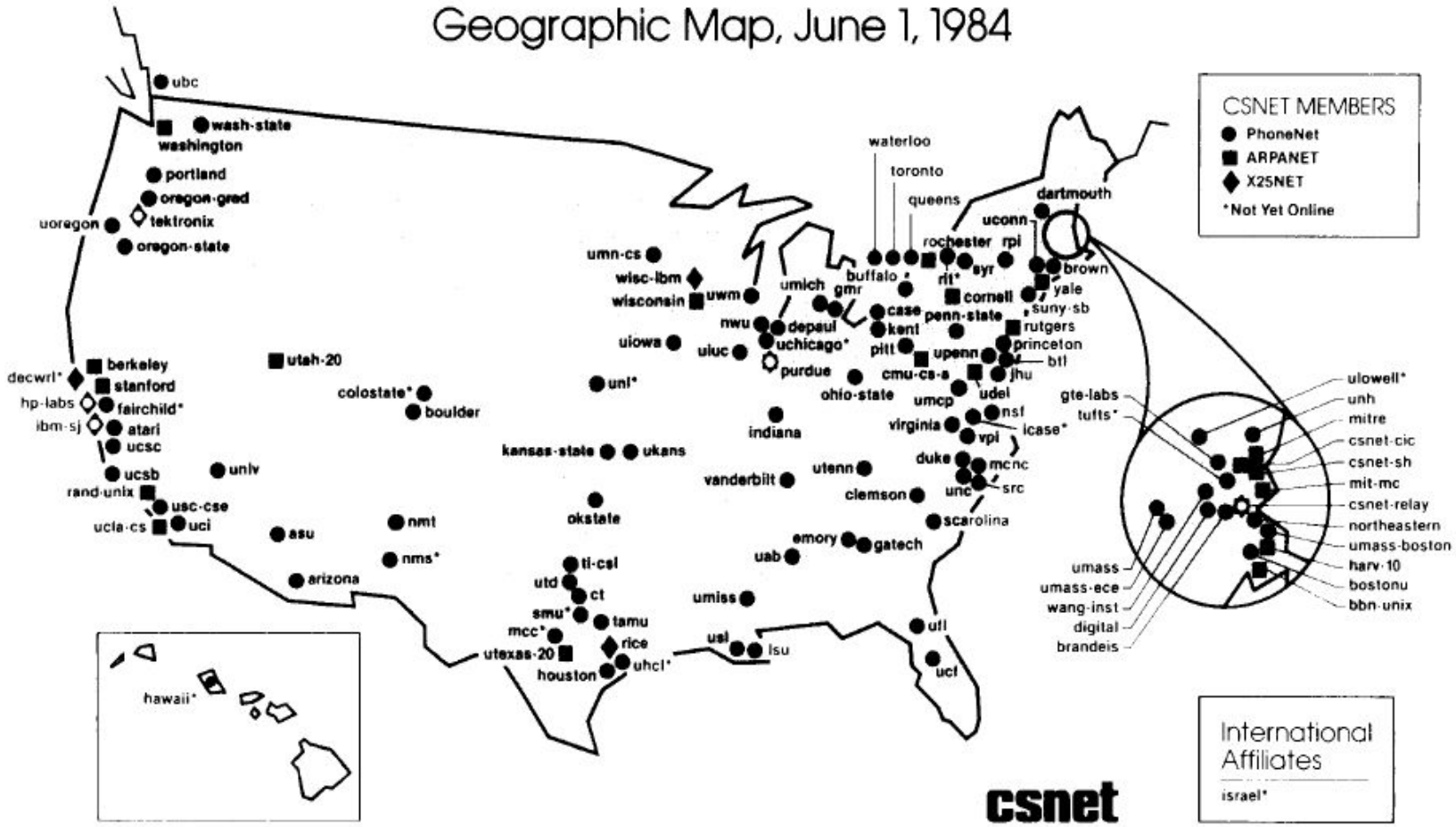
Source: vox.com

1973 – ARPANET



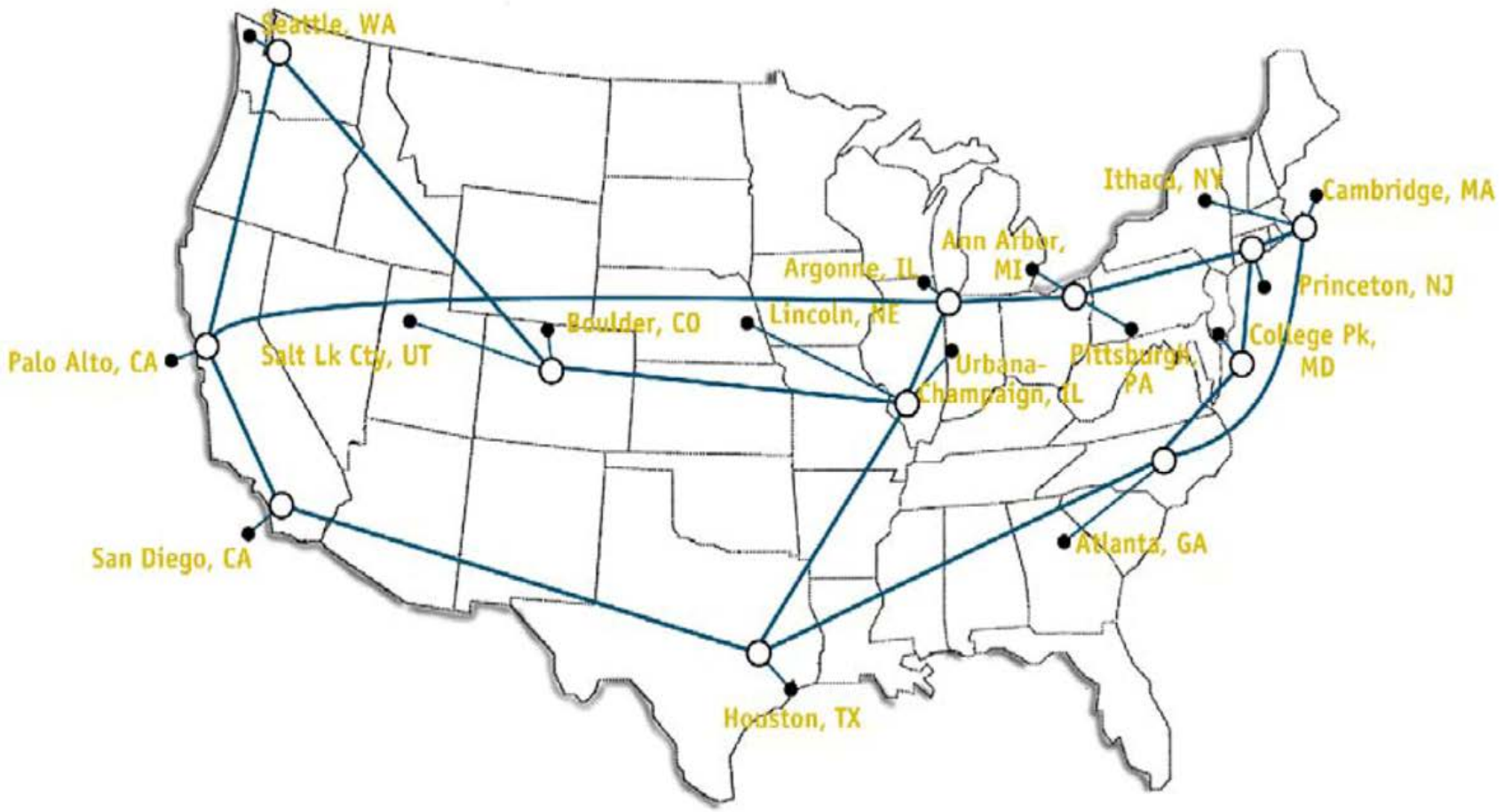
Source: vox.com

1984 – ARPANET BECOMES “INTERNET”



