BRIEFING BOOK

Cyber Strategic Inquiry

Enabling Change Through a Megacommunity Strategic Simulation

Washington, DC
17-18 December 2008

Acknowledgements

Business Executives for National Security (BENS) would like to thank Booz Allen Hamilton for its support in the planning, design, and execution of the Cyber Strategic Inquiry 2008 (CSI'08).

For over a quarter century, BENS has been the primary non-partisan, nationwide channel through which senior business executives have helped to enhance our country's security. BENS's mission is simple -- to help ensure a safer and more resilient America.

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for more than 90 years. Providing a broad range of services in strategy, operations, organization and change, information technology, systems engineering, modeling, simulation, wargaming and analysis, and program management. Booz Allen is committed to delivering results that endure.

Table of Contents

Executive Summary

Introduction: We are presented with a unique opportunity to shape the national and international dialogue and enable change and transformation. The United States may be facing the most serious economic and national security challenge of the 21st century; our government and private sector networks and information are being exploited at unprecedented scale by a growing array of state and non-state actors. Over the past year, this malicious activity has grown more sophisticated, more targeted, and more serious, and we expect these trends to continue. The situation calls for a new type of tri-sector leadership in which government, business, and civil society work together in a common quest that benefits all without requiring the participants to give up their core identities or values

The Briefing Book: The purpose of this document is to help prepare readers to participate in the *Cyber Strategic Inquiry*. The first sections contain administrative information, information regarding the simulation's objectives and design, and biographies of speakers. The final section contains reference information, including descriptions of cyber vulnerabilities, the cyber security challenges facing government and industry, an overview of civil society efforts, and the potential solutions that are being developed to address these challenges. A list of acronyms is included at the end of the Briefing Book.

Simulation Overview: The *Cyber Strategic Inquiry* aims to create a shared knowledge of cybersecurity risks and potential solutions through the exploration of several key issues. These issues include identifying: overlapping vital interests between government, business, and civil society when managing cyber challenges; the key cyber risks for government, industry, and civil society; and the critical next steps for creating persistent means to address cybersecurity needs. Participants will be assigned to teams that represent their functional/stakeholder interests. Government teams include Defense, Civil Agencies, Intelligence, and Homeland Security. Industry teams include Financial Services, Telecommunications/ Information Technology, Energy, and Transport. The final team, Civil Society, represents think tanks, non-government organizations, and academia. Teams will have three "moves," or scenario installments, to explore opportunities for enhanced collaboration.

Cyber Vulnerabilities: The cyber environment is composed of govemment, public, and private networks that are increasingly inter-reliant. Perpetrators of cyber crimes represent a diverse group of actors, such as foreign national governments, terrorists, industrial spies and organized crime groups, disgruntled employees, activists, and hackers, capable of significant exploitation of cyber vulnerabilities. The Department of Homeland Security tracked 37,258 cyber attacks in 2007, and the numbers of attacks continue to increase in both quantity and sophistication. Types of attacks include unauthorized access, denial of service, malicious code, and social engineering.

Executive Summary (continued)

Industry: Industry faces an array of challenges as the volume and sophistication of cyber crimes and cyber attacks increase. These vulnerabilities include physical security, commercial espionage, network resiliency, identity theft, database integrity, secure communications, cyber extortion, and encryption technologies. To protect our vital industries, steps have been taken to bolster cyber security measures, and industries are working towards achieving sector wide coordination and public-private cooperation.

Government: The US Government's federal network, which controls classified information, nuclear weaponry, and some critical infrastructure, is vulnerable to cyber attack. In response to the threats to both the government itself and to vital private networks, the government has developed the Comprehensive National Cybersecurity Initiative and the National Cyber Security Center within the Department of Homeland Security. Agencies and offices also exist within the Department of Defense, the Secret Service, the intelligence communities, and the Department of Justice that specifically focus on addressing cybersecurity threats.

Civil Society: Numerous non-government organizations focus on cybersecurity issues. Some, such as the US Cyber Consequences Unit, provide assessments of the strategic and economic consequences of possible cyber-attacks and cyber-assisted physical attacks. Others, like the CyLab, deliver security technologies, research expertise, and a consortium of industry leaders to counter cybersecurity vulnerabilities. Still others, such as the Center for Strategic and International Studies, provides strategic insights and policy solutions regarding cybersecurity to decision-makers.

Policies: Numerous strategies and policies have been developed to provide a strategic context for cyber and information security and to direct departments and agencies to undertake various measures to improve the security of the United States. The *National Strategy to Secure Cyberspace* outlines a framework to reduce our nation's vulnerability to attacks against our critical information infrastructures. *Homeland Security Presidential Directive 7* establishes a national policy to protect United States critical infrastructure and key resources from terrorist attacks. The *National Strategy for Information Sharing* aims to coordinate information about terrorist activity across all relevant government agencies and departments.

Way Ahead: Our increasingly globalized and interconnected world is creating issues that are too large for any one authority to solve alone. The situation consequently calls for a new type of tri-sector leadership in which government, industry and civil society work together in a state of permanent negotiation and interaction. By networking government, industry, and civil-sector communities together—creating Megacommunities—leaders will be able to share resources, talent, and innovative ideas in new ways that produce enduring solutions to the world's most significant problems, such as cybersecurity challenges.

Table of Contents

Venue Details

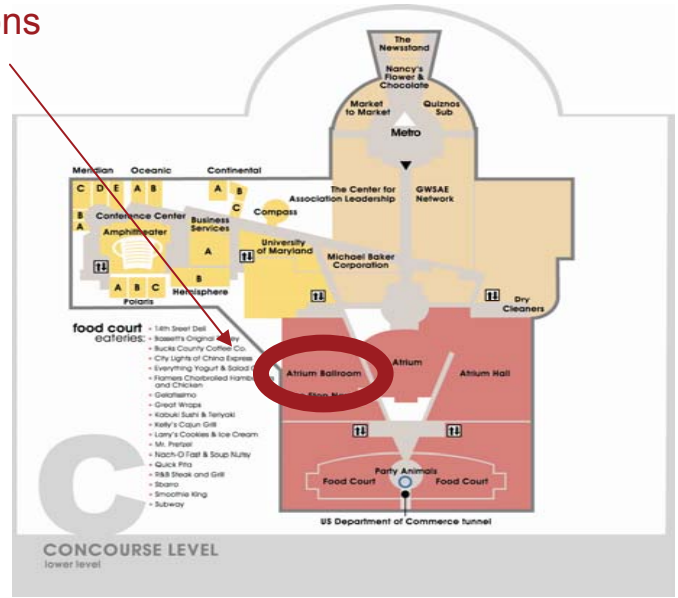
Thank you for agreeing to participate in CSI'08. CSI'08 will be held December 17-18 at the Ronald Reagan Building and International Trade Center.

- The Ronald Reagan Building and International Trade Center is located 1300 Pennsylvania Avenue in Washington, D.C.
- The Federal Triangle metro stop (orange/blue lines) is connected to the Ronald Reagan Building and International Trade Center by a covered passageway. The Metro Center metro stop (red line) is two blocks away
- Daily parking is available in underground parking garage (max daily fee- $21.00)
  - Access is available via 13½ Street (off Pennsylvania Avenue) and via two entrances on 14th Street from 5:00 am until 2:00 am
  - There is a 100% vehicle/id check, please allow time

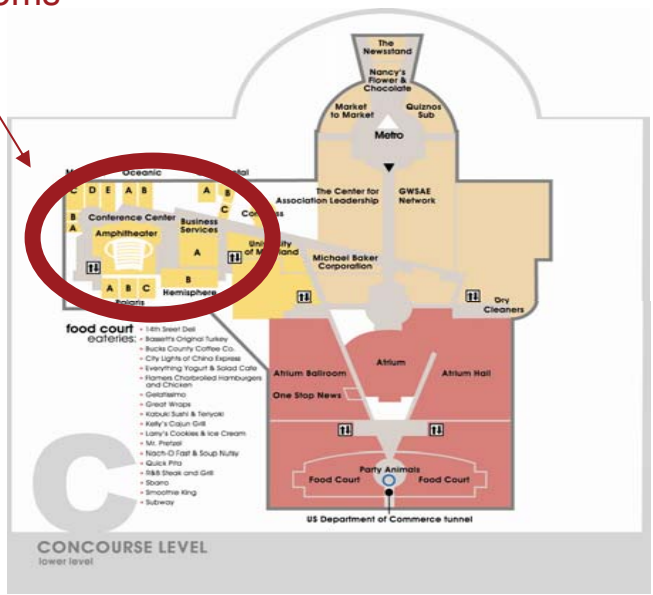
Event Details

- Registration will begin at 11am on December 17th
- Lunch will be available starting at 11am in the Atrium Ballroom
- All plenary sessions will take place in the “Atrium Ballroom” located on the concourse level
- Participants will move to assigned team rooms following the first plenary (also located on the concourse level)

Plenary Sessions



Team Rooms



Administrative Information

- There is no conference fee for this event
- The dress code is business attire
- A reception and dinner will be held the evening of December 17th in the Pavilion Room located on the Second Floor
- A registration desk will be staffed throughout the event for phone messages
  - A phone number for incoming messages will be provided at registration

Table of Contents

Why conduct a cyber simulation now?

- We are presented with a unique opportunity to shape the national and international dialogue and enable change and transformation
- The United States may be facing the most serious economic and national security challenge of the 21st century; our government and private sector networks and information are being exploited at unprecedented scale by a growing array of state and non-state actors
- Over the past year, this malicious activity has grown more sophisticated, more targeted, and more serious, and we expect these trends to continue
- The US must take action to protect the critical components upon which our economy, government, and national security are based from potential exploitation, disruption or destruction
- We are evolving to more and more complex network structures, where interdependencies lead to expanded opportunities and increased vulnerabilities; given this, cybersecurity is simply too large and complex for any one authority to solve alone
- The situation calls for a new type of tri-sector leadership in which government, business, and civil society work together in a common quest that benefits all without requiring the participants to give up their core identities or values

The *Cyber Strategic Inquiry* will be a forum for key government, business, and civil society stakeholders to explore the shared cybersecurity challenges and examine the potential opportunities of a Megacommunity approach to address the challenges of balancing cyber accessibility and security

The *Cyber Strategic Inquiry* will create a shared knowledge of cybersecurity risks and potential solutions

Objectives

- Create awareness of the urgency and the interconnectedness of government, business, and civil society to address the shared risks and opportunities inherent in cybersecurity
- Identify activities that will enable public and private sectors, and other elements of civil society, to work together to identify new solutions for assuring the resilience of our cyber infrastructure
- Generate a shared vision of the responsibilities and investment strategies (e.g., talent, technology, money, leadership) that will be required across government, business, and civil society to meet future cybersecurity and resilience issues
- Explore the attributes of persistent means – for example, a Cyber Megacommunity – that will enable affected public and private entities and other elements of civil society to more effectively and openly address cybersecurity challenges and opportunities

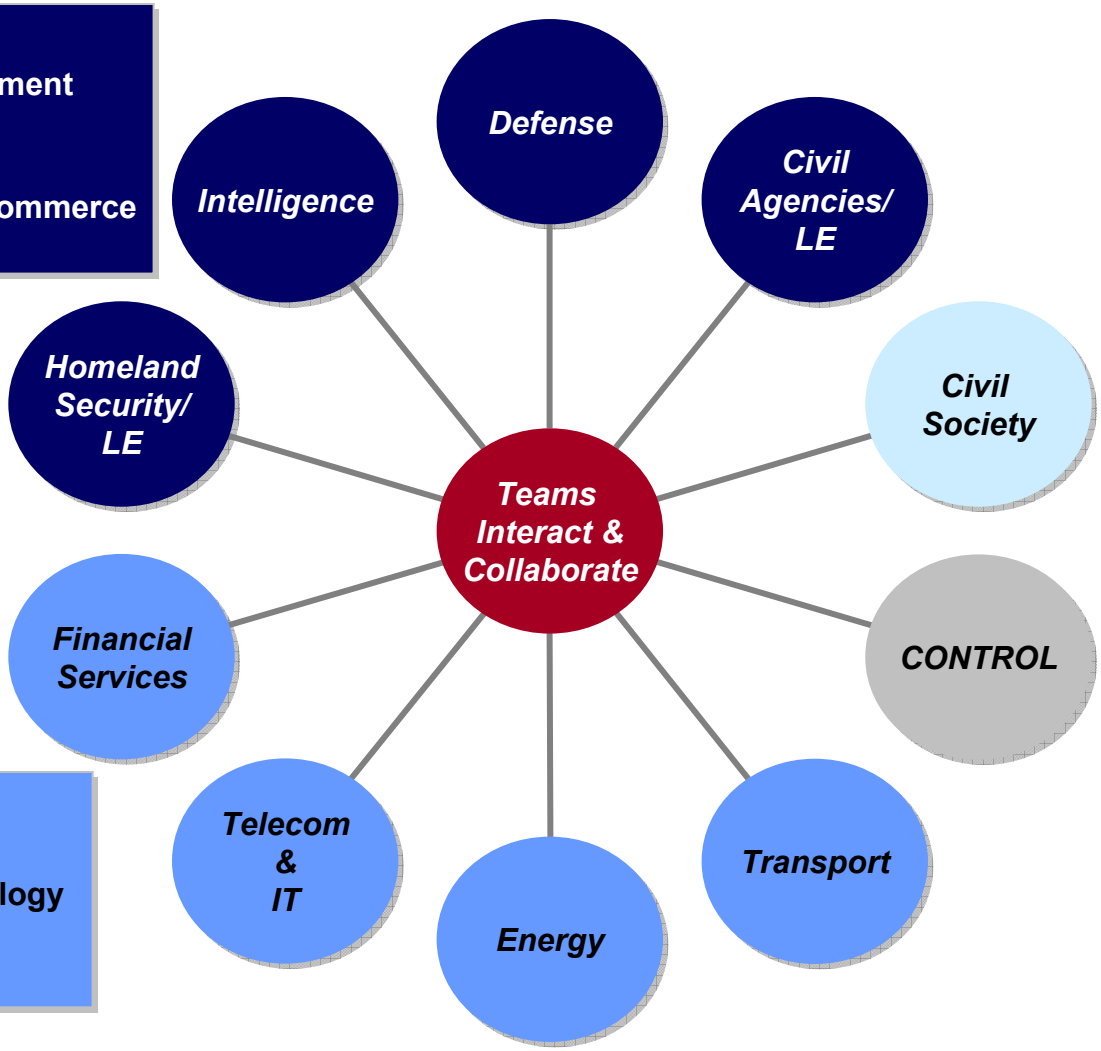
Inquiry participants will explore a series of key issues

Key Issues

- What are the overlapping vital interests (known and unknown) between government, business, and civil society when managing cyber challenges?
- What are the key cyber risks for government, business, and civil society?
- How can government, business, and civil society collaborate to develop new solutions to cyber challenges? What are the key actions/activities that can be undertaken to assure the resilience of our cyber infrastructure?
- What investment strategies are required to address cyber opportunities?
  - What kinds of people are required?
  - What technologies are essential?
  - What funding is required?
  - What leadership is required?
  - What is the long term research and development strategy?
- What are the critical next steps for creating persistent means to address cybersecurity?
  - What outcomes are expected?
  - How can we influence and expand the national and international cyber dialogue?

