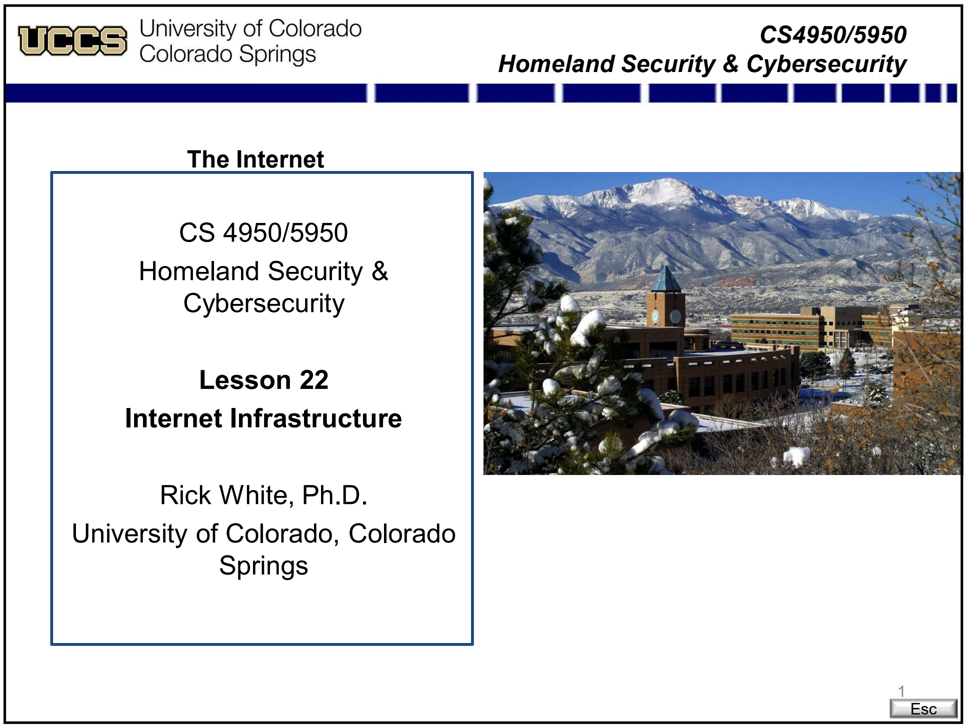


UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

The Internet

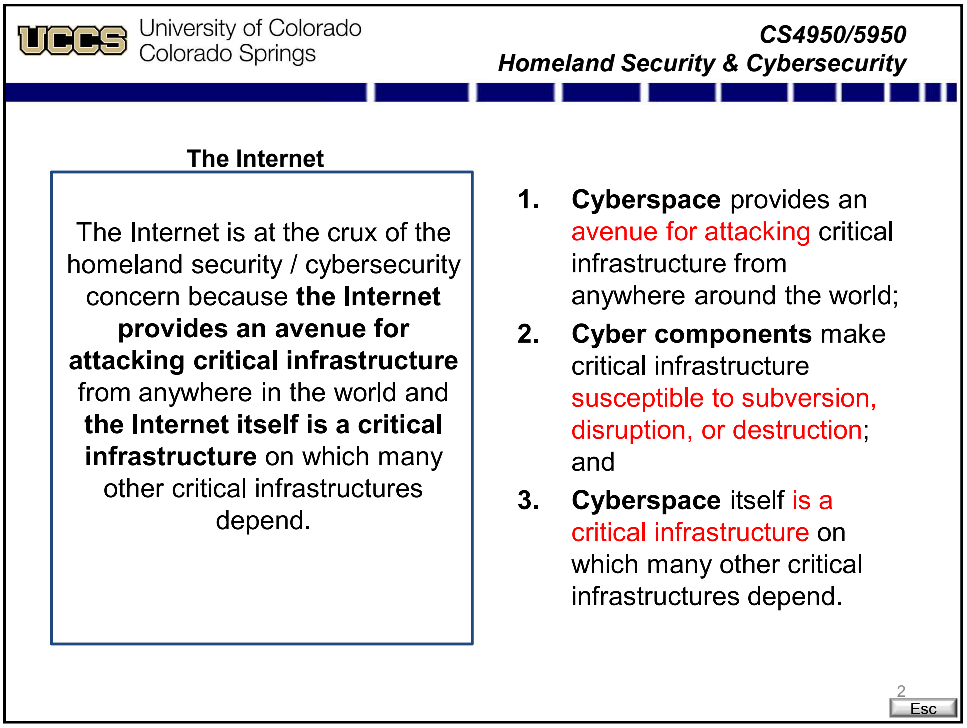
CS 4950/5950
Homeland Security & Cybersecurity