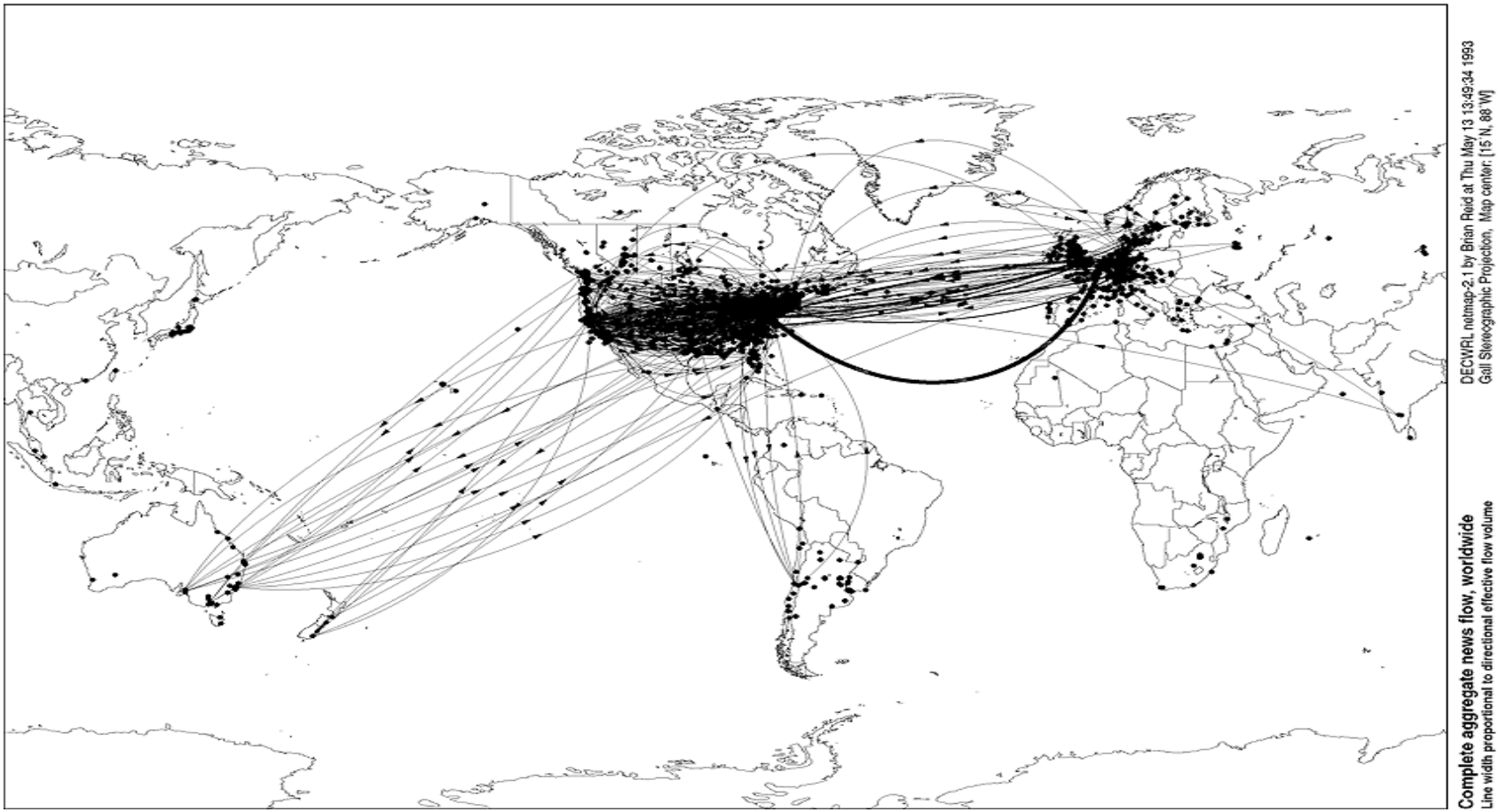
Source: vox.com

1986 – NSFNet BECOMES BACKBONE



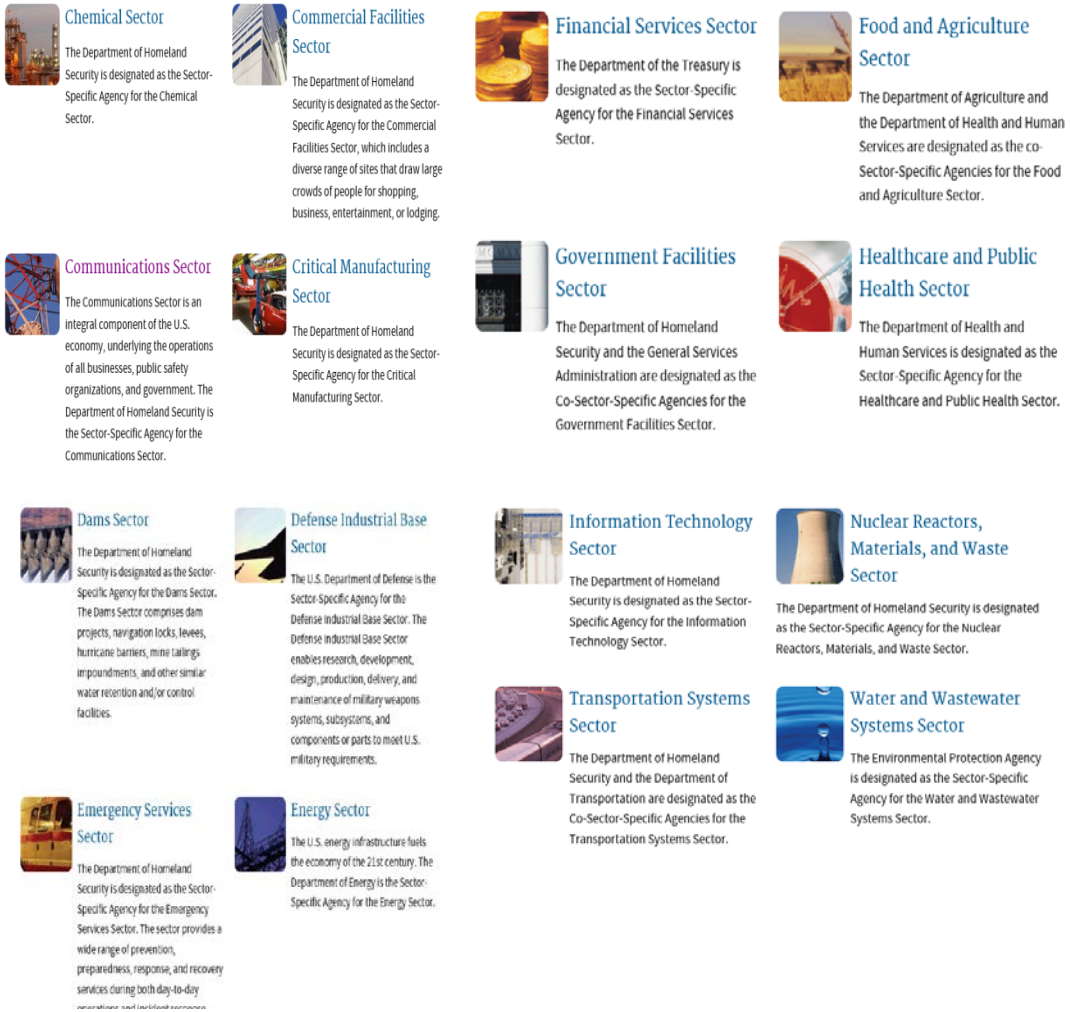
National Science Foundation T3 Network
Source: vox.com

1993 – internet goes global



Map of Usenet (online bulletin board), 1993
Source: vox.com

What is critical infrastructure?



Chemical Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Commercial Facilities Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector, which includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.

Financial Services Sector

The Department of the Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Food and Agriculture Sector

The Department of Agriculture and the Department of Health and Human Services are designated as the co-Sector-Specific Agencies for the Food and Agriculture Sector.

Communications Sector

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. The Department of Homeland Security is the Sector-Specific Agency for the Communications Sector.

Critical Manufacturing Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Government Facilities Sector

The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Healthcare and Public Health Sector

The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Dams Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Defense Industrial Base Sector

The U.S. Department of Defense is the Sector-Specific Agency for the Defense Industrial Base Sector. The Defense Industrial Base Sector enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.

Information Technology Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Nuclear Reactors, Materials, and Waste Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

Transportation Systems Sector

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Water and Wastewater Systems Sector

The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

Emergency Services Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day

Energy Sector

The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector-Specific Agency for the Energy Sector.

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Critical Infrastructure Information

How Does the PCII Program Support Infrastructure Protection?

What are the threats to critical infrastructure?