The *Inquiry* is designed to represent a variety of functional/ stakeholder interests and highlight interconnectedness

Government:
- Federal Law Enforcement (LE)
- International (State)
- Financial Services/Commerce (Treasury/IRS)



Civil Society:
- Think Tanks
- NGOs
- Academia

Control Team:
- Oversees Simulation Play
- Reacts/Plays for All Others (e.g., White House, Congress, International Actors, Media)
- Introduces External Shocks
- Assesses Impact

Industry:
- Public Safety
- Information Technology
- Supply Chain
- Retail

Government Teams represent key US government agencies and entities with cyber roles and responsibilities

Homeland Security/Law Enforcement

- Represents US Government entities that play a homeland security function
- US Department of Homeland Security (i.e. US-CERT, National Cyber Security Center, Critical Infrastructure Protection Advisory Council), FBI

Defense

- Represents US Government entities that play a defense function
- US Department of Defense (i.e. Office of the Secretary of Defense, Joint Staff), Combatant Commands (i.e. USSTRATCOM, USNORTHCOM), key defense entities (i.e. JTF-GNO, DISA, DARPA, DoD Cyber Crime Center)

Intelligence

- Represents US Government entities that serve an intelligence function
- Office of the Director of National Intelligence, National Security Agency, Central Intelligence Agency

Civil Gov Agencies/Law Enforcement

- Represents civil US Government agencies
- Department of the Treasury, Federal Reserve and IRS; Department of Transportation and FAA; Department of Energy, FERC, and NRC; Department of Commerce and National Institute of Standards and Technology; Department of Justice; Department of State; National Science Foundation

The Control Team represents: The White House, Congress, International Actors, and the Media

Industry Teams represent various interests of the private sector

Financial Services

- Represents the Financial Services Sector
- Banks, Exchanges, Financial/Payment Utilities, Investment Firms, Retail, Credit Card Providers/Processors

Energy

- Represents the Energy Sector
- Utility Companies (i.e. Con Edison), Energy Providers (i.e. Exxon Mobile), Pipelines

Transportation

- Represents the Transportation Sector
- Passenger and Freight Providers (Air, Rail, and Sea), Metro Transit Authorities (i.e. New York Metropolitan Transit Authority), Automakers

Telecom/IT

- Represents the Telecommunications and Information Technology Sector
- Telecom includes: Internet Service Providers, Telecom Service Providers
- IT Includes: Hardware/Software Developers (i.e. Microsoft and Symantec)

The Civil Society Team represents NGOs, Think Tanks, Academia and the Public

Civil Society

- Represents Academic Institutions (i.e. Carnegie Mellon CyLab)
- Represents NGOs (i.e. Electronic Frontier, National Cyber Security Alliance)
- Represents Think Tanks (Center for Strategic and International Study)
- Provides the Perspective of Public Reaction

The *Inquiry* will seek to unlock capabilities among stakeholders to address cyber challenges and opportunities

HOW IT WORKS

- Participants are assigned to teams representing a functional focus
  - Teams will be "mixed" to provide participants with an opportunity to experience an alternative perspective, with a core of the team representing the specific functional focus
- Scenarios provide a dynamic environment in which stakeholders address cyber challenges, make decisions, and identify opportunities to develop new cyber solutions
- The *Inquiry* progresses over a series of two scenario moves and one insights move
- During moves, teams:
  - Identify objectives, priorities, and strategies
  - Take actions to achieve strategy
  - Collaborate with other teams to meet overlapping vital interests
  - Brief decisions and rationale to all other teams after each move
- Teams communicate via email and face-to-face sessions

Teams will have three moves to engage opportunities for enhanced collaboration across the Cyber Megacommunity

MOVE 1

Afternoon Session 1 – Detection

- How are you reacting to the cyber challenges in your sector?
- What are your options for determining the root cause and diagnose the cyber challenges?
- Who must you coordinate with to detect the full extent of the cyber challenges you are facing? What coordination mechanisms/venues are you using?

MOVE 2

Afternoon Session 2 - Mitigation

- What innovative solutions and/or programs are needed to meet your interests and address (treat) the cyber challenges?
- Who must you coordinate with to mitigate the effects of your sector's cyber challenges?
- What barriers do you face in coordinating? How can these be overcome?

INSIGHTS GAINED

Morning Session - Prevention

- Looking back…what could you have done 6 months ago to prepare for/prevent these cyber challenges?
  - Innovative solutions/programs?
  - Coordinating mechanisms?
  - Investment strategies?
- What are the critical next steps for creating persistent means to address cybersecurity?
  - What outcomes are expected?
  - How can we influence and expand the national and international cyber dialogue?
- What should be our engagement model going forward for the Cyber Megacommunity?
  - Who should initiate/convene?
  - How should the megacommunity measure its progress?

Cyber Strategic Inquiry Schedule

	DAY 1 | December 17, 2008	
Introduction	11:30-12:00	Welcome Luncheon Speaker: Cristóbal Conde, CEO SunGard (confirmed)
	12:00-12:30	Megacommunity primer and introduction to the inquiry instructions for Move 1
Move 1	12:30-12:45	Get organized – Assess challenges
	12:45-2:00	Take actions – Communicate with other teams Complete response for Move 1 – Complete briefing
Brief Move 1	2:00-3:15	Each team briefs its challenges and rationale to all Feedback from Control – and Update for Move 2
Move 2	3:15-3:30	Assess feedback and new challenges
	3:30-4:30	Take actions – Communicate with other teams
	4:30-4:45	Complete response for Move 2 – Complete briefing
Brief Move 2	4:45-6:00	Each team briefs its actions and rationale to all
	6:00-8:00	Reception & dinner Keynote Speaker: General James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff (confirmed)
	DAY 2 | December 18, 2008	
Insights	8:00-8:30	Welcome Breakfast Speaker: Dan Hesse, CEO Sprint (confirmed)
	8:30-8:45	Re-Cap of Day 1 – Instructions for Insights Session
	8:45-10:00	Teams identify insights and next steps
Brief Insights	10:00-11:30	Each team briefs its insights and next steps (with Principal Deputy Director of National Intelligence Dr. Donald Kerr)
	11:30-12:30	General discussion of insights and next steps Speaker: Secretary Michael Chertoff, US Department of Homeland Security (confirmed)
	12:30	Strategic Inquiry concludes

Ground Rules

- All discussions must remain at the UNCLASSIFIED level
- Please don't fight the scenario
  - "Incredible" things happen all the time – accept and work with them
  - The objective is not to argue about whether or not something could happen, but rather to explore how we would deal with an event if it did happen
- We never have as much information as we would like to make decisions in the real world – nonetheless, decisions must be made
  - This situation will not be any different
  - We will use what we have and make the best decision possible
- Play is on a "non-attribution" and "not-for-release" basis
  - Please do not attribute any statement or action to any individual or organization

The simulation allows communications between teams by email and ad-hoc face-to-face meetings

- Teams are located in several breakout rooms
- Teams communicate via email and possibly face-to-face meetings if approved by the Control Team
- Use the email system installed in all team rooms for communications between teams (e.g., gather information, request assistance, coordinate response, inform the public)
  - Each team is supported by a rapporteur who will operate the email system for you and assist in preparing your briefing slides
  - If you need to communicate with someone not represented by another team, send the message to Control identifying the target of communications or request
  - Control must be copied on all emails – it only “happened” if Control knows it happened
  - Please submit all emails/responses to the rapporteur in written form

Get organized as a team and begin preparing your briefing no later than 15 minutes before the plenary session

- Facilitators will guide you through the process and ensure that the team discussions stay on track
- At the beginning of each Move, the team should agree on a team briefer to present the briefing slides during the plenary session – this may be a different person for each Move
- Lay out your decisions and rationale using the provided agenda / briefing template (your rapporteur has an electronic copy of your templates)
  - These are the questions you must answer during the Move
  - Your decisions and rationale become your briefing to all in the plenary session
  - Copies of each team's briefing will be provided to all teams following the plenary session
- During the plenary session, ask questions and take notes of critical actions you will want to discuss when you return to your team rooms to begin the next Move

Table of Contents

Speaker Biography – Cristóbal Conde, CEO, SunGard

Cristóbal Conde is SunGard's president and chief executive officer, and a member of its board of directors. He was elected chief executive officer in 2002 and has been a board member since 1999. Mr. Conde served as chief operating officer between 1999 and 2002 and previously headed up SunGard's Trading Systems division, which he started in 1990. Prior to joining SunGard, Mr. Conde co-founded Devon Systems International, Inc., which was acquired by SunGard in 1987. At the time, Devon focused on providing systems for the interest rate and currency derivatives markets. Born in Santiago, Chile, Mr. Conde is a U.S. citizen and holds a BS in Astronomy and Physics from Yale University.

Source: SunGard, http://www.sungard.com/aboutsungard/managementteam.aspx

Keynote Speaker Biography – General James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff

General Cartwright serves as the eighth Vice Chairman of the Joint Chiefs of Staff. In this capacity, he is a member of the Joint Chiefs of Staff and the Nation's second highest ranking military officer. As Vice Chairman, General Cartwright chairs the Joint Requirements Oversight Council, Co-Chairs the Defense Acquisition Board, and serves as a member of the National Security Council Deputies Committee, the Nuclear Weapons Council and the Missile Defense Executive Board. In addition, he Co-Chairs the Deputies Advisory Working Group, which provides advice to the Deputy Secretary of Defense Gordon England on resourcing and other high level departmental business issues. General Cartwright was commissioned a second lieutenant in the Marine Corps in November 1971. He completed Naval Flight Officer training in April 1973 and graduated from Naval Aviator training in January 1977. He has operational assignments as an NFO in the F-4, and as a pilot in the F-4, OA-4, and F/A-18. He is a distinguished graduate of the Air Command and Staff College at Maxwell AFB, received his Master of Arts in National Security and Strategic Studies from the Naval War College, Newport, Rhode Island and completed a fellowship with Massachusetts Institute of Technology. General Cartwright's command assignments include: Commander, United States Strategic Command (2004-2007); Commanding General, First Marine Aircraft Wing (2000-2002); Deputy Commanding General, Marine Forces Atlantic (1999-2000). General Cartwright's joint staff assignments include: Director for Force Structure, Resources and Assessment, J-8 the Joint Staff (2002-2004); Deputy Director for Force Structure, Requirements, J-8 the Joint Staff (1996-1999).

Source: Joint Chiefs of Staff, http://www.jcs.mil/bios/bio_cartwright.html

Speaker Biography – Dan Hesse, CEO, Sprint Nextel Corporation

Dan Hesse, 55, was named chief executive officer of Sprint Nextel on Dec. 18, 2007. Prior to his appointment as Sprint CEO, Hesse was the Chairman and CEO of Embarq Corporation, which generated more than $6 billion in revenues annually, providing voice, data, wireless, and entertainment services in eighteen states. Hesse also spent 23 years at AT&T. From 1997 - 2000, he served as the President and CEO of AT&T Wireless Services, at the time the United States' largest wireless operator. Previously, as the leader of the Online Services Group, Hesse launched AT&T's global online initiatives, which included the AT&T Worldnet family of internet services. From 1991-1995, he served as the President and CEO of AT&T Network Systems International, a joint-venture telecommunications technology company with revenues of $2 billion and a work force of 7,000 employees. He also held prior AT&T management assignments in Network Operations, Network Engineering, International Services, Human Resources, Strategic Planning, Product Management and Sales. From 2000 - 2004, he served as chairman, president and chief executive officer of Terabeam Corporation, a wireless telecommunications service provider and technology company. Hesse received a master of science degree from the Massachusetts Institute of Technology, a master's degree in business administration, with distinction, from Cornell University, and a bachelor of arts degree, with honors, from the University of Notre Dame. He was awarded the Brooks Thesis Prize for writing the outstanding master's thesis from all master's programs at MIT's Sloan School of Management. Hesse has been named Wireless Industry "Person of the Year" by RCR magazine, "Executive of the Year" by Wireless Business and Technology magazine and "Most Influential Person in Mobile Technology" by LAPTOP Magazine.

Source: Sprint, http://www2.sprint.com/mr/ex_dtl.do?id=560

Speaker Biography – Secretary Michael Chertoff, US Department of Homeland Security

On February 15, 2005, Judge Michael Chertoff was unanimously confirmed by the Senate and sworn in as the second Secretary of the Department of Homeland Security. He formerly served as United States Circuit Judge for the Third Circuit Court of Appeals, after his June 2003 Senate confirmation. Secretary Chertoff was previously confirmed by the Senate in 2001 to serve as Assistant Attorney General for the Criminal Division at the Department of Justice. As Assistant Attorney General, he oversaw the investigation of the 9/11 terrorist attacks. He also formed the Enron Task Force, which produced more than 20 convictions, including those of CEOs Jeffrey Skilling and Ken Lay. Before joining the George W. Bush Administration, Chertoff was a Partner in the law firm of Latham & Watkins. From 1995 to 1996, he served as Special Counsel for the U.S. Senate Whitewater Committee. Prior to that, Chertoff spent more than a decade as a federal prosecutor, including service as U.S. Attorney for the District of New Jersey, First Assistant U.S. Attorney for the District of New Jersey, and Assistant U.S. Attorney for the Southern District of New York. As a federal prosecutor, Chertoff investigated and personally prosecuted significant cases of political corruption, organized crime, and corporate fraud. Among them was the “Mafia Commission” case, in which the leaders of La Cosa Nostra were all convicted and sentenced to 100 years in prison for directing the criminal activities of the American Mafia. Chertoff graduated magna cum laude from Harvard College in 1975 and magna cum laude from Harvard Law School in 1978. From 1979-1980 he served as a clerk to Supreme Court Justice William Brennan, Jr.

Source: US Department of Homeland Security, http://www.dhs.gov/xabout/structure/biography_0116.shtm

Table of Contents

Reference Material

The following pages are designed to serve as reference materials, providing participants with background information for each sector represented in the simulation (Civil Society, Government, and Industry), to include an overview of the vulnerabilities faced and potential solutions being developed by each sector.

The reference materials are intended to provide an initial foundation for simulation play, with participants working during the simulation to develop innovative new solutions to the most pressing cyber challenges.