Lesson 22
Internet Infrastructure

Rick White, Ph.D.
University of Colorado, Colorado Springs

1
Esc

1



UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

The Internet

The Internet is at the crux of the homeland security / cybersecurity concern because **the Internet provides an avenue for attacking critical infrastructure** from anywhere in the world and **the Internet itself is a critical infrastructure** on which many other critical infrastructures depend.

1. **Cyberspace** provides an avenue for attacking critical infrastructure from anywhere around the world;
2. **Cyber components** make critical infrastructure susceptible to subversion, disruption, or destruction; and
3. **Cyberspace** itself is a critical infrastructure on which many other critical infrastructures depend.

2
Esc

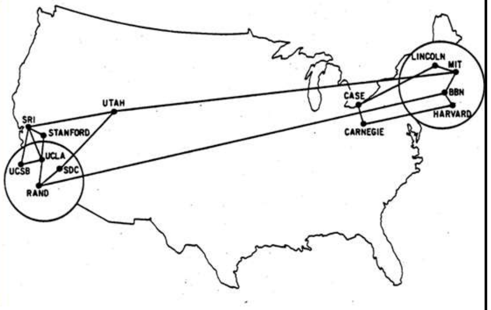
2

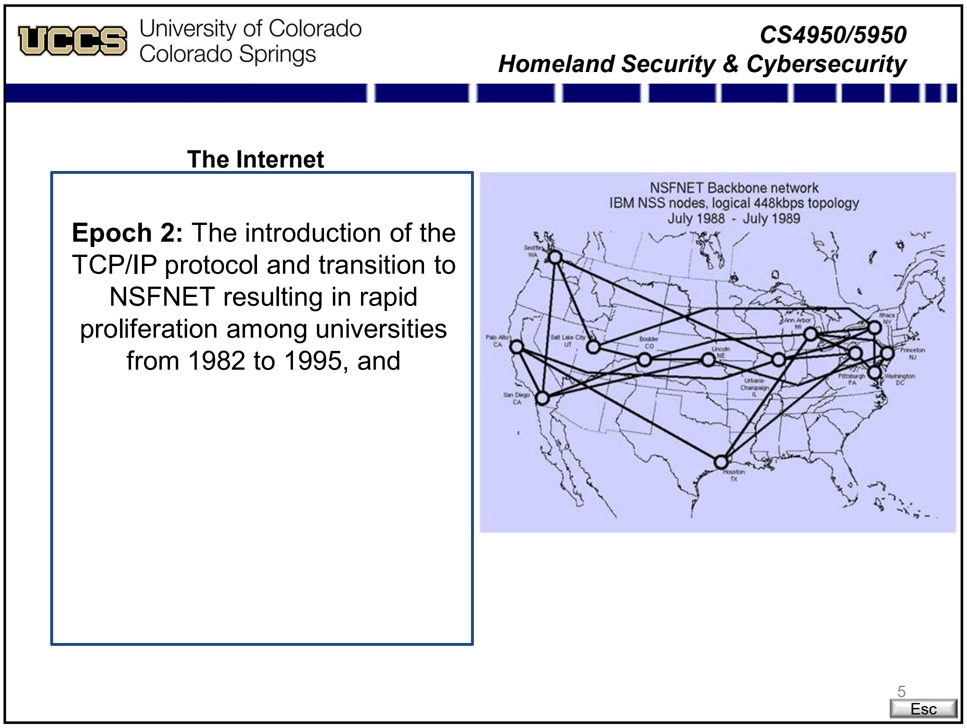
The Internet

- Not surprisingly, the Internet is the youngest of the four infrastructures we examine in this course.
- Developed in the 1960s, the Internet has undergone rapid evolution that may be summarized in **three epochs**...

The Internet

Epoch 1: The creation and expansion of the ARPANET for government-related research from 1969 to 1981.