An integrated threat model

State-Sponsored Espionage

Foreign adversaries use cyber tools as part of traditional intelligence-gathering and espionage activities. These adversaries conduct computer network operations that target military and governmental organizations' intellectual property and insider information.

"Advanced Persistent Threat (APT)"

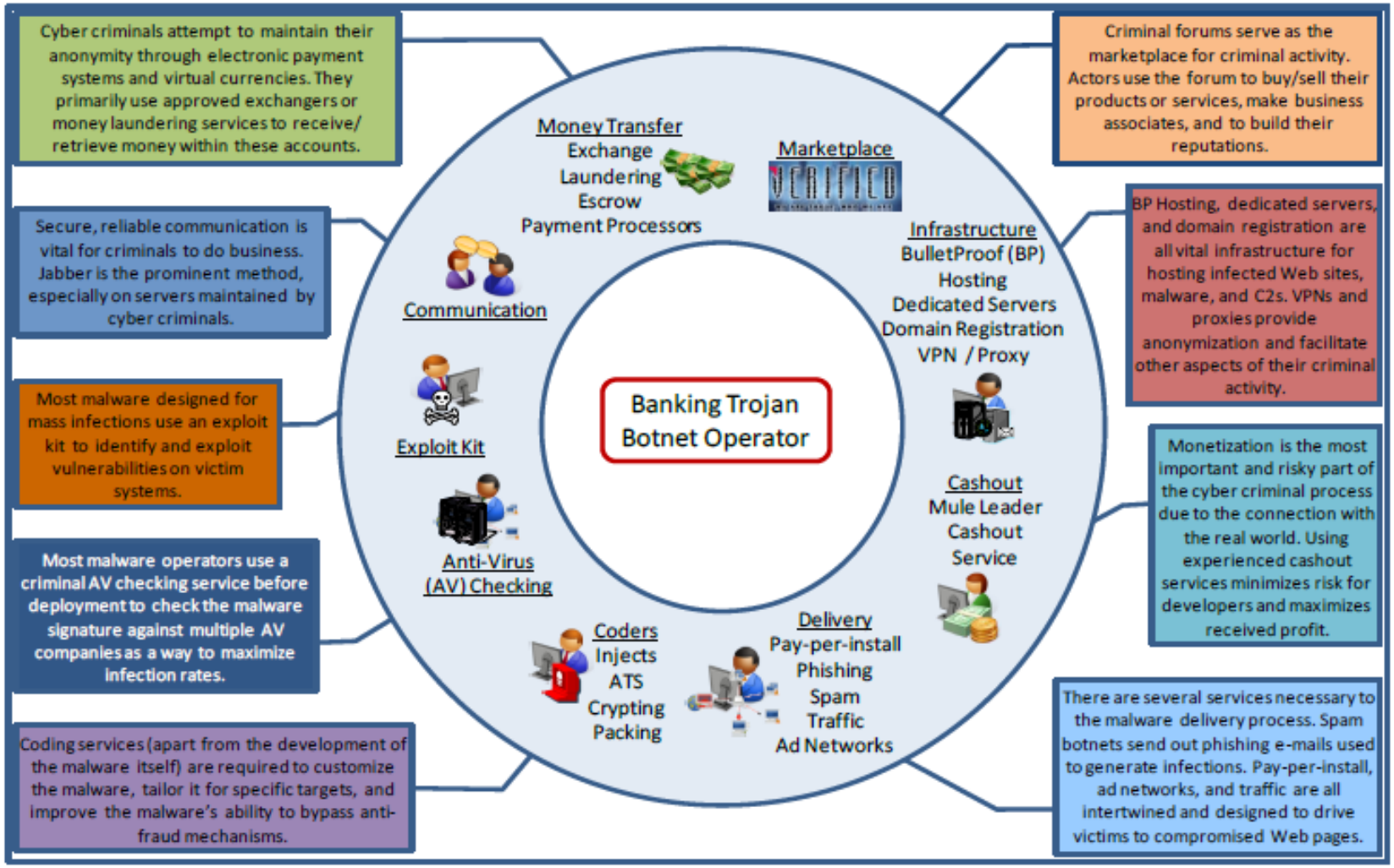
Industrial Espionage

Every year, billions of dollars are lost to foreign and domestic competitors who deliberately target economic intelligence in U.S. industries and technologies. Through cyber intrusions, these intruders search for intellectual property, prototypes, and company trade secrets to gain an illegitimate advantage in the market.

Hacktivists:
Anonymous and Splinter Groups

Financially motivated criminal actors

The Cyber Underground



FBI Cyber Division

An Internet *within* the Internet

Cyber Threats

Threat Actors

Cyber Attacks

- Unauthorized Access
- Theft of Data
- Destruction of Data
- Misappropriation or Misuse
- Unauthorized Disclosure, Disposal, Transmission
- Unauthorized Encryption of Data for Ransom
- Denial of Service
- Integrity Loss (Unauthorized Changes)
- Privilege/Access Escalation
- Impersonation

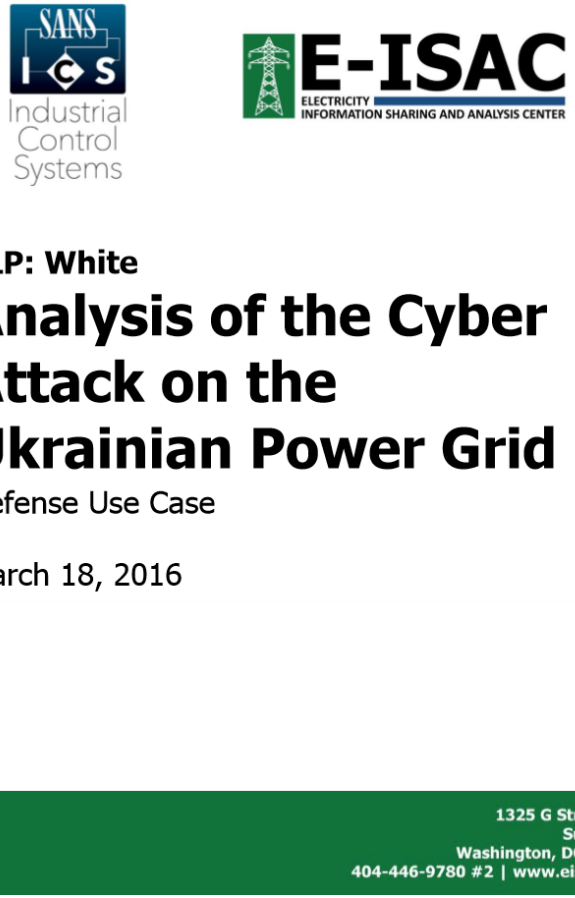
What's at risk?

- Service Delivery
- Infrastructure
- Sensitive Company Information
- Customer Service
- Personal Information

Examples of Recent Attacks in the Headlines

- **Equifax** – theft of credit records
- **WannaCry and Notpetya** – worldwide ransomware attack
- **Yahoo!** – theft of account information
- **Democratic National Committee** – sensitive emails
- **Ukraine Power Company** – blackout
- **Hollywood Presbyterian Medical Center** – ransomware
- **OPM** – theft of background check data
- **Sony** – destructive malware, theft of IP, PII and emails
- **Blue Cross Blue Shield** – theft of PII and PHI
- **Sands Casino** – destructive malware
- **JPMorgan Chase** – theft of financial account Information
- **Target** – theft of credit card data
- **Saudi Aramco** – destructive malware
- **Top 50 U.S. Banks** – denial of service attacks
- **Attacks on the legal sector** – insider trading, theft of IP

Attacks on the power grid - Ukraine



- December 23, 2015, the Ukrainian *Kyivoblenergo*, a regional electricity distribution company, reported service outages to customers.
- The outages were due to illegal entry into the company's computer and SCADA systems.
- **30 substations** were disconnected for three hours.
- It was revealed that three different distribution oblenergos suffered power outages that caused approximately 225,000 customers to lose power across various areas
- Ukrainian government officials claimed the outages were caused by Russian security services.

It’s déjà vu all over again…

MOTHERBOARD

RUSSIA | By Kim Zetter | Jan 10 2017, 3:07pm

The Ukrainian Power Grid Was Hacked Again

Experts say the country appears to be a “testbed” for cyber attacks that could be used around the world.