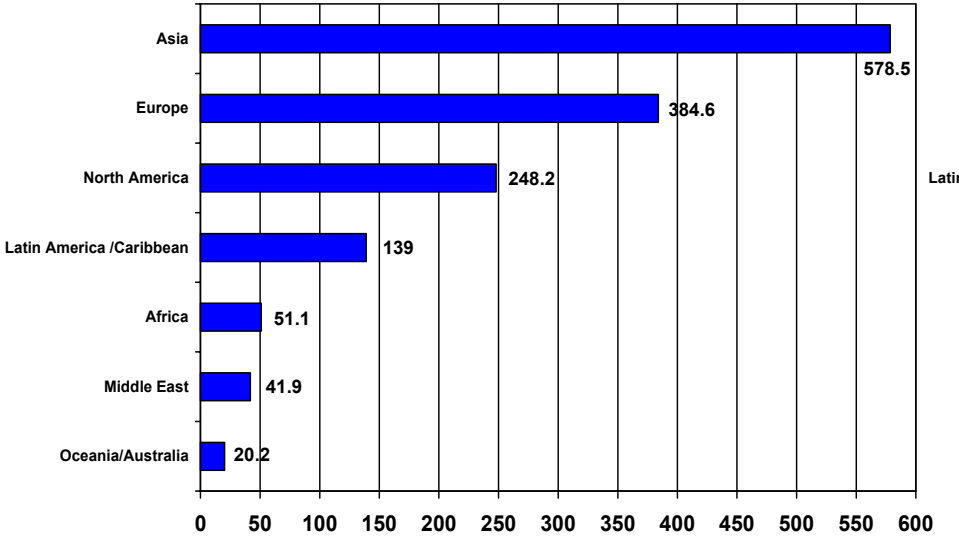
Reference Material

The Internet contains millions of networks accessed by over a billion people with an increasing percent found in developing regions

- As of March 31, 2008, 1.464 billion people (21%) of the global population used the Internet
  - Growth rates of internet users for the past seven years suggest that the largest areas of growth will not be in North America or Europe, but rather in the Middle East, Africa, and Latin America
  - As the rest of the world grows more internet literate, US networks will likely need to be prepared to face more sophisticated attacks from abroad

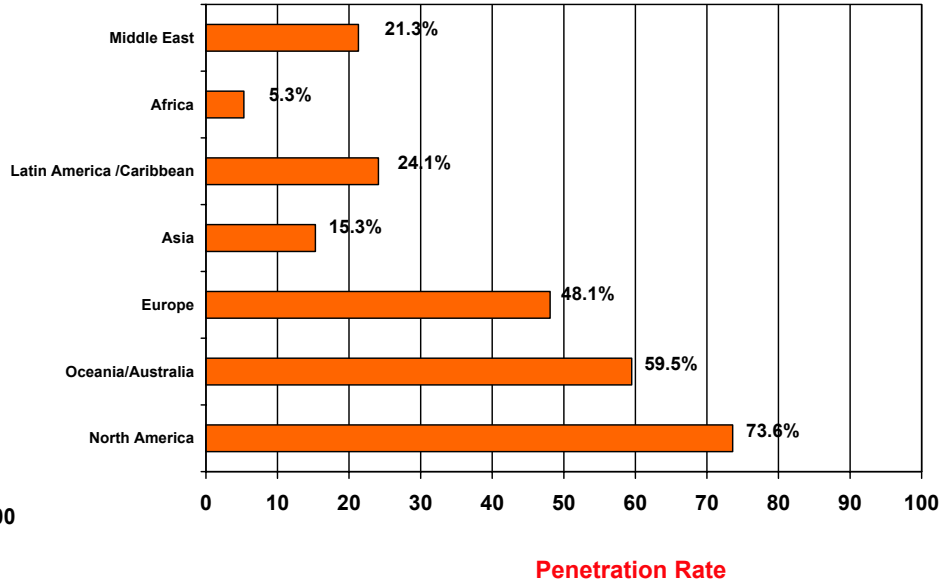
Internet Users in the World

March 2008



World Internet Penetration Rates

March 2008



Sources: Internet World Stats at www.internetworldstats.com

Key definitions shape the cyber environment

Term	Working Definitions
Cyber	The Internet, computer-managed networks, computer-managed processes and controllers, software and hardware controlled devices, software, human management and use of the above networks, and devices
Cyber security	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wired communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation
Cyber Incident	Any attempted or successful access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application or an information system, without lawful authority
Cyber Threat Investigation	Any actions taken by the US, consistent with the applicable laws and Presidential Guidance, to determine the identity, location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more cyber threat groups or individuals

There are many different definitions for key cyber terms, for the purposes of our simulation, the above definitions will be used

Sources: Booz Allen analysis

The cyber environment is composed of government, public, and private networks that are increasingly inter-reliant

- Because the internet is a “network of networks” where all types of secure government, open public, and restricted private networks are located, security deficiencies in one network can be used to exploit vulnerabilities in another
  - As a result, megacommunities and partnerships between the US Government, International entities/countries, and industry will be increasingly important, especially as criminals and terrorists join their motivations and capabilities
- The US military is supported partly by civilian high technology services and products, most often in the form of communications systems and computer software
  - In future conflicts that involve cyberwarfare between nations, the distinction between US military and civilian targets may be blurred and civilian computer systems may increasingly be seen as viable targets vulnerable to attack by adversaries
- At the same time, several criminals who have recently been convicted of cybercrimes used their technical skills to acquire stolen credit card information in order to finance other conventional terrorist activities
  - It is possible that as criminals and terrorist groups explore more ways to work together, a new type of threat may emerge where extremists gain access to the powerful network tools now used by cybercriminals to steal personal information, or to disrupt computer systems that support services through the Internet

Sources: CRS Report “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress” November 2007

Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the unique identifiers of internet addresses

- **What is the ICANN?**
  - To reach another person on the Internet you have to type an address into your computer - a name or a number
  - That address has to be unique so computers know where to find each other; ICANN coordinates these unique identifiers across the world
  - ICANN does not control content on the Internet nor does it create or make Internet policy
  - ICANN is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable

- **What is the DNS?**
  - A Domain Name System is an amorphous linking of millions of web servers
  - DNS helps users find their way around the Internet by converting IP addresses into a familiar string of letters

- **What is the relationship between ICANN and the DNS?**
  - ICANN is responsible for coordinating the management of the technical elements of the DNS to ensure universal resolvability so that all users of the Internet can find all valid addresses
  - It does this by overseeing the distribution of unique technical identifiers used in the Internet's operations, and delegation of Top-Level Domain names (such as .com, .gov, .org, .info)

Sources: Internet Corporation for Assigned Names and Numbers; http://www.icann.org/en/about/

Cyber perpetrators represent a diverse group of actors capable of significant exploitation of cyber vulnerabilities

Potential Perpetrators	Extent of Cyber Vulnerabilities
▸ Foreign National Governments ▸ Terrorists ▸ Industrial Spies and Organized Crime Groups ▸ Disgruntled Employees ▸ Activists ▸ Hackers	▸ In 2005, there were 4,095 digital attacks on the U.S. Government – 1,806 involved malware, 31 were DDoS attacks, and 304 involved unauthorized access ▸ DHS tracked 37,258 cyber attacks in 2007 ▸ According to the Office of Management and Budget (OMB), these numbers are low and mask much larger numbers of unreported or udetected attacks

Sources: US Computer Emergency Readiness Team, "Cyber Threat Source Descriptions," http://www.us-cert.gov/control_systems/csthreats.html; "Bush Looks to Beef Up Protection Against Cyber Attacks," Wall Street Journal, January 28, 2008; "OMB: Modest Gains in Federal Cyber Security," Brian Krebs, Washington Post, March 7, 2006

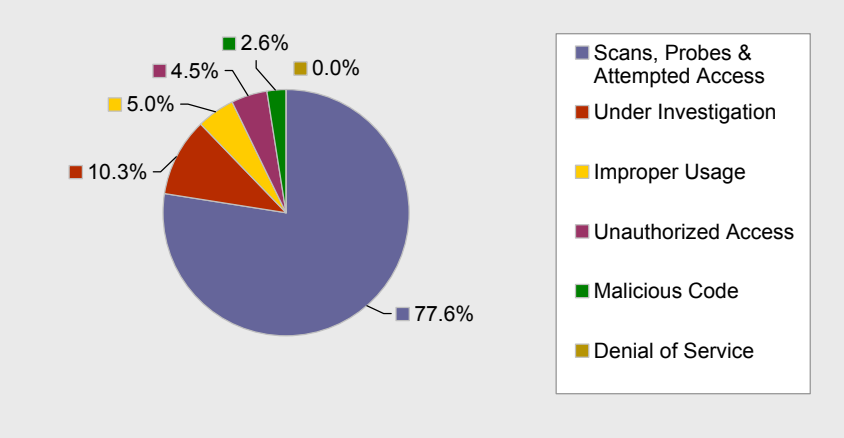
The United States Computer Emergency Readiness Team (US-CERT) publishes a list of the most prevalent cybersecurity trends, metrics, and security indicators

- **Unauthorized Access** - An individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource
- **Denial of Service (DoS)** - An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources; you can be the perpetrator, victim, or unconscious facilitator of a DoS
- **Malicious Code** - Malicious software (e.g., virus, worm, spyware, bot control software, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application); The full extent of malicious code in networks is underreported because agencies are not required to report malicious logic that has been successfully quarantined by antivirus (AV) software
- **Improper Usage** – Term describing any violation of acceptable computing use policies
- **Scans, Probes, & Attempted Access** - Activities that seek to access or identify a federal agency computer, open ports, protocols, service, or any combination thereof for later exploit; this activity does not directly result in a compromise or denial of service
- **Social Engineering/ Phishing:** Criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication

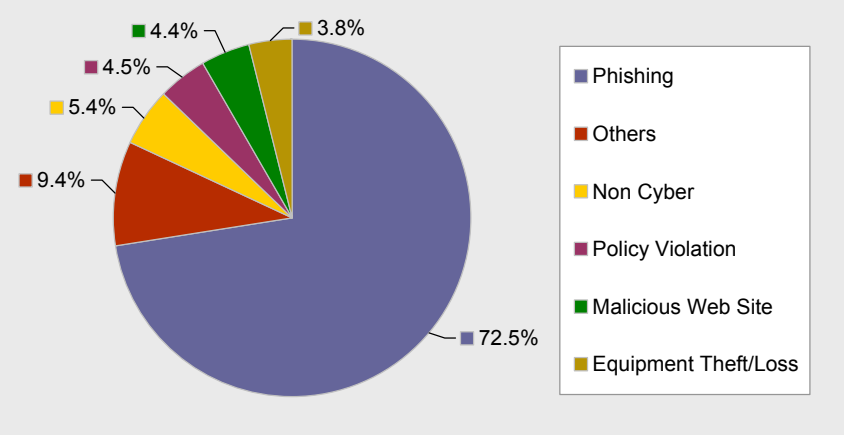
Source: US CERT Quarterly Trends and Analysis FY08 Q2

US-CERT reports that scans, probes, and attempted access constitute the greatest trend in cybersecurity, while phishing accounts for the greatest proportion of incidents

Cyber Trends: FY08 Q2



Cyber Incidents: FY08 Q2



Source: US CERT Quarterly Trends and Analysis FY08 Q2

US Government and Industry are prey to numerous types of cyber attacks that use human engineering techniques or take advantage of Web 2.0 opportunities

WEB 2.0 AND CLIENT-SIDE ATTACKS	▸ Web 2.0 and client-side attacks take advantage of the movement towards interactive websites – Interactive websites – such as blogs, wikis, and social networking sites – allow hackers to embed malicious code on an otherwise legitimate website – Traditional attacks work on these new web applications – Motivators include financial gain, stealing private data, and corporate espionage – Gaining access to individuals' sensitive information on a widespread scale could disrupt the national economy and cause massive confusion and panic
TARGETED MESSAGING ATTACKS	▸ Targeted messaging attacks induce individuals to relinquish sensitive or proprietary information – Attacks pinpoint individual users to steal authentication and private data through e-mail ("phishing"), instant messaging, peer-to-peer (P2P) networks, short message service (SMS) text messages ("smishing"), and Voice over Internet Protocol (VoIP) ("vishing") – A lack of trust on the Internet may challenge the productivity gains users expect from Internet use – If directed at individuals privy to confidential or classified information, these attacks could endanger proprietary interests or national security – Security technologies such as antivirus and anti-spam may continue to make progress in blocking cyber attacks, but as the internet becomes increasingly anonymous and decentralized, traditional security approaches become less effective

Sources: Georgia Tech Information Security Center, Emerging Cyber Threats Report for 2008 October 2, 2007; Top Ten Web 2.0 Attack Vectors by Shreeraj Shah in Help Net Security

US Government and Industry cyber vulnerabilities include malicious software and susceptibilities in cellular networks

BOTNETS	▸ Botnets are networks of computers controlled by a malicious actor, but their lawful owners do not know this – Botnets successfully used to attack the Estonian government in 2007. Their use poses significant challenges – Botnets can be used to coordinate attacks and distribute malware, spam, and phishing scams – Botnets can be used to initiate distributed denial-of-service (DDOS) where a coordinated attack from a system takes up so much of a shared resource that none of the resource is left for other users – Botnets can be formed in P2P networks to avoid detection by traditional systems
VULNERABILITIES TO FIXED MOBILE CONVERGENCE	▸ Fixed mobile convergence vulnerabilities could have a significant impact on cellular and emergency response services – As more users synchronize their desktop computer to their mobile devices, attackers can steal information or commit fraud through smart phones and other mobile devices – Traditional security solutions do not scale well for this environment – The sheer number of users and applications, and the diverse types of carriers require highly customized solutions – Bringing down cellular networks could impact emergency response systems and cause mass confusion

Sources: Georgia Tech Information Security Center, Emerging Cyber Threats Report for 2008, October 2, 2007; "Fixed Mobile Convergence Spawns Security Concerns," Telecom News by Neil Roiter, http://searchtelecom.techtarget.com/news/article/0,289142,sid103_gci1263793,00.html#

The US may be susceptible to radio frequency technologies that can provide access to sensitive materials

RADIO FREQUENCY IDENTIFICATION (RFID) ATTACKS

- RFID attacks could endanger US national security by providing unauthorized access to sensitive materials and locations
  - RFID technologies remotely read sensors over radio frequencies, linking the sensors to a particular ID
  - Analysts expect investments in RFID and sensor networks to fuel an $11.6 billion global market by 2012
  - RFID protocols, frequencies, and formats have been consolidated, making hacking easier
  - Existing countermeasures for RFID vulnerabilities are extremely limited
  - Security has focused on strengthening the encryption of RFID communication and blocking unwanted signals
  - It's possible to walk by someone carrying a RFID-enabled access key and steal the identification and authentication information
  - New U.S. passports employ RFIDs and there is some idea that terrorists could remotely interrogate the passports to identify Americans for attack

Source: Georgia Tech Information Security Center, Emerging Cyber Threats Report for 2008, October 2, 2007

Recent events highlight vulnerabilities associated with external media, such as USB thumb drives

- November 19, 2008 – Symantec's Security Intelligence Analysis Team noted an increase in malicious applications that use USB flash drive devices as a propagation method
- Two popular methods for infecting USB flash drives with malicious code have been observed
  1. Simple File Copy - Malicious code initially resides on an infected computer and copies itself to all the storage devices connected to the affected computer; this method requires the user to access the USB flash drive and execute the malicious code
  2. AutoRun.inf Modification – Malicious code alters or creates an autorun.inf file on targeted storage devices connected to the affected computer; when an infected USB flash drive is connected to another computer, the malicious code can be automatically executed with no additional user interaction

Under Worm Assault, US Military Bans Disks, USB Drives

"…The Defense Department's geeks are spooked by a rapidly spreading worm crawling across their networks. So they've suspended the use of so-called thumb drives, CDs, flash media cards, and all other removable data storage devices from their nets, to try to keep the worm from multiplying any further. The ban comes from the commander of U.S. Strategic Command, according to an internal Army e-mail. It applies to both the secret SIPR and unclassified NIPR nets. The suspension, which includes everything from external hard drives to "floppy disks," is supposed to take effect "immediately." Similar notices went out to the other military services…"

Noah Shactman
Wired Magazine,
November 19, 2008

Source: "Increase in USB-Based Malware Attacks," Symantec, https://forums.symantec.com/syment/blog/article?blog.id=malicious_code&thread.id=220; "Under Assault, US Military Bans Disks, USB Drives," Wired Magazine, http://blog.wired.com/defense/2008/11/army-bans-usb-d.html

Border Gateway Protocol (BGP) security weaknesses allow for the interception of internet traffic

> *"We're not doing anything out of the ordinary…There's no vulnerabilities, no protocol errors, there are no software problems. The problem arises (from) the level of interconnectivity that's needed to maintain this mess, to keep it all working."*
>
> Anton "Tony" Kapela
> Wired Blog, August 26, 2008

The Border Gateway Protocol (BGP) is the core routing protocol of the Internet – It works by maintaining a table of Internet Protocol networks or 'prefixes' which designate network reachability among autonomous systems (AS)