UCCS University of Colorado Colorado Springs

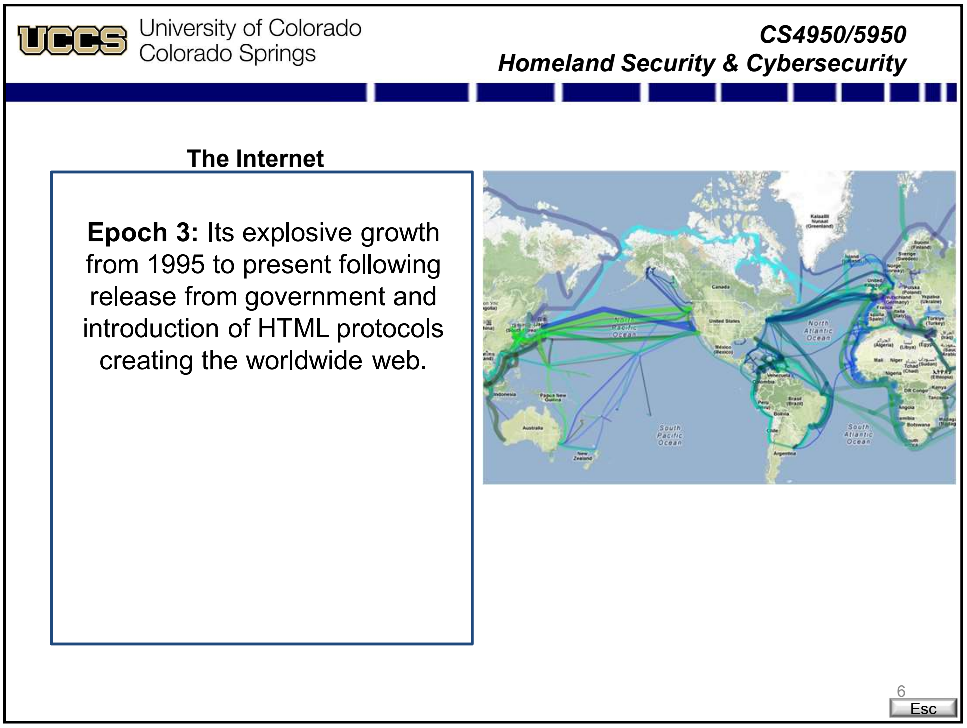
CS4950/5950
Homeland Security & Cybersecurity

The Internet

Epoch 2: The introduction of the TCP/IP protocol and transition to NSFNET resulting in rapid proliferation among universities from 1982 to 1995, and

NSFNET Backbone network
IBM NSS nodes, logical 448kbps topology
July 1988 - July 1989

5



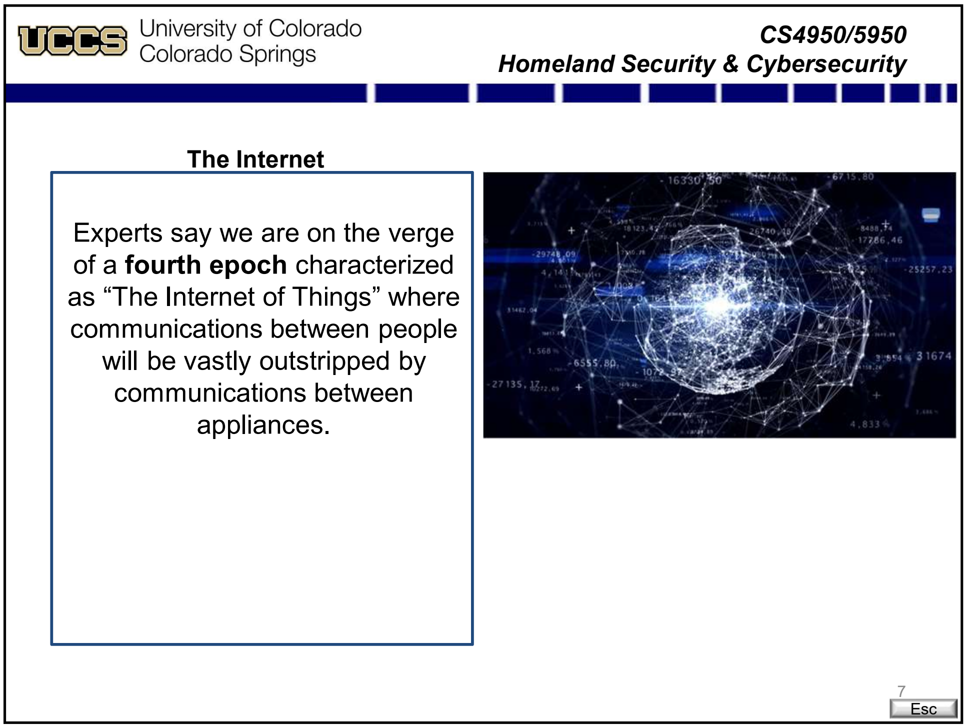
UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