- December 17, 2016
- Ukraine's state-owned national power company *Ukrenergo* experienced an outage at an electrical substation in Kyiv.
- Researchers have subsequently confirmed that the outage was the result of a protracted campaign that began December 6 and lasted through December 20.
- This campaign included remote access and denial-of-service attacks against systems belonging to the transportation, energy, and government sectors in Ukraine.

JPMorgan fell victim to the largest theft of customer data from a financial institution in US history

Portia Crowe Nov. 10, 2015, 10:12 AM

The US Attorney for the Southern District of New York, Preet Bharara, has charged three people in connection to "the largest theft of customer data from a U.S. financial institution in history."

JPMorgan Chase CEO Jamie Dimon.
Thomson Reuters

One of the victims is JPMorgan Chase, which suffered a 2014 data breach.

Gery Shalon, Joshua Samuel Aaron, and Ziv Orenstein were charged in a 23-count indictment related to the computer hacking of several financial institutions and financial news publishers.

They are accused of stealing the personal information of over 100 million customers, according to the indictment.

The New York Times

3 Men Made Millions by Hacking Merger Lawyers, U.S. Says

Preet Bharara, the United States attorney in Manhattan. Andrew Kelly/Reuters

Federal prosecutors in Manhattan have charged three Chinese citizens with making more than $4 million by **trading on information** they got by hacking into some of the top merger-advising law firms in New York.
The three men targeted at least **seven New York law firms** to try to obtain information about deals in the works, according to an indictment unsealed on Tuesday.

The New York Times

U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam

Cyberattackers attempted to gain control of the Bowman Dam in Rye, a suburb of New York, in 2013. The effort failed, but worried American investigators because it was aimed at seizing a piece of infrastructure.
Christopher Capozziello for The New York Times

By David E. Sanger

The New York Times

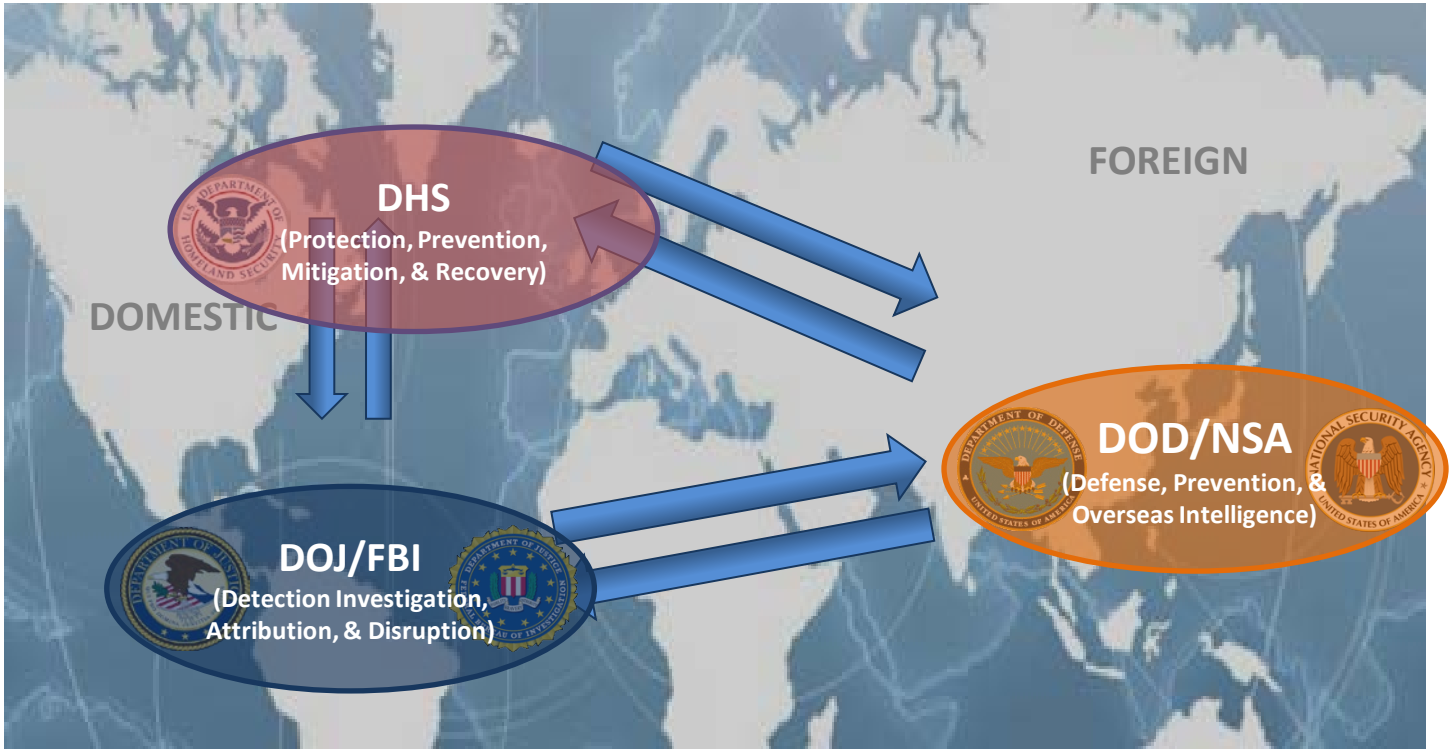
A Cyberattack Hobbles Atlanta, and Security Experts Shudder

By Alan Blinder and Nicole Perlroth

March 27, 2018

ATLANTA — The City of Atlanta's 8,000 employees got the word on Tuesday that they had been waiting for: It was O.K. to turn their computers on.

What is the USG strategy?



FBI Cyber Priorities

To protect the United States against:

- Terrorist attack
- Foreign intelligence operations and espionage
- Cyber-based attacks and high technology crimes

*As the only U.S. agency with the authority to investigate **both criminal** and **national security** cybersecurity threats, the FBI is following a number of emerging trends.*

FBI Cyber Presence – US and Worldwide

- FBI Operates 56 Field Offices in U.S., plus “RAs”
- LEGAT offices in 87 locations
- In 2010, FBI Cyber Division instituted Cyber ALAT Program

Cyber ALATs

- FBI Operates LEGAT offices in 87 locations
- In 2010, FBI Cyber Division instituted Cyber ALAT Program
  - Embed ALATs with host nation counterparts
    - Bucharest, Romania
    - Kyiv, Ukraine
    - Riga, Latvia
    - Tallinn, Estonia
    - The Hague, Netherlands

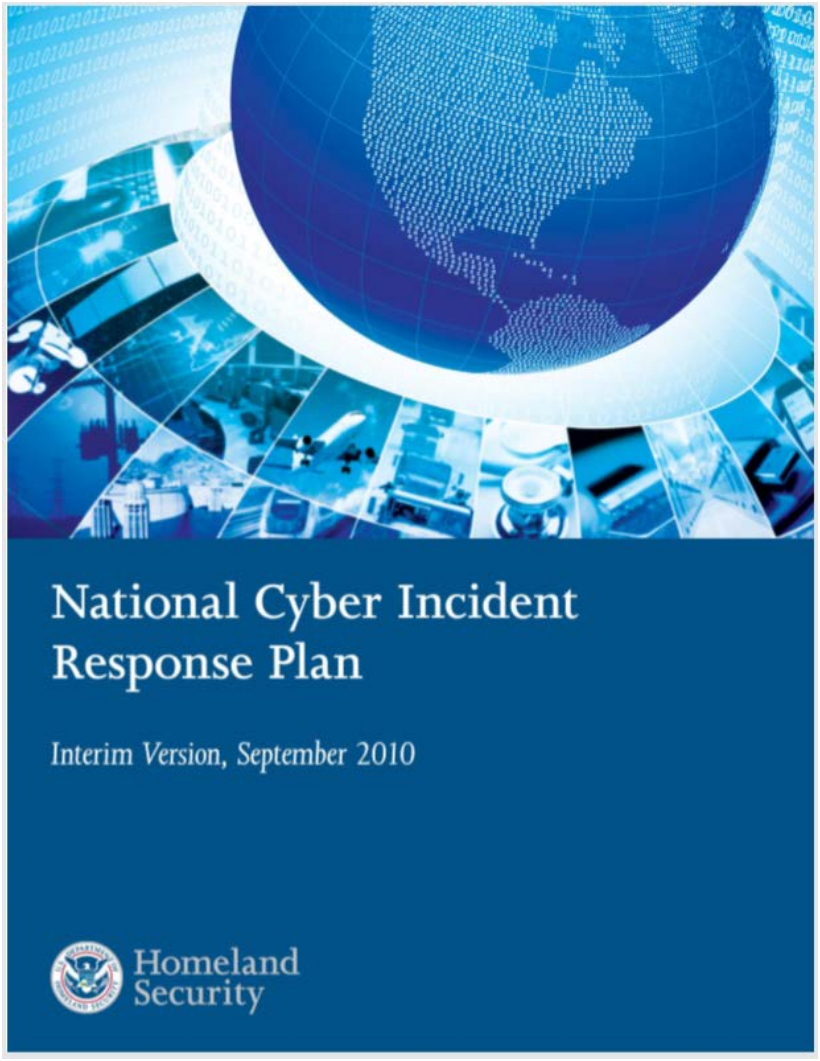
United States Secret Service

- Evolution of the Electronic Crimes Task Force (ECTF)
- Field Offices/ECTF locations nationwide