- The tactic exploits the internet routing protocol BGP to let an attacker secretly monitor unencrypted internet traffic anywhere in the world, and even modify it before it reaches its destination
- Anyone with a BGP router could intercept data headed to a target IP address or group of addresses
- The attack intercepts only traffic headed *to* target addresses, not from them, and it can't always vacuum in traffic within a network -- say, from one AT&T customer to another
- To intercept data, an eavesdropper would advertise a range of IP addresses he wished to target that was narrower than the chunk advertised by other networks; the advertisement would take just minutes to propagate worldwide, before data headed to those addresses would begin arriving to his network
- The method conceivably could be used for corporate espionage, nation-state spying or even by intelligence agencies looking to mine internet data without needing the cooperation of Internet Service Providers
- In early 2008, Pakistan Telecom attempted to block customers to YouTube by falsely broadcasting instructions worldwide claiming to be the legitimate destination for anyone trying to reach YouTube's range of Internet addresses

Source: Kim Zetter, "Revealed: The Internet's Biggest Security Hole", Wired Blog, http://blog.wired.com/27bstroke6/2008/08/revealed-the-in.html; http://news.cnet.com/8301-10784_3-9878655-7.html

The SysAdmin, Audit, Network, Security (SANS) Institute has created a list of the top ten cybersecurity menaces for 2008

1. Increasingly sophisticated web site attacks that exploit browser vulnerabilities—especially on trusted websites
2. Increasing sophistication and effectiveness of Botnets
3. Cyber espionage efforts by well resourced organizations looking to extract large amounts of data - particularly using targeted phishing
4. Mobile phone vulnerabilities, especially against iPhones and Android-based phones; plus VoIP
5. Insider attacks
6. Advanced identity theft from persistent bots
7. Increasingly malicious spyware
8. Web application security exploits
9. Increasingly sophisticated social engineering including blending phishing with VoIP and event phishing
10. Supply chain attacks infecting consumer devices (USB thumb drives, GPS systems, photo frames, etc.) distributed by trusted organizations

Source: Top Ten Cyber Security Menaces for 2008, http://www.sans.org/2008menaces/

In recent years, there have been numerous incidences of cyber intrusions and attacks that have gained national and international attention

- The following slides contain examples of reported cyber crimes
  - Hacker Manipulates Radio Station Phones to Win Prizes: 1990
  - T.J. Maxx and Others Hacked Through “War Driving”: 2005
  - Hacker Penetrates Unclassified Office of the Secretary of Defense Email System: 2007
  - World Bank Under Perpetual Cyber Siege Since September 2007
  - Russia Launches Cyber-War on Estonia: 2007
  - Russia Disables Georgian Government Websites: 2007
  - China Scanning and Mapping Indian Networks: 2007-2008
  - McCain and Obama Campaign Networks Hacked: 2008
  - Pro-Tibetan Websites Under Attack from Chinese Government: 2008
  - Sunni Extremists Hack Top Shiite Cleric’s Website: 2008
  - Al Qaeda Propaganda Websites Under Attack: 2008
  - Storm Worm Botnet Continues to Infect Computers and Cause DoS attacks: 2007-Present

Hacking has led to the loss of billions of dollars to industry

Hacker Manipulates Radio Station Phones to Win Prizes: 1990	▸ Kevin Poulsen and two others hacked into LA radio's KIIS-FM phone lines to be the winning caller for numerous promotional events ▸ They were able to win two new Porsches, two Hawaiian vacations, and $20,000 in cash ▸ A notorious "black hat" hacker (a hacker who works to exploit computer systems), Poulsen was featured on Unsolved Mysteries in 1991, and hacked the 1-800 phone lines when his photo appeared, resulting in the collapse of the show's phone system ▸ He was eventually captured and served five years in prison
T.J. Maxx and Others Hacked Through "War Driving": 2005	▸ Eleven people were charged with stealing more than 41 million credit card numbers, the largest hacking and identity theft ring ever exposed ▸ "War driving," the primary hacking method used by the accused, involves hackers driving around and scanning retail wireless networks, looking for security holes ▸ Thieves installed "sniffer" programs tapped into the networks and obtained stored credit, debit, and PIN numbers ▸ The stolen numbers were sent away to computers in the US and Eastern Europe ▸ Christopher Scott, one of the conspirators, "compromised wireless access points at a Marshalls in Miami and used them to download payment information from computers at TJX (the parent company of T.J. Maxx) headquarters" in Massachusetts ▸ TJX says it has spent at least $130 million on legal and other matters related to the security breach

Sources: "Top Ten Most Famous Hackers of All Time" http://www.itsecurity.com/features/top-10-famous-hackers-042407/ April, 24 2007; Brad Stone, "11 Charged in Theft of 41 Million Card Numbers", The New York Times http://www.nytimes.com/2008/08/06/business/06theft.html?_r=1&scp=1&sq=TJ%20maxx%20credit%20card%20theft&st=cse&oref=slogin, August 5, 2008

Cyber vulnerabilities exist within all levels of government, and also affect international organizations

Hacker Penetrates Unclassified Office of the Secretary of Defense Email System: 2007	▸ The Pentagon took down the network for more than a week, although attacks continued despite this action ▸ The system carries "routine mail" involving administrative matters ▸ Secretary of Defense Robert Gates said that the DOD is "under constant attack" ▸ The Financial Times reported that the Chinese Military was responsible ▸ The White House began investigating whether it would be appropriate to restrict BlackBerry use
World Bank Under Perpetual Cyber Siege Since September 2007	▸ Hackers, some of whom have IP addresses originating from China, penetrated the World Bank's highly-restricted treasury unit, extracting mountains of data ▸ An internal memo stated that eighteen servers were compromised, including the Bank's security and password server and a Human Resources server "that contained scanned images of staff documents" ▸ The FBI was brought in to investigate at least six major intrusions ▸ The Bank's computers contained critical inside information on bids, contracts, minutes of confidential board meetings, and the Bank's position on currencies
McCain and Obama Campaign Networks Hacked: 2008	▸ Attacks originated from China, but investigators are not sure if they are the work of the Chinese Government of unaffiliated hackers ▸ The cyber attackers "successfully downloaded large quantities of information from the campaign networks, which security agencies believed was an attempt to learn more about the contenders' policy positions"

Sources: Demetri Sevastopulo, "Chinese hacked into Pentagon", The Financial Times, http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html, September 3, 2007; "Pentagon email hacked", Australian IT, http://www.australianit.news.com.au/story/0,24897,21948818-15306,00.html, June 22, 2007; Richard Behar, "World bank Under Cyber Siege in 'Unprecedented Crisis'", http://www.foxnews.com/story/0,2933,435681,00.html, October 10, 2008; Demetri Sevastopulo," Cyber attacks on McCain and Obama teams 'came from China'", Financial Times, http://www.ft.com/cms/s/0/3b4001e2-ac6f-11dd-bf71-000077b07658.html?nclick_check=1, November 7, 2008

Denial of service is a cyber attack method that is used frequently to impair normal functionality

Russia Launches Cyber-War on Estonia: April-May 2007	▸ There was a three week onslaught of cyber-attacks on Estonian ministries, political parties, banks, companies, and media ▸ The cyber-war erupted after the Estonians removed the Bronzed Soldier Soviet War Memorial in central Tallinn ▸ Estonian officials claimed that one of the masterminds behind the attack was connected to the Russian security service ▸ Target sites were hit by "denial of service" attacks—this involves a site being bombarded with so many fake requests for information that it crashes
Russia Disables Georgian Government Websites: August 2007	▸ Using the same "denial of service" requests used to bring down Estonian websites, Russia disabled Georgian government sites, including the site for the Ministry of Foreign Affairs, before and during the recent armed conflict between the two countries ▸ The National Bank of Georgia website was also defaced at one point with pictures of 20th century dictators and an image of Georgian President, Mikheil Saakashvili ▸ A research director for a nonprofit technical organization that tracks Internet traffic noted that cyber attacks are surprisingly inexpensive—about four cents per machine—and are "almost a certainty in modern warfare"

Sources: Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia, May 17, 2007; "Estonia Under Attack", The Economist, http://www.economist.com/displayStory.cfm?Story_ID=E1_JTGPVJR, May 10, 2007; John Markoff, "Georgia Take a Beating in the Cyberwar with Russia", The New York Times Bits Blog, http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia/, August 11, 2008

Many incidences of national and international cyber attacks have been traced to sources in China

China Scanning and Mapping Indian Networks: 2007-2008	▸ Since early 2007, China has been conducting daily attacks on public and private networks in India ▸ Indian officials say that China is trying to gain "an asymmetrical advantage" ▸ China primarily uses three tactics when hacking into Indian networks: BOTS, key loggers, and mapping of networks – "A BOT is a parasite program embedded in a network that hijacks the network and makes other computers act according to its wishes"; there are close to 50,000 BOTS in India as of May 2008 – Key loggers are "software that scans computers and their processes and data the moment you hit a key on the keyboard"; the data, including password changes, is carried over to an external controller – Mapping of networks allows for the Chinese to obtain critical knowledge of content and how to disable the network should a conflict arise ▸ These tactics could potentially hamper India's decision-making processes
Pro-Tibetan Websites Under Attack from Chinese Government: 2008	▸ "Activists from the International Tibet Support Network were sent emails that appeared to come from sympathetic organizations, with attached documents containing states of support or evidence of human rights breaches by the Chinese Government" ▸ The attachments contained a "trojan," which is installed when the user opens the file, allowing for the computer to be controlled from a remote location ▸ The Chinese Government was the likely culprit as most of the attacks connected back to servers on CHINANet

Sources: "China mounts cyber attacks on Indian sites", The Times of India http://timesofindia.indiatimes.com/China_mounts_cyber_attacks_on_Indian_sites/articleshow/3010288.cms, May 5, 2008; "Net activists in the firing line", http://news.bbc.co.uk/2/hi/technology/7314201.stm, March 26, 2008

There are numerous instances of cyber attacks on international websites

Sunni Extremists Hack Top Shiite Cleric's Website: 2008	▸ The hacked site contained a statement accusing Gran Ayatollah Ali al-Sistani of issuing "perverse" edicts ▸ A video clip featuring comedian Bill Maher was added to the site ▸ Hackers were trying to imply that Maher was issuing an edict—handed down by al-Sistani—on sexual behavior ▸ The extremists claimed that the site was giving "a bad name" to Sunnis
Al Qaeda Propaganda Websites Under Attack: September 2008	▸ Three websites used to broadcast al Qaeda propaganda, al Ekhalas, al Buraq, and al Firdaws, have been closed since September 11, 2008 due to consistent cyber attacks ▸ All three sites are linked to al-Fajr, al Qaeda's media distribution arm ▸ The sites had video clips of martyrdom operations in Iraq, Afghanistan, and other locations ▸ Rumors of "joint Anglo-US operations have surfaced but neither government will confirm involvement"

Sources: "Web site of influential Shiite cleric hacked", http://www.cnn.com/2008/WORLD/meast/09/19/al.sistani.hacked/index.html, September 19, 2008; "Top Shiite cleric's website hacked", http://www.usatoday.com/news/world/iraq/2008-09-20-cleric-website_N.htm, September 20, 2008;
Ian Black, "Cyber-attack theory as al-Qaida websites close", The Guardian, http://www.guardian.co.uk/world/2008/oct/22/alqaida-terrorism-internet, October 22, 2008

Coordinated Botnet attacks have the potential to overwhelm and disable significant portions of the Internet

Storm Worm attacks target computers worldwide: 2007-Present

- Originated in January 2007 – "Storm Worm" spam email attacks were so named because the most common headline associated with early attacks was "230 Dead as Storm Batters Europe"
- Since the original emails, Storm Worm has employed a variety of News-related headlines to trick users to click onto links (e.g. "FBI v. Facebook;" or "Strongest Earthquake hits Beijing")
- Emails contained a malicious payload targeting Windows platforms - Trojan.Peacomm, Win32.Small.DAM, and Win32.Small were most common culprit
- Users are directed to click on links in the targeted email activating the malicious payload and rendering machines part of the "Storm Botnet"
- Unlike Botnets that operate from a central "command and control" network, the Storm Worm Botnet operates Peer-to-Peer, rendering attempts to disable key "central" operators ineffective
- Peer-to-Peer updates allow the Storm Worm to independently alert and retrench the virus within machines as patches and fixes are deployed by antivirus software
- The massive amount of infected computers, on major network providers including SBC, Comcast, and Roadrunner, allow Storm Worm operators to run coordinated DoS attacks overwhelming certain segments of the internet
- It is believed that the Storm Worm's operators are based out of Russia

Sources: ""Storm Worm" http://snopes.com/computer/virus/storm.asp last updated 1 August 2008. "Intelligence Note: Storm Worm Virus" http://www.ic3.gov/media/2008/080730.aspx last updated 30 July 2008; and "Storm Worm Launched on the Internet on the tail of European Storm," http://www.f-secure.com/f-secure/pressroom/news/fs_news_20070119_1_eng.html 19 January 2007

Reference Material

Private industry faces an array of challenges as the volume and sophistication of cyber crimes and cyber attacks increase

KEY CHALLENGES FOR INDUSTRY

- Physical Security
- Commercial Espionage
- Network Resiliency
- Identity Theft
- Database Integrity
- Secure Communication
- Cyber Extortion
- Encryption Technologies

The Financial Services and Commerce industries are prime targets of malicious actors in cyberspace

US-based financial institutions remain the most frequent target for phishing attempts	▸ Of the top 20 companies targeted by phishing in 2007, 19 were in the banking industry ▸ The financial and economic impact of a one-day cyber event targeting US credit and debit card transactions is estimated at $35 billion ▸ In December 2007, a banking Trojan called SilentBanker stole user data from more than 400 banks worldwide
Bank websites are increasingly using Web 2.0 applications that are vulnerable to attack	▸ These websites require authentication that uses Web 2.0 applications ▸ When authentication is complete, the user is given a cookie that is deleted after logging out ▸ If the user keeps the browser open and visits a malicious website, attackers can access the user's and bank's critical information
Spam can be disguised as business content to lure Internet users into phishing schemes in order to gain access to personal information	▸ Identity theft burdens financial institutions that bear the cost of restitution

Sources: Microsoft Security Intelligence Report (January through June 2008); Booz Allen Analysis; Georgia Tech Information Security Center, Emerging Cyber Threats Report for 2008 October 2, 2007, Top Ten Web 2.0 Attack Vectors by Shreeraj Shah in Help Net Security

Instances of cyber attacks on the Telecommunications and Information Technology industries are increasing

- In the US, Trojan Downloaders, like Win32/Zlob, account for the largest single category of vulnerabilities in the Telecommunications and Information Technology industries
- A hacker could program 50 million mobile or VoIP phones to call 911 simultaneously to disable the 911 system
- An attack on WiFi services could bring down entire cellular networks
  - Carriers often have the same core and WiFi networks
  - Since mobile WiFi security lags behind core network security, attacks on WiFi network can damage the core cellular network
  - Viruses can be easily loaded on the WiFi services and then spread to the core network to bring down the entire cellular network
- Critical Infrastructure entities are the preeminent targets for terrorists and foreign military cyber warfare units
  - In May 2007, cyber attacks on a wide range of civilian and government networks in Estonia crippled state-run banks, telecommunications companies and news organizations for weeks

Sources: Microsoft Security Intelligence Report (January through June 2008), Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence." J Michael McConnell, February 5, 2008; Georgia Tech Information Security Center, Emerging Cyber Threats Report for 2008, October 2, 2007; "Fixed Mobile Convergence Spawns Security Concerns," Telecom News by Neil Roiter, http://searchtelecom.techtarget.com/news/article/0,289142,sid103_gci1263793,00.html#

The Transportation industry is vulnerable to several cybersecurity challenges that could lead to severe consequences