The Internet

Epoch 3: Its explosive growth from 1995 to present following release from government and introduction of HTML protocols creating the worldwide web.

6



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

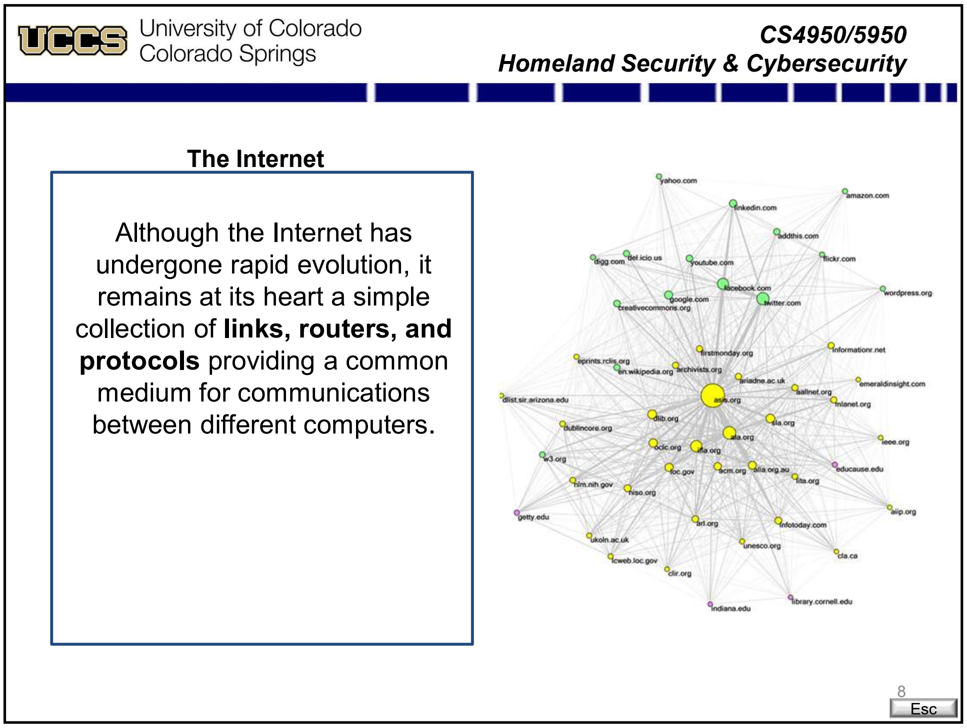
The Internet

Experts say we are on the verge of a **fourth epoch** characterized as "The Internet of Things" where communications between people will be vastly outstripped by communications between appliances.

7

Esc

7



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

The Internet

Although the Internet has undergone rapid evolution, it remains at its heart a simple collection of **links, routers, and protocols** providing a common medium for communications between different computers.

8

Esc

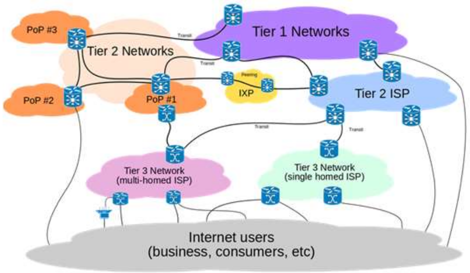
8

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

The Internet

Nobody owns the Internet, however the vast majority of links and routers are owned by a small number of very large, Tier 1, corporate Internet Service Providers.