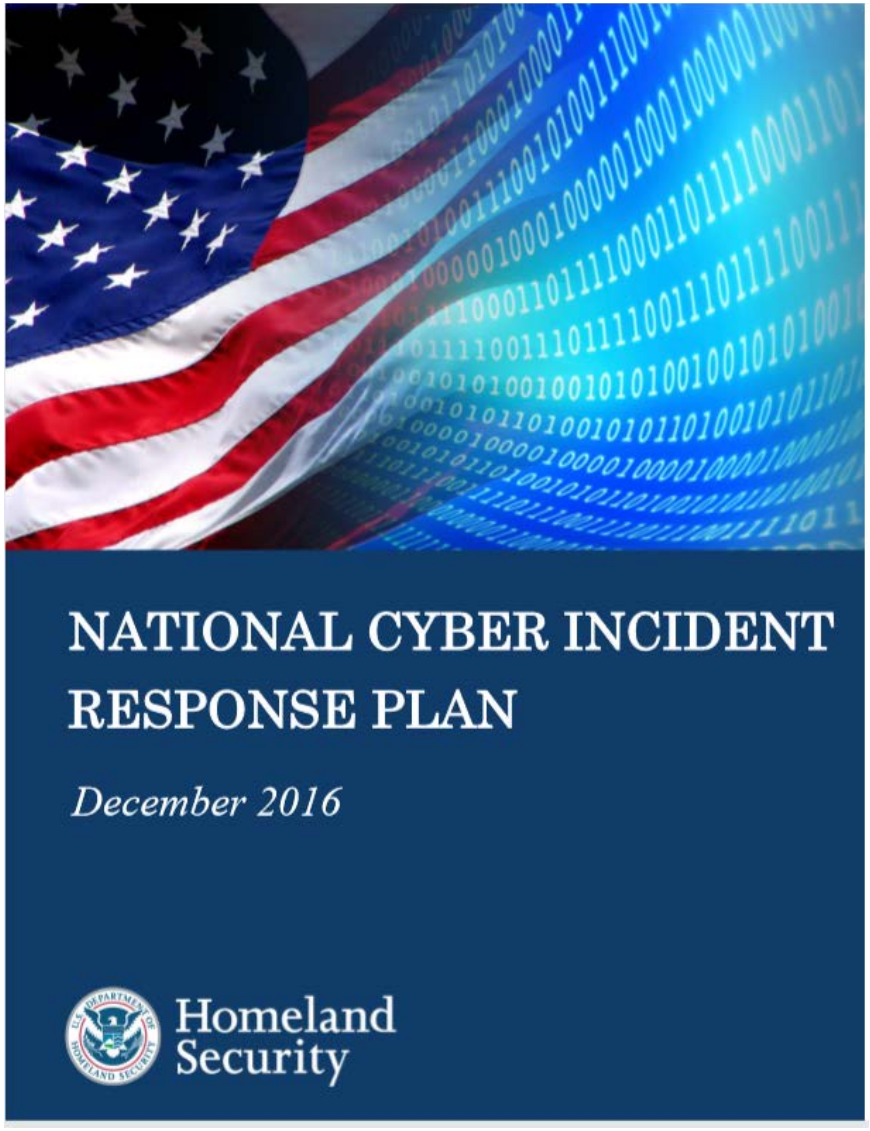
Development of a national plan
The National Cyber Incident Response Plan

National Cyber Incident Response Plan 2.0
Kick-Off
June 13, 2016

NCIRP replaces prior “interim” plan



December 2016 – NCIRP approved



Three lines of effort during a critical incident

Threat Response

As the lead Federal agency for threat response during a significant cyber event, DOJ, through the FBI, will coordinate with the DHS as the lead Federal asset response agency, and with the Office of the Director of National Intelligence (ODNI), through its National Cybersecurity and Communications Integration Center (NCCIC), as the lead Federal intelligence support agency.

Asset Response

DHS

Responsible for coordinating and developing response tasks; communicating with the affected entity to understand the nature of the incident; coordinating consistent, accurate, and appropriate communications regarding the incident to affected parties and stakeholders, including the public; to facilitate affected entity and asset response efforts to effectuate response and recovery from a significant cyber incident.

Intelligence Support and Related Activities

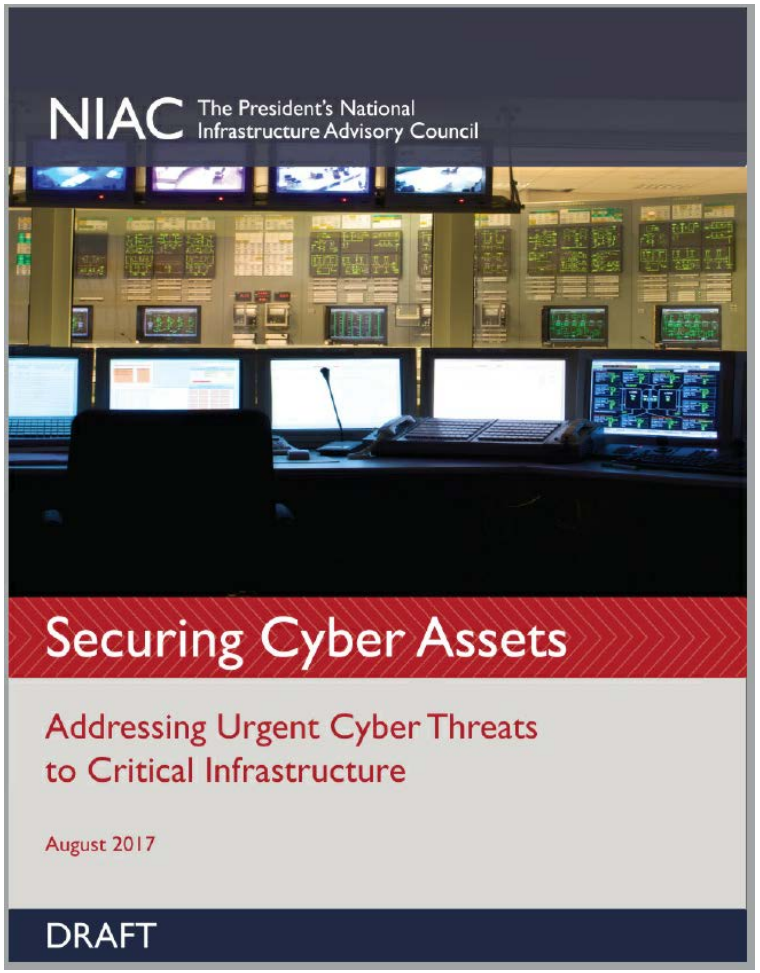
The Director of National Intelligence serves as the head of the Intelligence Community, acts as the principal advisor to the President for intelligence matters relating to national security, The Intelligence Community, comprising 17 elements across the Federal government will respond.