The US transportation system infrastructure is a prime cyber target of enemy nations	▸ The sector's size, its physically dispersed and decentralized nature, the many public and private entities involved in its operations, and the critical importance of cost considerations, lead to cybersecurity vulnerabilities ▸ The applications of technology, IT, and telecommunications serve as common threads for networking and communication amongst the transportation industry, and if disrupted by cyber attack, can directly impact the security of the nation
The vulnerability of the Transportation industry to cyber threats varies depending on the type of technology and the extent of its use	▸ Systems with a large number of users are at risk ▸ The use of mobile systems increases the risk ▸ Multiple system access points may be less secure (e.g. two-way radios on trucks and web points)
Manipulation of transportation cyber systems can lead to numerous consequences	▸ Transportation accidents ▸ The release of materials during storage or transportation ▸ Locating shipments to hijack or attack ▸ Diverting shipments to unauthorized destinations ▸ Re-routing shipments through sensitive areas to be attacked ▸ Disrupting the flow of materials ▸ Delaying shipments ▸ Substitution of materials

Source: GTISC, "Emerging Cyber Threats Report for 2009, http://www.gtiscsecuritysummit.com/pdf/CyberThreatsReport2009.pdf; Comprehensive Cyber Security Vulnerability Analysis for Manufacturing Plants © 2004, Primatech Inc.; Volpe Journal 2003: Transportation and Security, http://www.volpe.dot.gov/infosrc/journal/2003/chap1.html

The Energy Sector is vulnerable to a growing number of cybersecurity threats, including those targeting critical infrastructure entities and utility interdependencies

- Critical infrastructure entities, including refineries and pipelines are increasingly threatened by hackers and are the preeminent targets for terrorist and foreign military cyber warfare units
  - Global utility operations are hit by up to an estimated 1,000 hackers/malicious code attacks annually
  - In the past three years, hackers have successfully penetrated multiple utility companies that use Supervisory Control and Data Acquisition (SCADA) systems; they are persistently vulnerable to cyber attack because they are an attractive target, use commercial software that has inadequate security, and are accessible via the Internet
- Cyber extortion is a growing vulnerability in the US, and attackers are now targeting electric, water, oil/gas, and other critical industry assets—online attackers have targeted an electrical grid, disrupting power in several cities
- The US Department of Homeland Security (DHS) demonstrated the "Aurora" Vulnerability of a cyber attack at the Idaho National Laboratory by hacking into a power plant generator and causing it to self-destruct
  - The same attack scenario could be used against generators that produce the country's electric power, with coordinated efforts causing damage that could take months to fix
- Interdependencies could create a cascade effect impacting national security
  - For example, it is thought that in 2003, a worm slowed downstream communication links between utility data centers that may have contributed to a power blackout across the Eastern US

Sources: Forbes.com, "Hackers Cut Cities' Power," 1/18/08; CRS Report for Congress, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," November 15, 2007; "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid, CNN, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html, Sept 26, 2007

ISACs have enabled the coordination of cybersecurity efforts for the Financial Services and Telecommunication industries

Financial Services and Commerce Industry	▸ The Financial Services ISAC (FS-ISAC) was launched in 1999 to establish an information sharing network for cyber and physical threats and vulnerabilities among the public and private financial services sector – Recent completion of the Critical Infrastructure Notification System (CINS) allows the FS-ISAC to speed security alerts to multiple recipients near-simultaneously – Provides an anonymous information sharing capability across the entire financial services industry ▸ The Financial Services Coordinating Council (FSSCC) for Critical Infrastructure Protection and Homeland Security identified the top priorities of its Research and Development Committee to address cyber security concerns, including secure and resilient financial transaction systems, data centric protection strategies, and understanding the human insider threat
Telecommunication and Information Technology Industry	▸ The Communications Sector Coordinating Council (CSCC), established in 2005, facilitates the coordination of sector-wide activities and initiatives designed to improve physical and cyber security of the critical infrastructures and related information flow – Identify, prioritize, and coordinate policy issues related to the protection of critical infrastructure and key resources – Facilitate sharing of information related to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices ▸ Internet Security Alliance (ISA) developed a market-based incentive model for the private industry for internet security as a substitute to Federal government regulation—was turned into a white paper at the request of Congress and DHS

Sources: FS-ISAC, http://www.fsisac.com/about/; FSSCC, https://www.fsscc.org/fsscc/reports/2008/RD_Agenda-FINAL.pdf, 2008; CSCC, http://www.commscc.org/ ; ISA, http://www.isalliance.org/index.php?option=com_content&task=view&id=7&Itemid=49

Steps have been taken within the Transportation and Energy industries to bolster cyber security measures

Transportation Industry	▸ Formation of Information Sharing and Analysis Centers (ISACs) to protect this critical infrastructure from cyber and physical attacks – Provides a vehicle for anonymous or attributable sharing of incident, threat, and vulnerability data – Surface Transportation ISAC and Public Transportation ISAC formed ▸ In November 2008, SRA International Inc. was awarded a $56 million contract from the Federal Aviation Administration to protect the Transportation Department, Federal Aviation Administration, and other organizations from cyber attacks – SRA will assist the Cyber Security Management Center, as the focal point for cybersecurity protection, with cyber-attack prevention, detection and response capabilities
Energy Industry	▸ "The Roadmap to Secure Control Systems in the Energy Sector" is a ten-year public/private collaborative initiative, begun in January 2006, that is aimed at providing cybersecurity for the nation's critical infrastructure ▸ To increase the security and reduce the risk of a successful attack, the utility industry is implementing eight mandatory cybersecurity standards approved by the Federal Energy Regulatory Commission ▸ Nexant Inc., a global energy software and consulting firm, and Promia, Inc., a developer of Enterprise Cyber Security and Asset Monitoring products, announced a partnership to deliver products and services supporting the FERC and Electric Reliability Organization (ERO) Critical Infrastructure Protection Standards (CIPS) for energy companies

Sources: Washington Technologies, http://www.washingtontechnology.com/online/1_1/33852-1.html, 2008; ISAC, http://www.surfacetransportationisac.org/, 2008; FERC, http://www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.asp, 2008; cnet, http://news.cnet.com/8301-13578_3-10040101-38.html?tag=mncol;txt, 2008; Automation World, http://www.automationworld.com/feature-4222, 2008; Reuters, http://www.reuters.com/article/pressRelease/idUS175607+25-Aug-2008+BW20080825, 2008

The Defense Industrial Base (DIB) presents a variety of national security concerns which underscore its importance in the field of cyber security

- Cyber sabotage is a new element in the emerging cyber threats to the DIB
  - In July 2007 a deliberate act of sabotage to a computer on the shuttle Endeavour was caught before the equipment was loaded onto the spacecraft
- Cyber espionage presents a recurring threat as nation-states use data theft to gain economic advantage in multinational deals
  - China has attempted to collect information on US military programs such as “quiet drive” technology that helps submarines evade detection
- It is possible that DIB targets may not yet be fully appreciated by cyber terrorists and state actors
- To increase the security of the DIB, the defense industry is working together with DOD to establish more secure software standards
- Many commercial firms are taking steps such as deploying data-leak prevention products
  - Tools monitor data that leaves the organization as well as helping to establish appropriate access controls procedures

Source: Defensetech.org/archives/cat_cyberwarfare.html

Several key public and private partnerships have been established to address cyber security…

Organization	Cybercrime Purpose	Primary stakeholders
Internet Crime Complaint Center	A partnership between the FBI and the National White Collar Crime Center serves as a means to receive Internet-related criminal complaints, further research and development, and refer criminal complaints to law enforcement and government agencies	Federal, state, local, or international law enforcement and/or regulatory agencies
InfraGard	An information sharing and analysis effort established by the FBI to protect physical and cyber-based critical infrastructure assets	Federal, state, and local law enforcement agencies, academia, private industry, and other government agencies
The National Cyber Security Alliance	A partnership established by the federal government to provide cyber security awareness and education resources for the home user, small business, and education audience	DHS, FTC, and private-sector corporations and organizations
National Cyber Forensics and Training Alliance	A partnership established by the FBI, the National White Collar Crime Center, and Carnegie Mellon and West Virginia Universities to provide a venue to share critical confidential information about cyber incidents and share resources	Industry, academia, and law enforcement
Electronic Crimes Task Forces	Established by the Secret Service to create strategic alliances among various stakeholders	Federal, state, and local law enforcement agencies and private-sector entities

Sources: Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO-07-705, June 2007

…by bringing together best practices from both government and industry

Organization	Cybercrime Purpose	Primary stakeholders
Cyber Initiative and Resource Fusion Unit	A spin-off of the IC3 that follows the early investigative trail in some complex technical cases. Center analysts eliminate false leads and refine a case before it is referred to a local or international law enforcement agency or task force. The center is supported by online organizations and merchants. Federal agents and analysts from industry and academia work together to find out where the crime originates, who is behind it, and how to fight it. They identify Internet crime trends and technologies, develop significant cases, and help law enforcement agencies worldwide identify and combat Internet crimes	Federal, state, and local law enforcement agencies, academia, private industry, and other government agencies
Anti-Phishing Working Group	An association focused on eliminating fraud and identity theft that result from phishing, pharming, and e-mail spoofing of all types	Private industry, academic institutions, and law enforcement agencies
SEARCH	A nonprofit membership organization that has developed extensive programs to assist justice and public safety agencies. Their cyber crime efforts support law enforcement by providing a High-Tech Crime Training Program, technical assistance, and research into emerging technology issues	State and local law enforcement agencies, first responders, and prosecutors
The Business Software Alliance	A nonprofit trade association dedicated to promoting a safe and legal digital world. It is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce.	Commercial software and computer hardware industry
Cybercrime Institute	A collaborative venture in Georgia with Kennesaw State University and the FBI, the Georgia Bureau of Investigation, the State Attorney General's Office, the Georgia Technology Authority, and the National White Collar Crime Agency to provide education and training in the fight against cyber crime	Professionals in governmental agencies, law enforcement, corporations, universities, and colleges

Sources: Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO-07-705, June 2007

Reference Material

The US Government's federal network, which controls classified information, nuclear weaponry, and some critical infrastructure, is vulnerable to cyber attack

"It has been ten years since the first reports called attention to America's vulnerability in cyberspace…those who wish to do harm to the US have not failed to notice the opportunities created by the weaknesses of US networks. There has been damaging losses of valuable information…in both the government and the private sector, creating major risks for national security and doing major damage to US global competitiveness. Cyber security is now one of the most important national security challenges facing the US…the US is not organized and lacks a coherent national strategy for addressing this challenge."

James Lewis, Center for Strategic and International Studies
Statement before the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
Cyber Security Recommendations for the Next Administration
September 16, 2008

- The government has had continued challenges in building a comprehensive national cyber response capability
- There is continued concern surrounding the definite possibility of a coordinated cyber attack on critical infrastructure, classified information, air traffic control, financial sectors, and nuclear weapons laboratories

Sources: Center for Strategic and International Studies, http://www.csis.org/media/csis/congress/ts080916_lewis.pdf; GAO, "DHS Needs to Fully Address Lessons Learned from It's First Cyber Storm Exercise," September 2008; "Public and Private Entities Face Challenges in Addressing Cyber Threats," June 2007

Departments and agencies across the government are all facing challenges associated with their unique cyber vulnerabilities

Examples of Vulnerabilities Include:

- The US Department of Defense (DOD) uses commercial hardware and software in core IT functions and in combat systems for all services
  - Commercial Off-The-Shelf (COTS) products lack adequate security and often become insecure when coupled to each other
  - Strengthening security to military standards is often too difficult and costly for commercial vendors; thus, vendors release products with errors that create system vulnerabilities
- Cyber security vulnerabilities at power plants and in telecommunications are amongst the most prevalent
  - Government-controlled SCADA systems are frequently used to regulate critical infrastructure and are consistently vulnerable to cyber attack
  - SCADA components are often unmanned, located in remote locations, and accessed only periodically; however, they are often linked to local area networks or the Internet
- Potentially, the highest impact cyber attack would result from penetration of US nuclear weapons laboratories or stockpiles
  - Los Alamos National Laboratories (LANL), one of three labs that designs nuclear weapons and carries out sensitive national security missions, has experienced several significant security breaches over the past decade, including those that inadvertently released highly classified nuclear weapons material, either by email or stolen equipment

Sources: GAO, "Challenges in Developing a Public/Private Recovery Plan," October 2007; CRS Report for Congress, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," November 15, 2007; Andy Greenberg, Forbes, "Congress Alarmed at Cyber Vulnerability of Power Grid," May 2008; GAO, "Los Alamos National Laboratory Faces Challenges in Sustaining Physical and Cyber Security Improvements," September 2008

The Comprehensive National Cybersecurity Initiative (CNCI) guides Federal efforts to protect against cyber attacks

- Presidential Directive 54/ Homeland Security Presidential Directive 23, signed in January 2008 by President Bush, is more commonly known as the CNCI
  - CNCI is a multi-agency, multi-year plan that lays out twelve steps to securing the federal government's cyber networks
  - It is intended to strengthen the Federal Government's ability to secure the electronic networks and databases upon which it relies
  - It requires DHS to coordinate efforts to protect the cybersecurity for the Nation's critical infrastructure
  - CNCI serves as a continuation of Federal efforts to secure government networks, protect against intrusion attempts, address vulnerabilities and anticipate future threats
- Analysts estimate that it will cost as much as $40 billion to implement the CNCI

Sources: DHS, Michael Chertoff, "Response to Chairman Lieberman's and Senator Collins' Questions Regarding the National Cyber Security Center," 18 July 2008; Stephanie Condon, "DHS stays mum on new 'Cyber Security' center," CNET, 31 July 2008; "National Cyber Security Initiative will have a Dozen Parts," NEXTGOV, 1 August 2008

The National Cyber Security Center (NCSC) was created to oversee and coordinate the efforts of the CNCI

- The National Cyber Security Center (NCSC), run by DHS, was created to oversee the actions of the CNCI, and will serve as the focus for improving federal government network defenses
- DHS has requested an additional $83 million for the NCSC for FY09 on top of the $115 million already awarded to the Center in 2008, and tripling the amount the DHS has spent on cyber security since 2007
- The creation of the NCSC marked the first time that the government's efforts in cybersecurity will run through a single office tasked with coordinating the work of separate federal cybersecurity organizations
  - It will serve as a single, central location for all-source awareness about cyber activity and security, coordinating and integrating information to secure US cyber networks
  - It will foster collaboration amongst Federal cyber entities responsible for various parts of the cyber security mission
- Rod Beckstrom, a well-known technology entrepreneur, was appointed as the Center's Director in March 2008

Sources: DHS, Michael Chertoff, "Response to Chairman Lieberman's and Senator Collins' Questions Regarding the National Cyber Security Center," 18 July 2008; Stephanie Condon, "DHS stays mum on new 'Cyber Security' center," CNET, 31 July 2008; "National Cyber Security Initiative will have a Dozen Parts," NEXTGOV, 1 August 2008

The CNCI is composed of a dozen components designed to better protect computer networks and systems

Several components/projects have been identified:

Trusted Internet Connections (TIC)	▸ The most established component of the initiative ▸ Designed to reduce the number of external connections that federal agencies have to the Internet to a few centralized gateways that can be better monitored for security – The number of connections was reduced from 4,300 to 2,700 between January and June – The target is less than 100 connections
Einstein II	▸ Einstein is a system that automatically monitors traffic on government networks for potential threats – Einstein II will serve as an upgraded system which will include intrusion-detection technology – Under CNCI, participation in Einstein for federal agencies managing Internet access will no longer be voluntary – If Einstein II finds a connection is not being properly managed, DHS will be able to shut it down
Federal Desktop Core Configuration (FDCC)	▸ Mandates that agencies adopt a common security protocol for their desktop systems ▸ As part of the CNCI, the NIST proposed in February to extend the FDCC to other operating systems, applications and network devices beyond the existing support for Windows XP and Vista