9
Esc

9

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

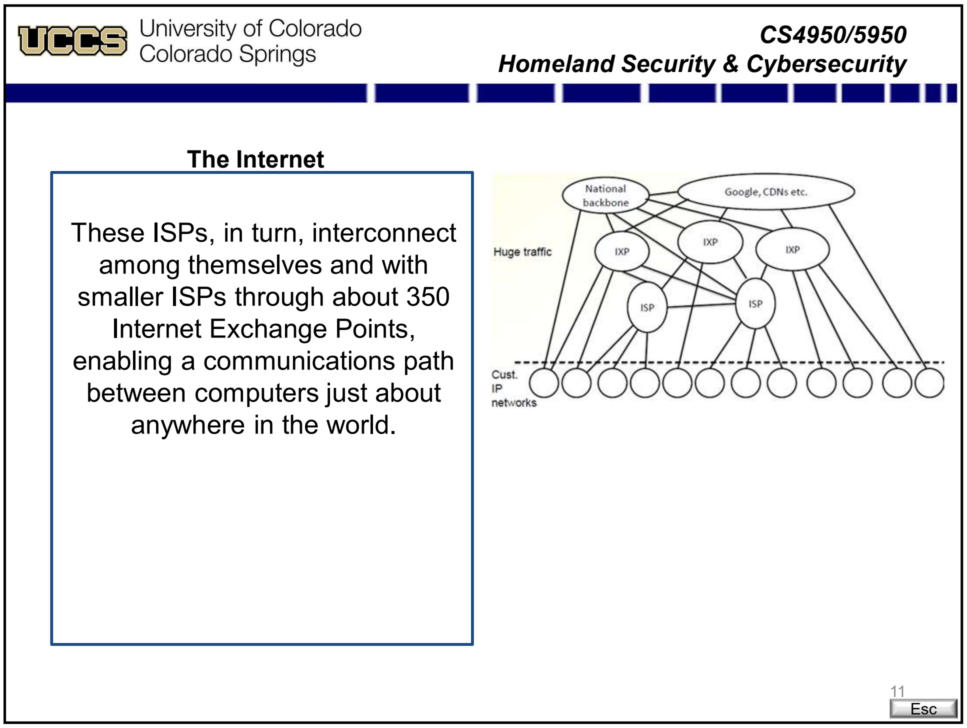
The Internet

In the US there are only 7 Tier 1 ISPs.

Tier 1
Internet Service Providers
AT&T
Verizon
Spring
Century Link
Level 3
NTT/Verio
Cogent

10
Esc

10



University of Colorado
Colorado Springs

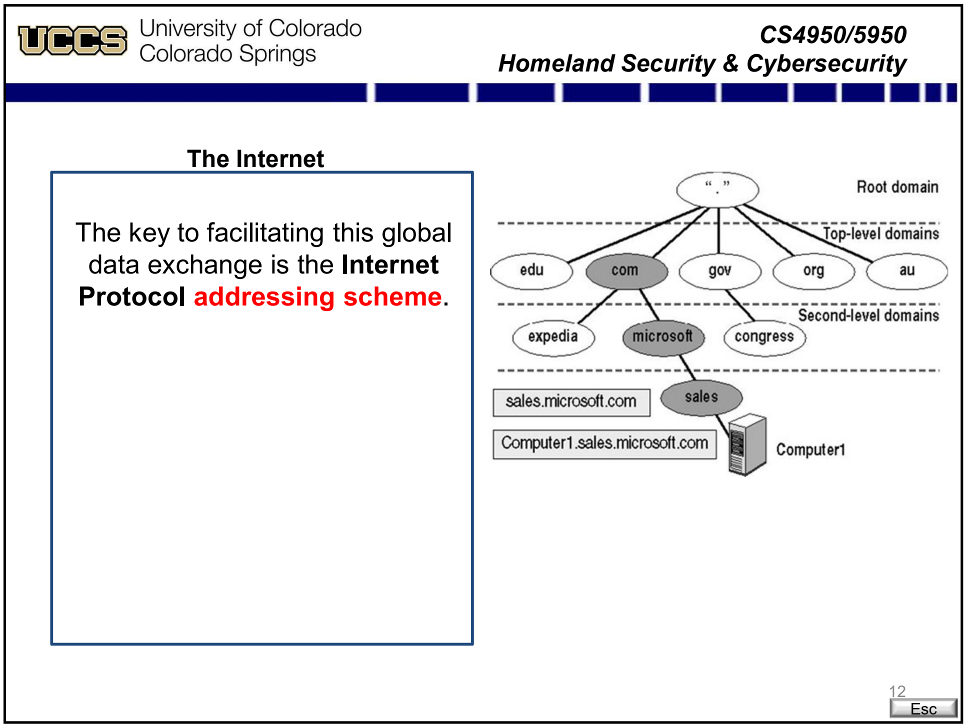
CS4950/5950
Homeland Security & Cybersecurity

The Internet

These ISPs, in turn, interconnect among themselves and with smaller ISPs through about 350 Internet Exchange Points, enabling a communications path between computers just about anywhere in the world.