NCIRP "2.0"

National Cyber Incident Response Plan

Table of Contents

The President's National Infrastructure Advisory Council (NIAC)



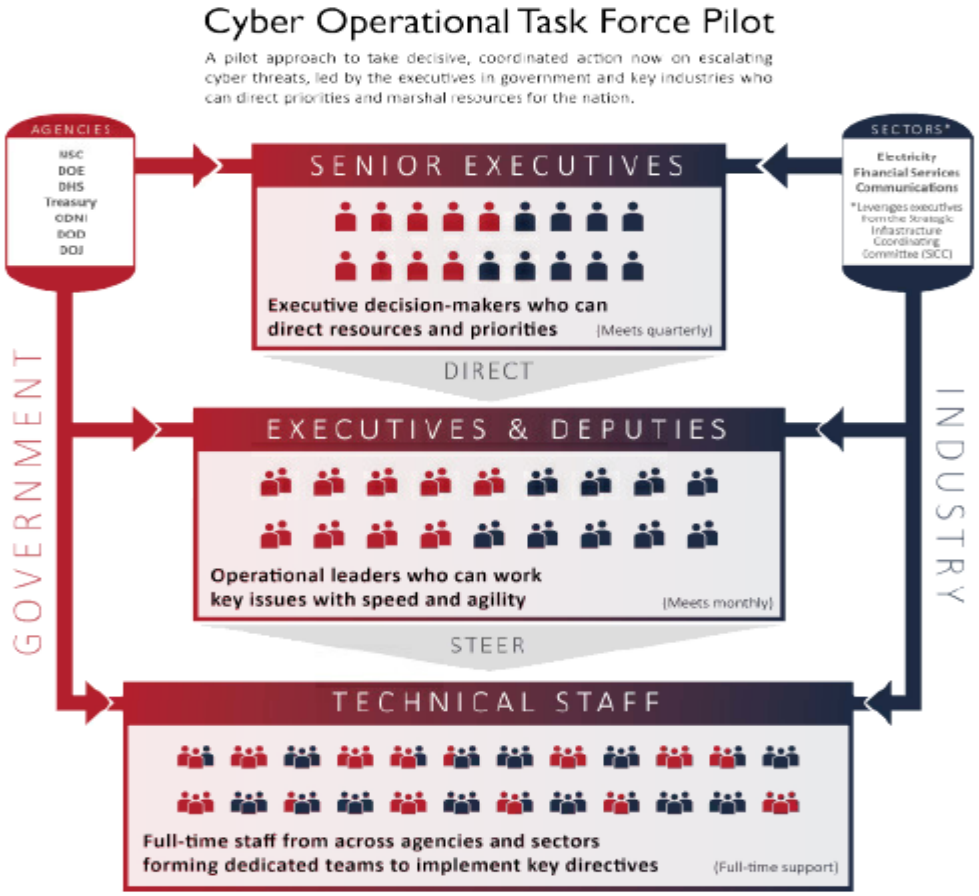
The President's National Infrastructure Advisory Council (NIAC) is composed of senior executives from industry and State and local government who own and operate the critical infrastructure essential to modern life.

The Council was established by executive order in October 2001 to advise the President on practical strategies for industry and government to reduce complex risks to the designated critical infrastructure sectors.

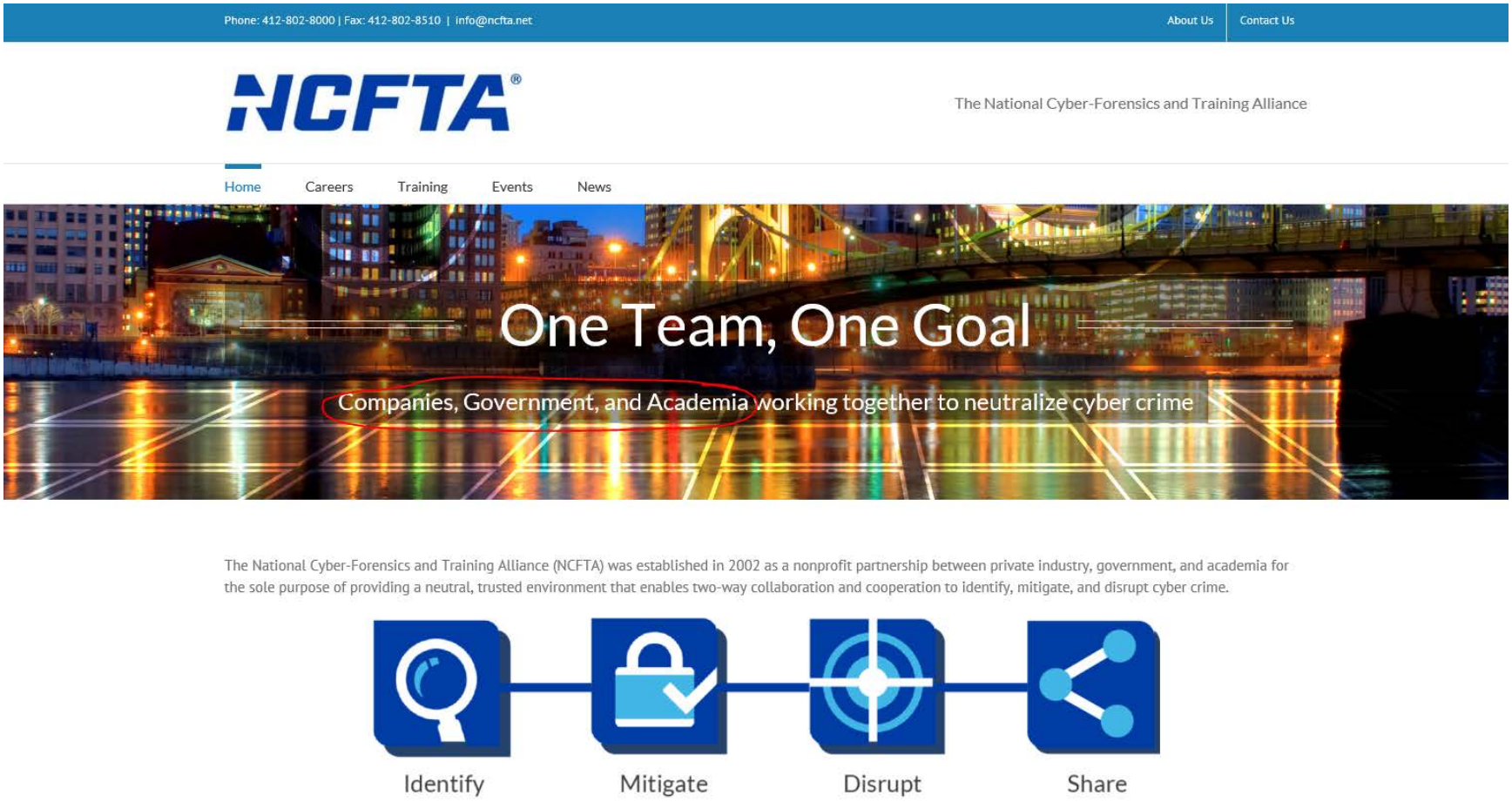
NIAC - Executive Summary: 11 Key Takeaways

1. Establish **SEPARATE, SECURE COMMUNICATIONS NETWORKS** specifically designated for the most **critical cyber networks,** including "dark fiber" networks for critical control system traffic and reserved spectrum for backup communications during emergencies.
2. FACILITATE A **PRIVATE-SECTOR-LED PILOT OF MACHINE-TO-MACHINE INFORMATION SHARING TECHNOLOGIES**, led by the Electricity and Financial Services Sectors, to test public-private and company-to-company information sharing of cyber threats at network speed.
3. Identify best-in-class **SCANNING TOOLS AND ASSESSMENT PRACTICES**, and work with owners and operators of the most critical networks to scan and sanitize their systems on a voluntary basis.
4. Strengthen the capabilities of **TODAY'S CYBER WORKFORCE** by sponsoring a public-private expert exchange program.
5. Establish a set of **LIMITED TIME, OUTCOME-BASED MARKET INCENTIVES** that encourage owners and operators to upgrade cyber infrastructure, invest in state-of-the-art technologies, and meet industry standards or best practices.
6. Streamline and significantly expedite the **SECURITY CLEARANCE PROCESS** for owners of the nation's most critical cyber assets, and expedite the siting, availability, and access of Sensitive Compartmented Information Facilities (SCIFs) to ensure cleared owners and operators can access secure facilities within one hour of a major threat or incident.
7. Establish clear protocols to **RAPIDLY DECLASSIFY CYBER THREAT INFORMATION** and proactively share it with owners and operators of critical infrastructure, whose actions may provide the nation's front line of defense against major cyber attacks.
8. **PILOT AN OPERATIONAL TASK FORCE OF EXPERTS IN GOVERNMENT AND THE ELECTRICITY, FINANCE, AND COMMUNICATIONS INDUSTRIES**— led by the executives who can direct priorities and marshal resources—to take decisive action on the nation's top cyber needs with the speed and agility required by escalating cyber threats.
9. **USE THE NATIONAL-LEVEL GRIDEX IV EXERCISE (NOVEMBER 2017) TO TEST** the detailed execution of Federal authorities and capabilities during a cyber incident, and identify and assign agency-specific recommendations to coordinate and clarify the Federal Government's unclear response actions.
10. Establish an **OPTIMUM CYBERSECURITY GOVERNANCE APPROACH** to direct and coordinate the cyber defense of the nation, aligning resources and marshaling expertise from across Federal agencies.
11. Task the National Security Advisor to review the recommendations included in this report and within six months **CONVENE A MEETING OF SENIOR GOVERNMENT OFFICIALS** to address barriers to implementation and identify immediate next steps to move forward.