Sources: "National Cyber Security Initiative will have a Dozen Parts," NEXTGOV, 1 August 2008; Brian Robinson, "Unlocking the National Cybersecurity Initiative," FCW, 22 September 2008; "National Cybersecurity Initiative R&D Effort Launched, October 14, 2008, http://www.fcw.com/online/news/154063-1.html

Although much of the CNCI remains classified, future components will address a range of cybersecurity issues

National Cyber Leap Year	▸ Seeks the most promising game-changing ideas with the potential to reduce vulnerabilities to cyber exploitations by altering the cybersecurity landscape ▸ Comprised of dual goals of forming a national research and development agenda that identifies the most promising technologies and how to bring them to fruition, and to jump-start game-changing, multidisciplinary efforts ▸ The Leap Year will run during FY09 ▸ The first stage of the project involves surveying the cybersecurity community for ideas, while the second phase involves a series of workshops to develop the best ideas
"Project 12"	▸ Will assemble a group of industry leaders to help DHS issue a report on how the government should work to protect the larger cyber infrastructure

- Other components are aimed at making improvements in the following areas:
  - Intrusion Detection
  - Intrusion Prevention
  - Research and Development
  - Situational Awareness
  - Cyber Counterintelligence
  - Classified Network Security
  - Cyber education and training
  - Implementation of information security technologies
  - Deterrence strategies
  - Global supply chain security
  - Public/private collaboration

Sources: "National Cyber Security Initiative will have a Dozen Parts," NEXTGOV, 1 August 2008; Brian Robinson, "Unlocking the National Cybersecurity Initiative," FCW, 22 September 2008; "National Cybersecurity Initiative R&D Effort Launched," October 14, 2008, http://www.fcw.com/online/news/154063-1.html

Cybersecurity responsibility is dependent upon the sector affected and falls under a variety of government departments and agencies

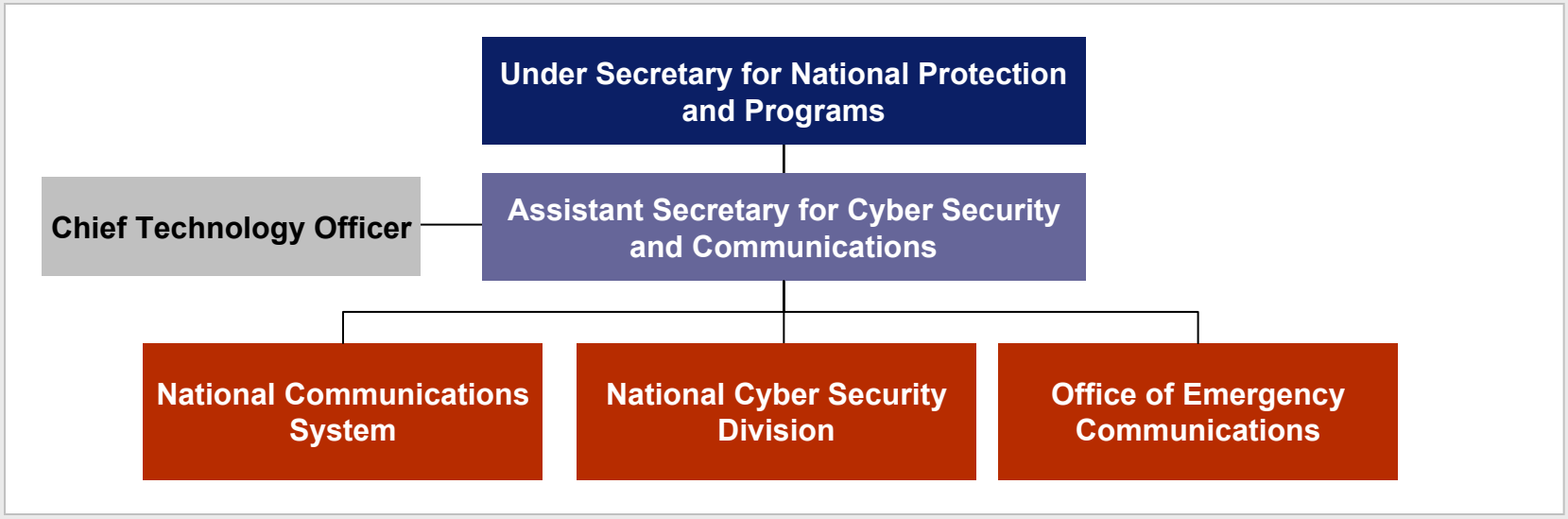
Sector Affected	Agencies and Departments with Primary Responsibility	
Civilian Defense	DHS NIST NSA	FBI DNI STRATCOM
Commercial Defense	DHS FBI Treasury Commerce	NIST NSA DNI STRATCOM
Intelligence/Military Defense	DHS (CONUS) DOD (OCONUS) DNI STRATCOM	NSA FBI State

- The President coordinates cybersecurity through the Assistant to the President for Homeland Security and the Assistant to the President for National Security
- DHS has been designated as the "lead agency" in the overall development of cyber capabilities
  - Other agencies support DHS in this effort and can sometimes take a lead role depending on the affected sector

Source: Interview with Booz Allen Subject Matter Expert

The Department of Homeland Security is the lead agency responsible for the Nation's cybersecurity

- DHS's cybersecurity mission is organized beneath the Under Secretary for National Protection and Programs, and is led by the Assistant Secretary for Cyber Security and Communications (CS&C)
- CS&C is tasked with ensuring the security, resiliency, and reliability of cyber and communications infrastructure
- CS&C is focused on preparing for and responding to catastrophic incidents involving our nation's Information Technology (IT) and communications infrastructure
- Three key entities carry out DHS's cyber security mission:
  - National Cyber Security Division (NCSD)
  - National Communications System (NCS)
  - Office of Emergency Communications (OEC)



Source: US Department of Homeland Security, www.dhs.gov

DHS has several programs aimed at preventing attacks and intrusions

- **US Computer Emergency Readiness Team (US-CERT):** DHS's 24/7 watch and warning center for the Federal Government's Internet infrastructure
- **Einstein Program:** Identifies unusual network traffic patterns and trends that might signal unauthorized network activity
- **Trusted Internet Connections Initiative:** Aims to consolidate the number of external connections for the Federal Government's Internet infrastructure
- **National Cyber Security Center (NCSC):** Brings together and coordinates Federal cybersecurity organizations and activities
- **National Infrastructure Protection Plan:** Facilitates coordination and information sharing between the government and private sector to reduce cyber risks, disseminate information, share best practices, and apply appropriate protective actions
- **Cyber Storm:** National exercise that brings together participants from government, the private sector, and the international community to strengthen the nation's cybersecurity capabilities
- **Critical Infrastructure Partnership Advisory Council (CIPAC):** Facilitates coordination between Federal infrastructure protection programs with the infrastructure protection activities of the private sector, and of state, local, territorial, and tribal governments

Source: "Protecting our Federal Networks against Cyber Attacks," US Department of Homeland Security, www.dhs.gov; "Critical Infrastructure Partnership Advisory Council," dhs.gov

The Secret Service lends supportive capabilities in investigating cyber crimes

- The Secret Service investigates crimes that are a threat to the country's financial infrastructures
  - Emphasis is placed on computer fraud, cyber crime, identity theft, and other types of electronic crime
- The Secret Service has a variety of programs specifically designed to combat and respond to cyber crimes
  - **Electronic Crimes Special Agents** investigate cyber crime, network intrusions, and conduct cyber forensics
  - **Electronic Crimes State and Local Programs** train law enforcement officers to investigate cyber crime
  - **Electronic Crimes Task Forces** creates strategic alliances among Federal, State, and Local law enforcement agencies and private sector entities to investigate and prevent electronic crime by increasing resources and sharing information
  - **Criminal Intelligence Section** is the central repository for data generated through Secret Service field investigations, open source Internet content, and information obtained through financial and private industry partnerships; monitors developing technologies to prevent attacks against the financial infrastructure
  - **Central National Computer Forensic Institute** serves as a national cyber crimes training facility where police officers, prosecutors and judges will receive training and equipment

Sources: US Secret Service, www.secretservice.gov; "Homeland Security Creates National Computer Forensics Institute," Information Week, 12 March 2007

Multiple offices and agencies within DOD play a role in cybersecurity

- Within the Office of the Secretary of Defense (OSD), several offices have cyber roles and responsibilities
  - Under Secretary of Defense for Acquisitions, Technology & Logistics (USD/AT&L)
  - Under Secretary of Defense for Policy (USD/P)
  - Under Secretary of Defense for Intelligence (USD/I)
  - Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer (ASD/NII/DOD CIO)
- Three directorates within the Joint Staff have critical cyber responsibilities
  - Joint Staff, J-3 Operations Directorate
  - Joint Staff, J-5 Strategic Plans and Policy Directorate
  - Joint Staff, J-6 Command, Control, Communications and Computer Systems Directorate
- One Combatant Command coordinates the military's role in cyber affairs
  - US Strategic Command (USSTRATCOM)
- Two defense agencies also support the cyber priorities of the Secretary of Defense
  - National Security Agency (NSA)
  - Defense Information Systems Agency (DISA)

Source: Booz Allen Analysis

Within the Office of the Secretary of Defense (OSD), cyber responsibilities are divided amongst four key offices

Acquisition, Technology and Logistics (AT&L) Office	Policy Office	Networks and Information Integration (NII) Office	Director for IO and Strategic Studies Office
▸ AT&L is responsible for making any major purchases related to cybersecurity	▸ The Under Secretary of Defense for Policy (USD/P) develops cyber policy for DOD ▸ Within this office, the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD/HD) is gaining increasing cyber authority	▸ NII's primary mission is to enable net-centric operations ▸ NII works with DNI to improve interoperability and information sharing between DOD and the Intelligence Community	▸ Within USD/Intelligence, the Director for Information Operations and Strategic Studies (DIOSS) plays a critical role in analyzing many elements of cyber security

Sources: Office of the Secretary of Defense, http://www.defenselink.mil/policy/sections/policy_offices/hd/faqs/homelandDefense/index.html; DoD CIO http://www.defenselink.mil/cio-nii/; Interview with Booz Allen Subject Matter Expert

Within the Joint Staff, J-3, J-5 and J-6 lead the military's operational response to cyber activity

Joint Staff, J-3 Operations Directorate

- J-39 Deputy Directorate for Strategic Operations-Information Operations/Cyber (DDSO-IO/Cyber) is responsible for cyber operations in the global network

Joint Staff, J-5 Strategic Plans And Policy Directorate

- J-5 is responsible for long-range cyber planning

Joint Staff, J-6 Command, Control, Communications And Computer Systems Directorate

- Develops an "implementation plan" to complement the classified National Military Strategy for Cyberspace Operations
  - This plan details the Pentagon's acquisitions for cyberspace operations equipment and services
  - It also includes a common lexicon to standardize cyberspace terminology

Sources: Joint Staff, www.jcs.mil; Interview with Booz Allen Subject Matter Expert; "Joint Staff Readies Cyber Operations Plan" Federal Computer Week, September 7, 2007

USSTRATCOM leads DOD's cyber missions and executes offensive and defensive computer operations

USSTRATCOM Cyber Mission
▸ Operates and defends the Global Information Grid to assure net-centric capabilities in support of DOD's war fighting, intelligence, and business missions ▸ Coordinates, plans, and executes the military's offensive and defensive computer network operations ▸ Initiates military operations in connection with cyber attacks ▸ Command lines established from the Secretary of Defense to Commander, USSTRATCOM, to the Joint Functional Component Command – Network Warfare (JFCC-NW), to each of the appointed Component Commanders within the Military Services

USSTRATCOM Entity	Cyber Focus
Joint Functional Component Command-Network Warfare (JFCC-NW)	▸ Facilitates cooperation with other government entities in network defense ▸ Mounts offensive computer network attacks
Joint Task Force-Global Network Operations (JTF-GNO)	▸ Ensures the availability and security of the systems and networks operated by the Services, Commands, and DOD civilian agencies ▸ Controls the GIG through operations and security centers ▸ Develops technologies to assure system and network availability, information protection, and information delivery

Sources: "Joint Task Force-Global Network Operations" US Strategic Command Fact Sheet, www.stratcom.mil; "US Military's Elite Hacker Crew," John Lasker, Wired Magazine; "Defending the Nation's Resources in Cyberspace," Jeremy Singer, Space News; "Global Network Guardians," Patrick Chisholm Military, Information Technology

DISA and NSA support network information systems' security

Defense Information Systems Agency (DISA)	▸ Plans, engineers, acquires, fields, and supports global net-centric solutions for the President, Vice President, the Secretary of Defense, and other DOD components ▸ Guarantees military forces' global information dominance and delivers the enabling capability to conduct network-centric operations ▸ Supports emerging national-level and DOD cyber security requirements ▸ Information Assurance division defines standards for classified systems across the US Government
National Security Agency (NSA)	▸ Partners with the National Institute of Standards and Technology (NIST) to characterize cyber vulnerabilities, threats, and countermeasures, and to provide practical cryptographic and cyber security guidance ▸ Partners with DHS to sponsor the National Centers of Academic Excellence Program to support the nation's cyber security needs and increase the efficiency of other Federal cyber security programs ▸ Supports the DHS National Cybersecurity Division (NCSD) in its mission to identify, analyze, and reduce cyber threats and vulnerabilities

Sources: DISA, www.disa.mil; "Future Defense Department Cybersecurity Builds on the Past," Lt. Gen. Harry D. Raduege Jr., USAF (Ret.), Signal Magazine, February 2008; Testimony of the National Security Agency's Information Assurance Director Before the Senate Homeland Security and Government Affairs Subcommittee on Federal Financial Management, Government Information, and International Security, July 28, 2006

The DOD Cyber Crime Center (DC3) serves as the focal point for incident reporting and computer emergency response

- Sets standards for digital evidence processing, analysis, and diagnostics for any DOD investigation that requires computer forensic support to detect, enhance, or recover digital media, including audio and video
- Assists in criminal, counterintelligence, counterterrorism, and fraud investigations of the Defense Criminal Investigative Organizations (DCIOs) and DOD counterintelligence activities
- DC3 Mission:
  - Digital evidence processing and electronic media analysis for criminal law enforcement and DOD counterintelligence investigations
  - Investigation and forensic training to DOD members to ensure that systems are secure from unauthorized use
  - Remain on the cutting edge of research, development, testing, and evaluation
  - Serves as the focal point and clearinghouse for Defense Industrial Base incident reporting and computer emergency response actions as part of the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council initiative
- To accomplish its mission, DC3 consists of:
  - The Defense Computer Forensics Laboratory (DCFL)
  - The Defense Cyber Investigations Training Academy (DCITA)
  - The Defense Cyber Crime Institute (DCCI)

Source: DOD Cyber Crime Center, http://www.dc3.mil/home.php

Under CNCI, DARPA is required to create a cyber warfare range, wherein scientists can try out new forms of electronic combat

- The Defense Advanced Research Projects Agency (DARPA) is the central research and development organization for DOD
- DARPA manages and directs research and development projects for DOD, and pursues research and technology where risk and payoff are both very high and where success may provide dramatic advances for military roles and missions
- DARPA's "National Cyber Range" would create a virtual environment where DOD can replicate real cyber warfare—both defensively and offensively
- DARPA envisions the range as a test site where the government can:
  - Conduct unbiased, quantitative and qualitative assessment of information assurance and survivability tools in a representative network environment
  - Replicate complex, large-scale, heterogeneous networks and users in current and future DOD weapon systems and operations
  - Enable multiple, independent, simultaneous experiments
  - Enable realistic testing of Internet/Global-Information-Grid (GIG) scale research
  - Develop and deploy revolutionary cyber testing capabilities
  - Enable the use of the scientific method for rigorous cyber testing

Sources: "National Cyber Range Proposers' Day Workshop," FedBizOpps.gov; Sharon Weinberger," Darpa's New 'Space Race'," Wired, 1 May 2008.