11
Esc

11



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

The Internet

The key to facilitating this global data exchange is the **Internet Protocol** **addressing scheme**.

12
Esc

12

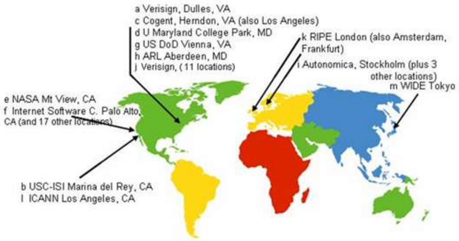
The Internet

- IP addresses are controlled by the Internet Corporation for Assigned Names and Numbers, "**ICANN**", a global non-profit agency operating out of Los Angeles.
- A department within ICANN called the Internet Assigned Numbers Authority, "**IANA**", manages several hundred geographically distributed **Domain Name Servers.**

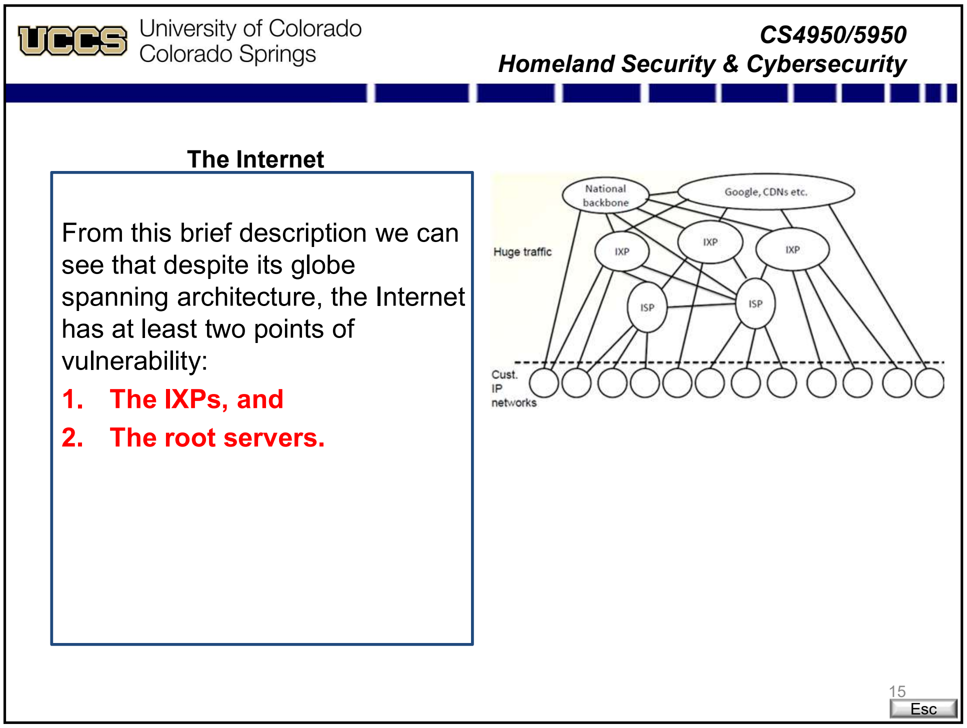
ICANN
The Internet Corporation for Assigned Names and Numbers