8. Public-private task force model – theoretical?



NCFTA – a Public-Private Partnership



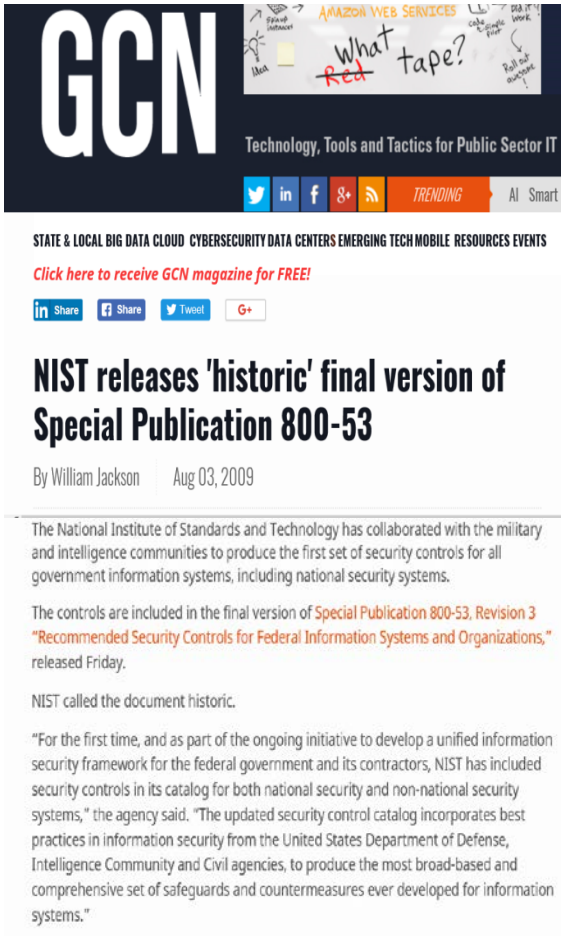
Problem: “The Fog of More”

The Council on Cybersecurity 2014 Annual Report coined the term: “Fog of More.”

It describes the “Overload of defensive support…more options, more tools, more knowledge, more advice, and more requirements, but not always more security.”

SP 800-53, Rev. 3 "Recommended Security Controls for Federal Information Systems and Organizations, August 2009

- "For the first time…NIST has included security controls in its catalog for both national security and non-national security systems."



GCN

Technology, Tools and Tactics for Public Sector IT

STATE & LOCAL BIG DATA CLOUD CYBERSECURITY DATA CENTERS EMERGING TECH MOBILE RESOURCES EVENTS

Click here to receive GCN magazine for FREE!

Share Share Tweet G+

NIST releases 'historic' final version of Special Publication 800-53

By William Jackson Aug 03, 2009

The National Institute of Standards and Technology has collaborated with the military and intelligence communities to produce the first set of security controls for all government information systems, including national security systems.

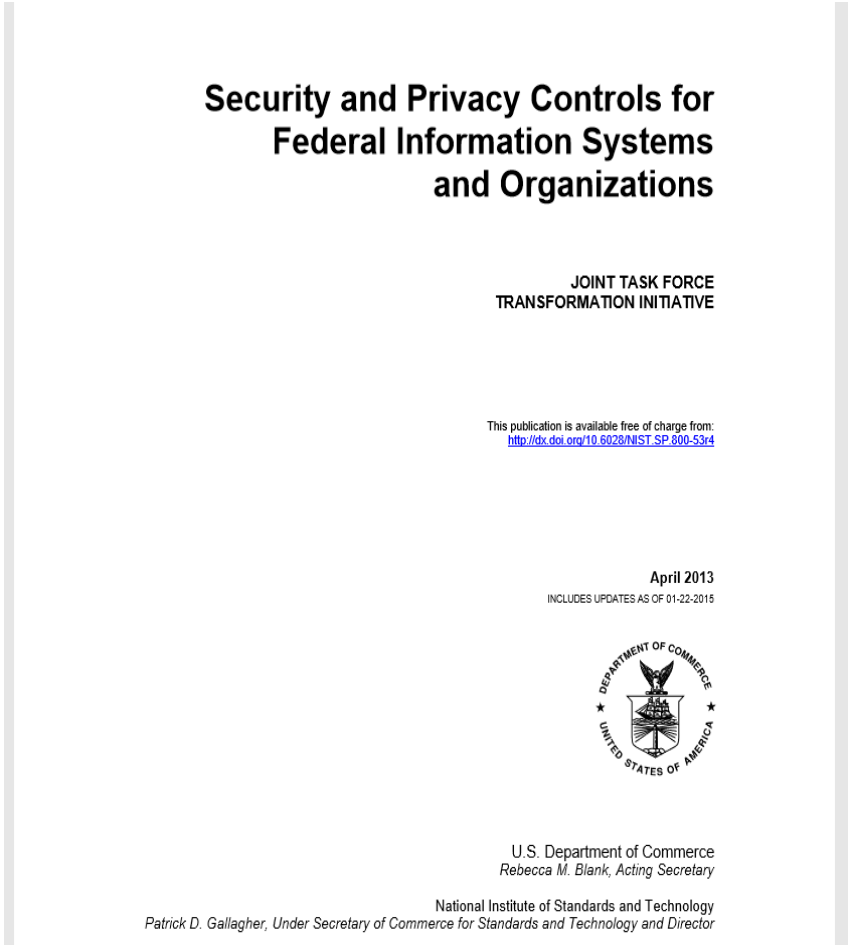
The controls are included in the final version of Special Publication 800-53, Revision 3 "Recommended Security Controls for Federal Information Systems and Organizations," released Friday.

NIST called the document historic.

"For the first time, and as part of the ongoing initiative to develop a unified information security framework for the federal government and its contractors, NIST has included security controls in its catalog for both national security and non-national security systems," the agency said. "The updated security control catalog incorporates best practices in information security from the United States Department of Defense, Intelligence Community and Civil agencies, to produce the most broad-based and comprehensive set of safeguards and countermeasures ever developed for information systems."

"NIST called the document historic. - April 3, 2009"

NIST SP 800-53 & the NIST Cybersecurity Framework (CSF)