The Intelligence Community plays a significant role in the cyber security of the nation

- The Director of National Intelligence (DNI) coordinates efforts to identify the source of cyber-attacks against government computer systems
- The Central Intelligence Agency (CIA) investigates intrusions by monitoring Internet activity and, in some cases, capturing data for analysis
- The Federal Bureau of Investigation (FBI) is the lead federal agency for the investigation of cyber crime
- The Defense Intelligence Agency (DIA) has a variety of cyber responsibilities, including:
  - Providing Global Information Grid (GIG) threat assessments and conducting GIG risk assessments for the OSD, Joint Staff, and Combatant Commanders/Services/Agencies (CC/S/A), and field activities
  - Analyzing foreign threat capabilities to conduct Information Operations (IO) (e.g., electronic warfare (EW), propaganda, and computer network attack (CNA)) and intelligence operations (e.g., electronic support, signals intelligence (SIGINT), and computer network exploitation (CNE))
  - Providing precise and timely intelligence on IO threat capabilities against DOD information, information systems, and interconnections with foreign partners
  - Providing intelligence and analytical support to determine attribution for reported incidents and unauthorized activities on the DOD networks
  - Analyzing the global cyber-threat environment to achieve predictive analysis of foreign activities against the GIG

Source: "Bush Expands Network Monitoring," Washington Post, January 26, 2008 "Chairman Of The Joint Chiefs Of Staff Instruction," August 15, 2007 http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

The Department of Justice (DOJ) combats electronic penetrations, data thefts, and cyber attacks on critical information systems

Computer Crimes and Intellectual Property Section (CCIPS)	▸ Works with other government agencies, the private sector, academia, and foreign counterparts to prevent, investigate, and prosecute computer and intellectual property crimes ▸ Trains Federal, State, and local law enforcement agents, prosecutors, and other government officials on cyber crime-related topics ▸ Develops policy and legislation to enhance the government's ability to combat cyber crime
Counterterrorism and Counterintelligence Bureaus	▸ Addresses cybersecurity when carried out by terror groups or foreign intelligence agencies
Fraud Section	▸ Investigates and prosecutes fraud offenses involving misuse of computers/Internet ▸ Coordinates with other government departments and law enforcement agencies in investigating and prosecuting Internet fraud ▸ Provides training for Federal, State, and local law enforcement agencies ▸ Participates in multilateral law enforcement meetings on Internet fraud and identity theft
US Attorneys Office—Computer Hacking and Intellectual Property (CHIP) units	▸ Prosecutes high-technology offenses, including computer hacking, virus and worm proliferation, and Internet fraud ▸ Offers training programs to increase expertise among Federal, State, and Local prosecutors ▸ Provides advice to prosecutors and law enforcement on the collection of digital evidence, cyber crimes, and intellectual property laws

Sources: US Department of Justice, www.doj.gov; Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO-07-705 June, 2007

The Federal Bureau of Investigation is an active participant in cyber security efforts

- The CNCI created a new, national-level organization, the National Cyber Joint Investigative Task Force (NCJITF), to coordinate all cyber investigations
- NCJITF is led by the FBI and is the first-ever interagency coordinated investigative system for cyber incidents
- The FBI sponsors InfraGard, a cutting-edge public and private alliance committed to information sharing and analysis to combine the knowledge base of a wide range of members
  - InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States
  - InfraGard Chapters are geographically linked with FBI Field Office territories
  - Currently, there are over 20,000 individual Infraguard members, representing 240 Fortune 500 companies and all national critical Infrastructure sectors

The Department of the Treasury and the Internal Revenue Service are responsible for protecting the financial services industry and internal cyber infrastructure

The Treasury's mission is to protect critical infrastructure for the financial services sector, which includes the protection of cyber-based infrastructures and resources

- **The Office of Terrorism and Financial Intelligence (TFI)** aims to safeguard the financial system against cyber threats through its intelligence and enforcement functions
- **The Financial and Banking Information Infrastructure Committee (FBIIC)** coordinates the efforts of Federal and State financial regulators to improve the resilience of the US financial system in the event of a cyber attack on critical infrastructure
- **The Financial Services Sector Coordinating Council (FSSCC)** facilitates the coordination of sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection (CIP)/Homeland Security
- **The Financial Services Information Sharing and Analysis Center (FS-ISAC)** provides a database, tools and information sharing facilities to submit reports about threats, vulnerabilities, incidents and solutions
- **Treasury Bureaus** provide cyber policy and guidance for the protection of financial institution, corporate, and taxpayer information and the internal resources involved in governmental cash flow

The Internal Revenue Service (IRS) aims to protect cyber infrastructure to maximize availability for tax collection

- The IRS is responsible for:
  - Policy guidance, tools and incidence management to minimize the impact of intrusions and data spills
  - Protecting taxpayer information and reducing fraud through partnerships with external tax collection service providers
  - Tracking and mitigating fraudulent preparer and phishing sites
  - Providing guidance and oversight to state agencies as related to the protection of tax payer information

Sources: US Department of the Treasury, http://www.treas.gov/offices/; http://www.fbiic.gov/; http://www.fbiic.gov/; https://www.fsscc.org/

The Department of Energy's cyber security program aims to improve mission success while protecting networks

Cyber Mission	▸ An agile, effective, and cost-efficient approach to cyber security aligned with current threats and to enable improved Department of Energy (DOE) mission success while strengthening the protection of systems and data
Strategic Goals	▸ Protect DOE information and information systems to ensure that the confidentiality, integrity, and availability of all information is commensurate with mission needs, information value, and associated threats ▸ Enable advanced cyber security capabilities ▸ Develop a workforce knowledgeable about cyber security ▸ Improve cyber security situational awareness
Challenges	▸ The Audit Report of the DOE Inspector General on the Department's Cyber Security Incident Management Program found the following challenges to its success: – DOE has eight independent cyber security organizations whose missions and functions were at least partially duplicative and not well coordinated – The Department had not adequately addressed known issues in its cyber security incident management and response programs through policy changes

Sources: "US Department of Energy Cyber Security Program Cyber Security Strategic Plan" February 12, 2007 http://cio.energy.gov/documents/Cyber_Security_Strat_Plan.pdf; "Audit Report: The Department's Cyber Security Incident Management," DOE, http://www.ig.energy.gov/documents/IG-0787.pdf

The Federal Energy Regulatory Commission regulates the cybersecurity operations at US electric and gas utilities

The Federal Energy Regulatory Commission develops cybersecurity standards for the US power grid

Key Activities	▸ In January 2008, the Federal Energy Regulatory Commission (FERC) approved eight mandatory critical infrastructure protection (CIP) standards intended to protect the nation's bulk power system against potential disruptions from cyber security breaches – The eight CIP reliability standards address the following topics: critical cyber asset identification, security management controls, personnel and training, electronic security perimeters, physical security of critical cyber assets, systems security management, incident reporting and response planning, and recovery plans for critical cyber assets – The ruling also directs FERC to monitor the development and implementation of cyber security standards by the National Institute of Standards and Technology (NIST) ▸ Although FERC has taken actions to improve cyber security practices and implemented protective measures, the Evaluation Report: The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2008, revealed that deficiencies may challenge the ability to reduce those risks – Systems were authorized to operate without sufficient testing of mandatory cybersecurity measures – Cyber security incidents were not always handled and reported in accordance with Federal requirements – A number of network accounts had not been terminated as required – Roles and responsibilities for individuals with significant development or cybersecurity functions had not been properly segregated

Source : FERC, http://www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.asp; http://www.ig.energy.gov/documents/IG-0802.pdf

The Nuclear Regulatory Commission has regulatory authority over nuclear facilities in the US

The US Nuclear Regulatory Commission develops cybersecurity mandates for securing its regulated nuclear facilities

Key Activities	▸ The US Nuclear Regulatory Commission (US NRC) has issued a series of cybersecurity advisories and orders requiring nuclear power plants to take certain actions, including enhancing protection of their computer systems ▸ Several new rulemakings are proposing further cyber security requirements – One proposed rule would require nuclear power plants to implement strategies to protect computer systems, detect cyber attacks, and isolate and neutralize cyber intruders – Computer systems that help operate the reactors and other power reactor safety equipment are isolated from the internet to protect against outside intrusion ▸ As suggested by the Energy Policy Act of 2005, the NRC added a cyber threat component to the Design Basis Threat (DBT) in January 2007 ▸ The NRC routinely interacts with the DHS's National Cyber Security Division to coordinate federal cyber security activities in the nuclear sector

Source : US NRC, http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/security-enhancements.html, October 2008

The Department of Transportation ensures the security of the Nation's transportation infrastructure against cyber attacks

Department of Transportation's Cyber Security Responsibilities	
▸ Implement cybersecurity programs to protect Department of Transportation (DOT) systems integrated with the national critical infrastructure ▸ Develop policies, regulations, and best practices to ensure the security of information networks	
DOT Entity	**Cyber Focus**
Federal Aviation Administration	▸ Establishes policies for information sharing and security of information networks ▸ Manages information integrity to ensure the security of civil and military aviation operations ▸ Adapts DOD standards, protocols, and practices for net-centric operations
Federal Motor Carrier Safety Administration	▸ Protects the accuracy and integrity of its data ▸ Works with system owners to solve identified security issues
National Highway Traffic Safety Administration	▸ Works with States to implement the Real ID Act, which will require them to operate a secure licensing system, ensuring the integrity of the driver license in proving identity in financial, security, and other transactions
Research and Innovation Technology Administration	▸ Safeguards Intelligence Transportation Systems (ITS) and data and other transportation-related computer controlled systems against interference, destruction, and misuse

Source : US Department of Transportation, http://www.dot.gov/stratplan2008/strategic_plan.htm

The Department of Commerce's National Institute of Standards and Technology (NIST) defines network security standards

Cyber Mission	▸ Develop cryptographic standards and methods to protect the integrity, confidentiality, and authenticity of information resources ▸ Raise awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies ▸ Research, study, and advise agencies of IT vulnerabilities and devise techniques for cost-effective security and privacy of sensitive Federal systems ▸ Develop standards, metrics, tests, and validation programs to promote, measure, and validate security in systems and services, educate consumers, and establish minimum security requirements for Federal systems ▸ Develop guidance to increase secure IT planning, implementation, management and operation
NIST Computer Security Activities	▸ Cryptographic standards and e-authentication ▸ Emerging technologies ▸ Management and assistance (computer security guidance) ▸ Security testing

Sources: www.csrs.nist.gov

NIST's Leap-Ahead Security Technologies initiative focuses on three elements of cyber security infrastructure

Leap-Ahead Security Technologies	
Technical Standards	▸ Create technical standards for generating, distributing, using, storing, and destroying secret numbers known as cryptographic keys, commonly used to grant access to authorized individuals on encrypted computer networks and systems ▸ This effort will be conducted in technical consultation with the National Security Agency (NSA) and the Department of Defense (DoD), as well as other government agencies and non-government organizations
Multifactor Authentication	▸ Nurture the development of "multifactor authentication" methods ▸ Such methods require users to verify their identities through multiple methods, such as passwords and iris scans, rather than just one ▸ NIST will develop a standardized framework that ensures these methods work across different computer platforms and operating systems ▸ The effort will be coordinated with vendors and federal departments, including the Department of Homeland Security
Federal Desktop Core Configuration	▸ Extend the Federal Desktop Core Configuration, a set of standard security settings that optimize security, to other operating systems, applications, and network devices beyond the existing support for Windows XP and Vista

Source: "Comprehensive National Cyber Security Initiative: Leap-Ahead Security Technologies(+$5million), "http://www.nist.gov/public_affairs/factsheet/cyber2009.html

The Department of Health and Human Services (HHS) Information Security and Privacy Program, Secure One HHS, helps protect against information technology threats

Health and Human Services responsibilities, including control of patient sensitive information, dictate a need for constant vigilance in the cyber security fields

Key Activities	▸ Ensuring compliance with federal mandates and legislation, including the Federal Information Management Act and the President's Management Agenda ▸ Protecting HHS ability to provide mission-critical operations, and enable e-government success
Offices	▸ **Information Security and Privacy Program** – Issues policy, guidance, legislation, and reports – Provides privacy impact assessments and resources – Provides incident management and response – Provides IT security awareness and training ▸ **HHS Office of Enterprise Architecture** – Oversees cybersecurity policy implementation – Monitors system integrity – Establishes best practices (including employee training) – Leads HHS Federal Computer Incident Response Capability

Sources: Department of Health and Human Services, http://www.hhs.gov/ocio/capitalplanning/exhibit300/PDF/itinfra.pdf; http://www.hhs.gov/ocio/ea/documents/hhs_ea_governance_plan_fy2007.pdf

The Department of State ensures the protection of it's cyber infrastructure through the Cyber Security Incident Program (CSIP)

- The purpose of the Cyber Security Incident Program (CSIP) is to enhance the protection of Department of State's cyber infrastructure by identifying, evaluating, and assigning responsibility for breaches of cybersecurity
- It focuses on accountability of personnel for actions leading to damage or risk to Department automated information systems (AISs) and infrastructure, even when only unclassified material or information is involved
- The program lays out cybersecurity definitions, AIS user responsibilities, the investigation and evaluation process for cybersecurity incidents, and the administrative actions that may be taken against personnel in violation of program

Source: http://www.state.gov/documents/organization/88409.pdf

National Science Foundation (NSF) Cyber Trust Program promotes research into more secure computer and network systems

- The NSF Cyber Trust Program, a $30 million research-based plan, is the cornerstone of NSF's cybersecurity research and development

- The Cyber Trust Program promotes a vision of network systems that are:
  - More predictable, more accountable, and less vulnerable to attack and abuse
  - Developed, configured, operated, and evaluated by a well-trained and diverse workforce
  - Used by a public educated in their secure and ethical operation.