The Internet

- IANA Domain Name Servers supply ISP routers with IP address translations that are essential to delivering communication packets to their correct destination.
- Although there are hundreds of Domain Name Servers, IANA maintains master IP address lists on only **13 "root servers".**


a Verisign, Dulles, VA
c Cogent, Herndon, VA (also Los Angeles)
d U Maryland College Park, MD
g US DoD Vienna, VA
h ARL Aberdeen, MD
j Verisign, (11 locations)
k RIPE London (also Amsterdam, Frankfurt)
i Autonomica, Stockholm (plus 3 other locations)
m WIDE Tokyo
e NASA Mt View, CA
f Internet Software C. Palo Alto, CA (and 17 other locations)
b USC-ISI Marina del Rey, CA
l ICANN Los Angeles, CA

iana
Internet Assigned Numbers Authority



UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

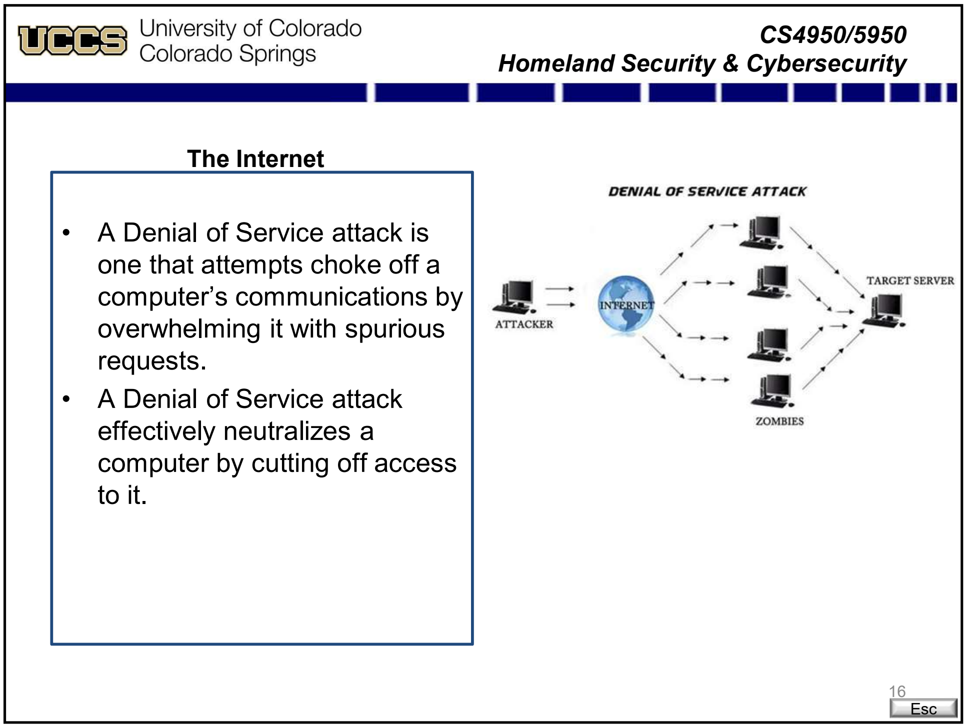
The Internet

From this brief description we can see that despite its globe spanning architecture, the Internet has at least two points of vulnerability:

1. **The IXPs, and**
2. **The root servers.**

15
Esc

15



UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

The Internet

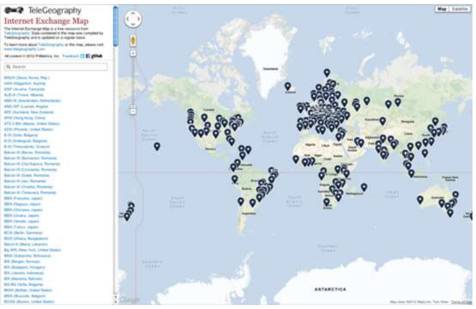
- A Denial of Service attack is one that attempts choke off a computer’s communications by overwhelming it with spurious requests.
- A Denial of Service attack effectively neutralizes a computer by cutting off access to it.

16
Esc

16

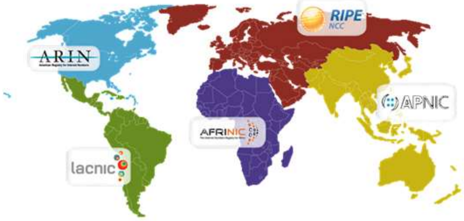
The Internet

It is surmised that a well-timed and coordinated massive Denial of Service attack **could bring down any number of IXPs taking down significant parts of the Internet.**



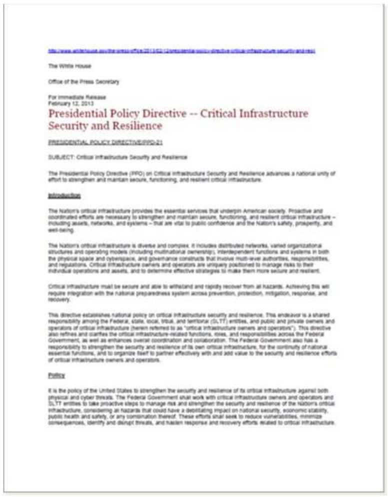
The Internet

- **A more likely target, though are the DNS root servers.**
- In fact, in December 2015, a coordinated Denial of Service attack from many sources succeeded in neutralizing 3 of the 13 IANA root servers.