Security and Privacy Controls for Federal Information Systems and Organizations

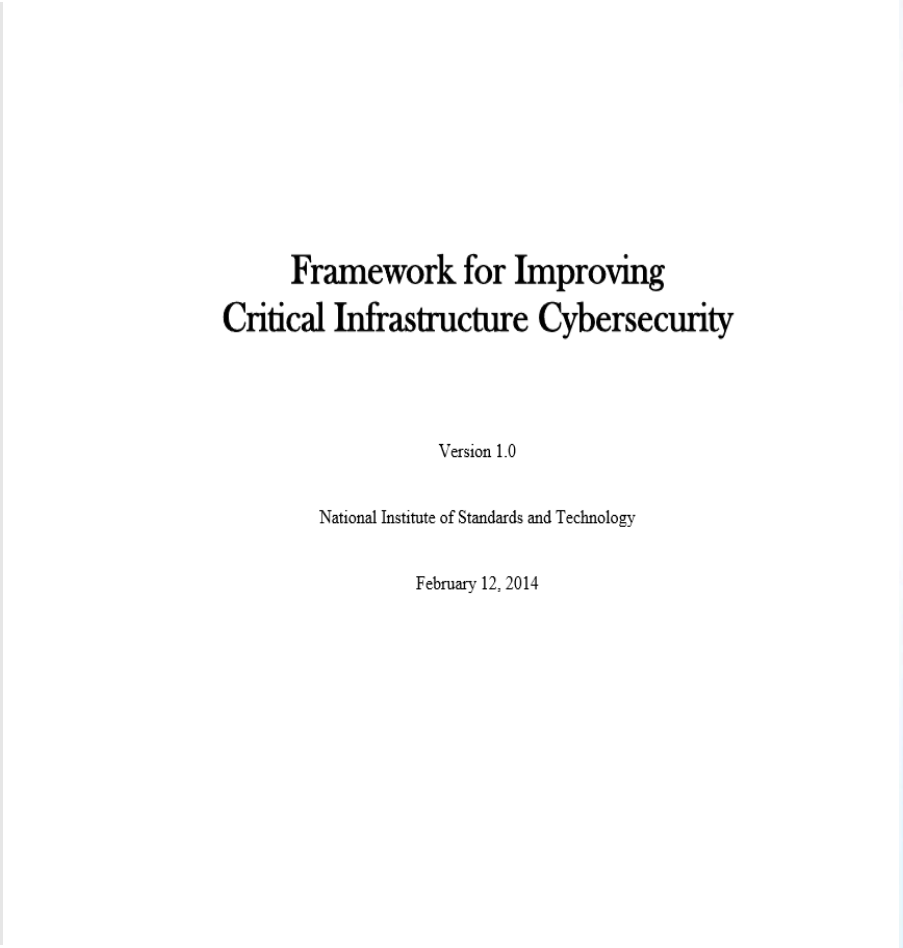
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

April 2013
INCLUDES UPDATES AS OF 01-22-2015

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director



Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

The NIST Cybersecurity Framework & Critical Security Controls

- What is the CSF and how can it help?

This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

NIST is finalizing an update to the Framework.

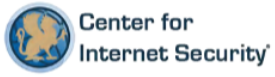
The Center for Internet Security's 20 Critical Security Controls (Formerly the SANS Top 20)

The CIS Critical Security Controls

for

Effective Cyber Defense

Version 6.1



The CIS (formerly SANS) Top 20

Review of Fundamentals

Good cyber hygiene will *significantly* reduce risk!

1. Hardware – Maintain an Inventory and Control of Authorized and Unauthorized Devices

2. Software – Maintain an Inventory and Control of Authorized and Unauthorized Software Programs

3. Vulnerability – Identify Vulnerabilities and Remediate to Minimize Opportunities for Attackers

4. Admin Privileges – Track, Control and Ensure the Proper Use of Administrative Privileges

5. Configurations – Implement and Manage the Security Configurations of Devices To Prevent Exploits

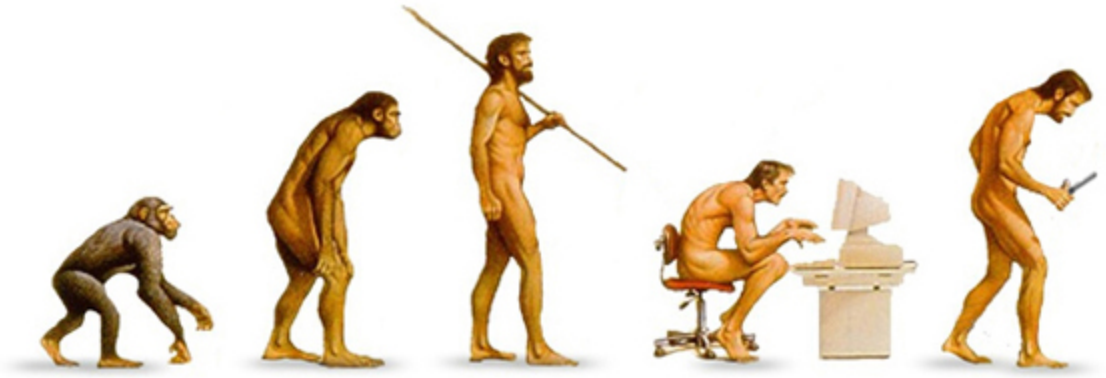
Other Law enforcement resources

- Threat Intelligence (For free!)
- PIN – Private Industry Notifications
- FLASH – FBI Liaison Alert System
- Value-added Incident Response

Information Sharing Opportunities

- DHS
  - Automated Indicator Sharing
  - National Cybersecurity and Communications Integration Center (NCCIC)
  - Cybersecurity Information Sharing and Collaboration Program (CISCP)
  - SAFETY Act Certification
- FBI
  - Cyber Division & FBI Field Offices
  - National Cyber Investigative Joint Task Force
  - Domestic Security Alliance Council
  - InfraGard
  - Investigative Tools – Parallax, Archer, Others
- DOE CRISP - Versions 1.0, 2.0
- ISACs and ISAOs
- Information Sharing Companies, e.g. IronNet

Perspectives on the future



Questions?

Jay Kramer
Partner, Data Privacy & Cybersecurity
Lewis Brisbois, New York
jay.kramer@lewisbrisbois.com
347.300.5120

LEWIS BRISBOIS

LEWIS BRISBOIS LOCATIONS NATIONWIDE

Albuquerque, NM
T: 505.828.3600 | F: 505.828.3900

Atlanta, GA
T: 404.348.8585 | F: 404.467.8845

Baltimore, MD
T: 410.525.6400 | F: 410.779.3910

Boston, MA
T: 857.313.3950 | F: 857.313.3951

Charleston, WV
T: 304.553.0166 | F: 304.343.1805

Chicago, IL
T: 312.345.1718 | F: 312.345.1778

Cleveland, OH
T: 216.344.9422 | F: 216.344.9421

Colorado Springs, CO
T: 719.622.6255 | F: 303.861.7767

Dallas, TX
T: 214.722.7100 | F: 214.722.7111

Denver, CO
T: 303.861.7760 | F: 303.861.7767

Fort Lauderdale, FL
T: 954.728.1280 | F: 954.728.1282

Fort Wright, KY
T: 859.663.9830 | F: 859.663.9829

Hartford, CT
T: 860.748.4806 | F: 860.748.4857

Houston, TX
T: 713.659.6767 | F: 713.759.6830

Indian Wells, CA
T: 760.771.6363 | F: 760.771.6373

Indianapolis, IN
T: 317.333.6421

Kansas City, MO
T: 816.299.4244 | F: 816.299.4245

Lafayette, LA
T: 337.326.5777 | F: 337.504.3341

Las Vegas, NV
T: 702.893.3383 | F: 702.893.3789

Los Angeles, CA
T: 213.250.1800 | F: 213.250.7900

Madison County, IL
T: 618.307.7290 | F: 618.692.6099

Miami, FL
T: 786.353.0210 | F: 786.513.2249

New Orleans, LA
T: 504.322.4100 | F: 504.754.7569

New York, NY
T: 212.232.1300 | F: 212.232.1399

Newark, NJ
T: 973.577.6260 | F: 973.577.6261

Orange County, CA
T: 714.545.9200 | F: 714.850.1030

Philadelphia, PA
T: 215.977.4100 | F: 215.977.4101

Phoenix, AZ
T: 602.385.1040 | F: 602.385.1051

Pittsburgh, PA
T: 412.567.5596 | F: 412.567.5494

Portland, OR
T: 971.712.2800 | F: 971.712.2801

Providence, RI
T: 401.406.3310 | F: 401.406.3312

Raleigh, NC
T: 919.821.4020 | F: 919.829.0055

Sacramento, CA
T: 916.564.5400 | F: 916.564.5444

San Bernardino, CA
T: 909.387.1130 | F: 909.387.1138

San Diego, CA
T: 619.233.1006 | F: 619.233.8627

San Francisco, CA
T: 415.362.2580 | F: 415.434.0882

Seattle, WA
T: 206.436.2020 | F: 206.436.2030

Tampa, FL
T: 813.739.1900 | F: 813.739.1919

Temecula, CA
T: 951.252.6150 | F: 951.252.6151

Tucson, AZ
T: 520.399.6990 | F: 520.838.8618

Weirton, WV
T: 304.224.2006 | F: 304.224.2263

Wichita, KS
T: 316.609.7900 | F: 316.462.5746

LewisBrisbois.com