The Internet

The Internet is classified as part of the Information Technology infrastructure in **PPD-21**, but also **forms the underlying support for most of the Communications infrastructure.**



http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

The White House

Office of the Press Secretary

For Immediate Release
February 12, 2013

Presidential Policy Directive -- Critical Infrastructure Security and Resilience

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.

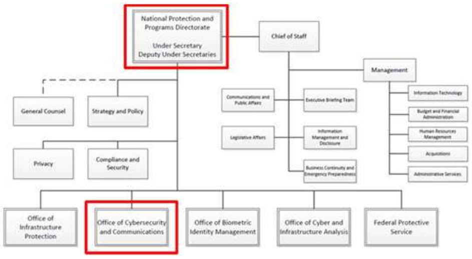
This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators"). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

Policy

It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.

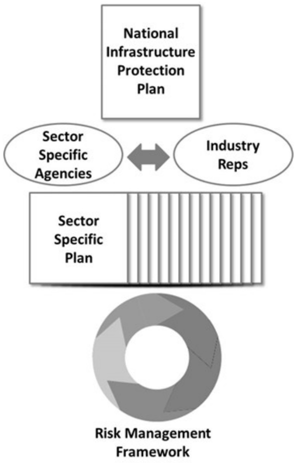
The Internet

The Department of Homeland Security **Office of Cybersecurity and Communications** under the National Protection and Programs Directorate is the designated **Sector-Specific Agency** for the Internet.


National Protection and Programs Directorate
Under Secretary
Deputy Under Secretaries
Chief of Staff
Management
General Counsel
Strategy and Policy
Communications and Public Affairs
Executive Briefing Team
Information Technology
Budget and Financial Administration
Legislative Affairs
Information Management and Disclosure
Human Resources Management
Privacy
Compliance and Security
Acquisitions
Business Continuity and Emergency Preparedness
Administrative Services
Office of Infrastructure Protection
Office of Cybersecurity and Communications
Office of Biometric Identity Management
Office of Cyber and Infrastructure Analysis
Federal Protective Service

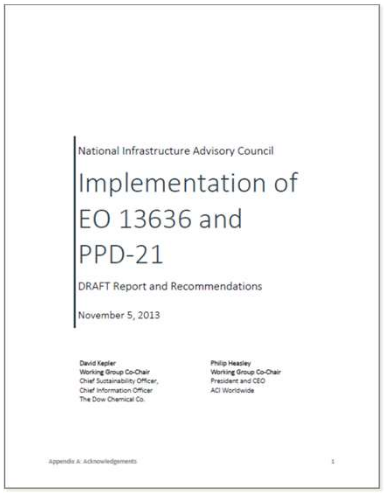
The Internet

DHS has no regulatory authority over the Internet but works with ISPs and ICANN on a voluntary basis.


National Infrastructure Protection Plan
Sector Specific Agencies
Industry Reps
Sector Specific Plan
Risk Management Framework

The Internet

In response to a NIST Request for Information stemming from **Executive Order 13636**, Improving Critical Infrastructure Cybersecurity, the Department of Homeland Security in May 2013 stated that it was not adverse to the NIST Cybersecurity Framework, but it was already employing the **Cyber Assessment Risk Management Approach, "CARMA",** to assess cybersecurity in the Information Technology Sector.



National Infrastructure Advisory Council

Implementation of EO 13636 and PPD-21

DRAFT Report and Recommendations

November 5, 2013

David Kepler
Working Group Co-Chair
Chief Sustainability Officer,
Chief Information Officer
The Dow Chemical Co.

Philip Heasley
Working Group Co-Chair
President and CEO
ACI Worldwide

Appendix A: Acknowledgements 1

Conclusion

Questions?

Esc