- To improve national cybersecurity, NSF supports a collection of projects, through grant funding, that together:
  - Contribute to the cybersecurity knowledge base, strengthen the foundations of cyber trust, and advance cybersecurity technologies
  - Define cyber trust broadly to include security, privacy, dependability, reliability, and usability
  - Consider social, economic, organizational, and legal factors influencing cybersecurity
  - Explore innovative new concepts anticipating advances in technology and society
  - Educate and train a diverse workforce in cybersecurity and software technologies

Source: NSF, http://www.nsf.gov/; http://www.nsf.gov/news/news_summ.jsp?cntn_id=100434

NSF's National Cyber Leap Year is designed to identify game-changing efforts for cyber security

- **What are the goals of the National Cyber Leap Year?**
  1. The construction of a national research and technology agenda that both identifies the most promising ideas and describes the strategy that brings those ideas to fruition
  2. Jumpstarting game-changing, multi-disciplinary development efforts

- **When will the National Cyber Leap year be implemented?** Fiscal Year 2009, with two implementation stages:
  - The first stage involves canvassing the cyber security community for ideas
  - The second stage, beginning in February 2009, is a series of workshops to develop the best ideas identified during Stage One

- **What are the end products?** The goal is to publish four types of findings:
  1. Game-changers
  2. Technical strategy
  3. Productization/implementation
  4. Recommendations

Source: NSF, http://www.nsf.gov/

Reference Material

The US Cyber Consequences Unit provides assessments of the strategic and economic consequences of possible cyber-attacks and cyber-assisted physical attacks

The US Cyber Consequences Unit (US-CCU) Mission

To provide America and its allies with the concepts and information necessary for making sound security decisions in a world where our physical well-being increasingly depends on cyber-security

Key Features

- Independent, non-profit, non-governmental, research institute
- Investigates the likelihood of cyber attacks and examines the cost-effectiveness of possible counter-measures
- Primarily concerned with the sort of larger scale attacks that could be mounted by criminal organizations, terrorist groups, rogue corporations, and nation states
- Produces reports that are supplied directly to the government, to entire critical infrastructure industries, and to the public
- Utilizes Value Creation Analysis as its primary analytic method
- Regularly conducts cyber-security exercises for critical infrastructure corporations and other institutions
- Exchanges information on new cyber-attack trends and new counter-measures with organizations in many different countries
- Engages in frequent communication with senior officials at the DOD, DHS, the Department of Commerce, the Department of Treasury, the Department of State, the Department of Energy, the Federal Reserve Board, the national laboratories, and the intelligence community

Source : The *US Cyber Consequences Unit, http://www.usccu.us/#null*

CyLab delivers security technologies, research expertise, and a consortium of industry leaders to counter cybersecurity vulnerabilities

The CyLab Strategy

Integrates response, prediction, education, and research & development to build technology capacity, personnel capacity, cyber awareness, and industrial capacity

Key Features	Areas of Technology Resources and Expertise
▸ Supported by public and private funding, government research funds, and partnering organizations ▸ One of the largest university-based cybersecurity education and research centers in the US ▸ Multi-disciplinary and university-wide, involving six colleges from Carnegie Mellon ▸ CyLab's goal is to build mutually-beneficial public-private partnerships to develop new technologies for measurable, available, secure, trustworthy, and sustainable computing and communications systems and to educate individuals at all levels ▸ A resource for government and business to draw on in addressing cyber risks that endanger national and economic security	▸ Technology Transfer: The Public Sector – multiple joint projects with government agencies; annual DOD program review ▸ Technology Transfer: The Private Sector – multiple joint projects with private sector companies; inventions and patents; and spin-off companies ▸ Information Assurance Professionals - goal is to build a national supply of experts in Information Assurance; developed the Information Assurance Capacity Building Program ▸ National Awareness Programs and Tools - provides web-based public access tools to raise national awareness of cybersecurity in the areas of internet-user awareness and child protection

Source : Carnegie Mellon CyLab, http://www.cylab.cmu.edu/about/about_cylab.html

The Cyber Security Industry Alliance advocates public policy concerning cybersecurity to the government

- The Cyber Security Industry Alliance (CSIA) is a public policy advocacy group that is dedicated to the privacy, reliability, and integrity of global information systems
- CSIA makes recommendations to the government concerning a wide range of cybersecurity issues, ranging from chemical plant security to VoIP, and from phishing to Supervisory Control and Data Acquisition (SCADA) systems—which monitor critical infrastructure functions
- CSIA is joining the Information Technology Association of America (ITAA) in order to create the industry's premier cybersecurity public advocacy and awareness program
  - This collaboration will create a unified voice on critical information security policy issues
  - ITAA offers the industry's only grassroots-to-global network, carrying the voice of information technology (IT) to companies, markets and governments at the local, state, national and international levels to facilitate growth and advocacy
- Recent Actions
  - Issued the CSIA 2007 Agenda for U.S. Government Action, which identified specific actions for Congress and the Administration to focus on improving information security for citizens, industry, and governments globally
  - Successfully lobbied for passage of data security bills in key Senate committees
  - Successfully lobbied for Senate passage of the Identity Theft Enforcement and Restitution Act of 2007 in November

Source : CSIA, http://www.csialliance.org/about_csia/index.html, http://www.csialliance.org/policy_priorities/2007_CSIA_ACCOMPLISHMENTS.pdf; ITAA, http://www.itaa.org/newsroom/release.cfm?ID=2589, April 2008;

The CERT® Program responds to major security incidents and analyzes organizational and product vulnerabilities

CERT® Program Function	
Develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, limit damage, and ensure continuity of critical services	
Key Features	**Areas of Work**
▸ Part of the Software Engineering Institute (SEI), a federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania ▸ Contains the CERT Coordination Center (CERT/CC), which coordinates communication among experts during security emergencies and aims to help prevent future cybersecurity incidents ▸ Works with the news media to raise the awareness of a broad population to the risks they face on the internet and steps they can take to protect themselves ▸ Publishes alerts about internet security problems, in conjunction with US-CERT	▸ Software Assurance – monitors public sources of vulnerability information and regularly receives reports of vulnerabilities; analyzes the state of internet security and conveys that information to the internet community ▸ Secure Systems – performs research in survivable systems engineering; the results contribute to network situational awareness ▸ Organizational Security – helps organizations protect and defend themselves by developing risk assessments that identify and characterize critical information assets and then identify risks to those assets ▸ Coordinated Response – regularly works with sites to help them form computer security incident response teams (CSIRTs); provides guidance and training to both new and existing teams ▸ Education and Training – offers public training courses for computer security incident response teams

Source : CERT, http://www.cert.org/meet_cert/

The Center for Strategic and International Studies (CSIS) is a think tank that provides strategic insights and policy solutions regarding cybersecurity to decision-makers

- CSIS is a bipartisan, nonprofit organization that conducts research and analysis, and develops policy initiatives for government, international institutions, the private sector, and civil society
- The CSIS Technology and Public Policy Program looks at how technological change affects security and economic growth in the new international environment
  - Current research includes cybersecurity, intelligence reform, military space, and Internet governance
  - The program hosts regular discussions with leaders in government, industry, and the private sector
- CSIS recently launched the "Commission on Cyber Security for the 44th Presidency," with the goal of creating a list of recommendations for the next US President
  - The commission is made up of 32 cybersecurity experts, including former cybersecurity directors from the Office of Management and Budget (OMB), a former Federal Trade Commission member, a former DHS assistant secretary for cybersecurity, and executives from the private sector

Source : CSIS, http://www.csis.org/tech/; "Think Tank, Lawmakers Create US Cybersecurity Commission, InfoWorld, Grant Gross, http://www.infoworld.com/article/07/10/30/US-cybersecurity-commission_1.html, October 30, 2007; "Cybersecurity Commission to Proffer Advice to Next President," cnet News, Declan McCullagh, http://news.cnet.com/8301-13578_3-10009603-38.html, August 7, 2008

On 8 December 2008, CSIS released "Securing Cyberspace for the 44th Presidency"

"Government must recast its relationship with the private sector as well as redesign the public-private partnership to promote better cybersecurity. A new partnership with more clearly defined roles and responsibilities, an emphasis on building trust among the partners, and a focus on operational activities will result in more progress on cybersecurity"

-Excerpt, "Securing Cyberspace for the 44th Presidency"

Key Findings	▸ Cybersecurity is a US national security concern of the highest order ▸ Prior to decisions and actions by the US, privacy and civil liberties concerns must be examined ▸ Security in cyberspace is only achievable through a comprehensive national security strategy - encompassing both domestic and international aspects of the cybersecurity problem
An Existing Framework	▸ The report urges that the US not "start over" and instead use what CSIS feels is a workable template in the Bush Administration's Comprehensive National Cybersecurity Initiative (CNCI)
Moving Forward	▸ CSIS recommends a multi-entity response to the cybersecurity challenge, where agencies support key roles through Presidential Directives, and action is coordinated through the White House ▸ The United States must assess and prioritize regulation of cyberspace to ensure delivery of critical services continues uninterrupted in the event of an attack – a comprehensive approach would include: – Better authentication of digital identities – Modernizing the governing mandates and laws regulating cyberspace – Aligning the cyber procurement processes with rigid security standards – Emphasize training, research, and education to improve long-term capabilities

Source: "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency" The Center for Strategic and International Studies, Washington, DC 8 December 2008

In order to achieve a reworked and reinvigorated Public-Private partnership CSIS has outlined a three-pronged approach

Rebuilding a Partnership with the Private Sector	
Presidential Advisory Committee	▸ Would be organized under the Federal Advisory Committee Act (FACA), with senior representatives from key cyber infrastructures ▸ Committee would incorporate (and absorb) the National Security and Telecommunications Advisory Committee (NSTAC) and the National Infrastructure Advisory Council (NIAC) ▸ The committee would lay the foundation for relationships with senior company executives while helping to build trust between the private and public sectors ▸ Membership would be restricted to C-level industry representatives – CSIS recommends replacements not be allowed to attend in lieu of the requisite C-level designee ▸ Financial, IT, and multi-state governmental ISACs would be attached to the Presidential Advisory Committee – DHS would be given discretion over the future of "non-essential" ISACs
National Town Hall	▸ A town hall process would be an inclusive forum assisting with general messaging, information sharing, and stakeholder input ▸ Members would come from the 18 associations and companies deemed critical by DHS ▸ The goal would be to build public awareness and create new relationship opportunities
The Center of Cybersecurity Operations (CCSO)	▸ CCSO would coordinate the trusted collaboration between the public and private sectors ▸ Guided by a board of directors from government, industry, and academia – CCSO would be a self-governing entity to address the operational issues affecting critical infrastructure ▸ A full-time, cross-sector operations center would provide 24-hour watch for cyber issues ▸ CCSO would work with other organizations, including relevant ISACs and academia to analyze and assess current problems and facilitate the execution of solutions from the research phase to application in the marketplace

Source: "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency" The Center for Strategic and International Studies, Washington, DC 8 December 2008 pp 43-48

Electronic Frontier Foundation is a civil liberties group defending the public's rights in the digital world

- Founded in 1990, the Electronic Frontier Foundation is a donor-funded, non-profit civil liberties group
- EFF defends the Internet as a platform for free speech and believes that when the public goes online, their rights should come with them
- EFF believes innovation is inextricably tied to freedom of speech, and innovators need to be protected from established businesses that use the law to stifle creativity and kill competition
- EFF fights to preserve balance and ensure that the Internet and digital technologies continue to empower you as a consumer, creator, innovator, scholar, and citizen

Key Issue Areas

- Free Speech
- Innovation
- Intellectual Property
- International
- Privacy
- Transparency

ELECTRONIC FRONTIER FOUNDATION

Source : Electronic Frontier Foundation, http://www.eff.org

The Center for Democracy and Technology works to promote democratic values and constitutional liberties in the digital age

The Center for Democracy and Technology (CDT) Mission

Conceptualize, develop, and implement public policies to preserve and enhance free expression, privacy, open access, and other democratic values in the new and increasingly integrated communications medium

Key Activities

- Free Expression
- Information Privacy
- Electronic Surveillance and Cryptography
- Online Democracy
- Coalition Building
- Public Education
- Research and Scholarship
- Development of Technical Standards
- Advocacy in the Regulatory Process
- Mobilizing Grassroots Participation
- Working Groups
- International Activism

Source : Center for Democracy and Technology, http://www.cdt.org

CDT's guiding principals promote the democratic potential of today's open, decentralized global Internet

Guiding Principals

1. **Unique Nature of the Internet**: The open, decentralized, user-controlled, and shared resource nature of the Internet creates unprecedented opportunities for enhancing democracy and civil liberties; a fundamental goal of CDT work is seeking public policy solutions that preserve these unique qualities and thereby maximize the democratizing potential of the Internet.
2. **Freedom of Expression**: CDT champions the right of individuals to communicate, publish and obtain an unprecedented array of information on the Internet. CDT opposes governmental censorship and other threats to the free flow of information. As an effective alternative to government controls, CDT believes that a diversity of technology tools can empower families and individuals on the Internet to communicate freely and make choices about the information they receive.
3. **Privacy**: CDT is working for individual privacy on the Internet. CDT believes that maintaining privacy and freedom of association on the Internet requires the development of public policies and technology tools that give people the ability to take control of their personal information online and make informed, meaningful choices about the collection, use and disclosure of personal information.
4. **Surveillance**: CDT challenges invasive government policies. CDT is working for strong privacy protections against surveillance on the Internet. CDT believes that the content of communications, stored information, and transactional data deserve strong legal protection against unreasonable government search and seizure. Protections against government searches should extend to the network, as well as to the home. CDT advocates for stronger legal standards controlling government surveillance to keep pace with the growing exposure of personal information in communications media.
5. **Access**: CDT is working to foster widely-available, affordable access to the Internet. CDT believes that broad access to and use of the Internet enables greater citizen participation in democracy, promotes a diversity of views, and enhances civil society. CDT works for public policy solutions that maximize, in a just and equitable fashion, the unique openness and accessibility of the Internet and preserve its vision as it evolves with ever more powerful broadband technologies.
6. **Democratic Participation**: CDT is pioneering the use of the Internet to enhance citizen participation in the democratic process, and to ensure the voice of Internet users is heard in critical public policy debates about the Internet. CDT believes that the Internet provides unique and effective means of promoting democracy and of facilitating grassroots organizing and public education. CDT supports using the Internet to afford citizens the immediate, broad access to government information necessary to the full practice of democracy.

Source : Center for Democracy and Technology, http://www.cdt.org

Reference Material

Presidential Decision Directive 63 was one of the first documents addressing the threat of attacks on the nation's cyber systems

Presidential Decision Directive 63

May 1998

- Sought to eliminate significant vulnerabilities to physical and cyber attack on critical infrastructures and protect the abilities of:
  - The Federal Government to perform essential national security missions and ensure public health and safety
  - State and local governments to maintain order and deliver essential services
  - The private sector to ensure the functioning of the economy and the delivery of telecommunications, energy, financial, and transportation services
- Designated the Departments of Commerce, Treasury, Transportation, Justice, Energy, HHS, and the Environmental Protection Agency (EPA), and Federal Emergency Management Agency (FEMA), as "lead agencies" for protecting the various sectors of "critical infrastructure" against cyber attack
- Created the National Infrastructure Protection Center (NIPC) within the FBI to serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement entity
- Created the Information Sharing and Analysis Center (ISAC) to gather, analyze, and disseminate private sector information on vulnerabilities and threats to both industry and the NIPC

Source: Presidential Decision Directive/NSC-63, May 22, 1998

The *National Strategy to Secure Cyberspace* outlines a framework to reduce our nation's vulnerability to attacks against our critical information infrastructures

National Strategy to Secure Cyberspace

February 2003

- The National Strategy to Secure Cyberspace seeks to:
  - Prevent cyber attacks against America's critical infrastructures
  - Reduce national vulnerability to cyber attacks
  - Minimize damage and recovery time from cyber attacks that do occur
- The Strategy articulates five national priorities:
  - A National Cyberspace Security Response System
  - A National Cyberspace Security Threat and Vulnerability Reduction Program
  - A National Cyberspace Security Awareness and Training Program
  - Securing Governments' Cyberspace
  - National Security and International Cyberspace Security Cooperation
- Highlights the role of public-private engagements

Sources: National Strategy to Secure Cyberspace, February 2003; National Strategy for Information Sharing, October 2007

Homeland Security Presidential Directive 7 establishes a national policy to protect United States critical infrastructure and key resources from terrorist attacks

Homeland Security Presidential Directive 7

2003

- HSPD-7 requires DHS to coordinate efforts to protect cyberspace for critical infrastructure
  - DHS serves as a focal point for the security of cyberspace, facilitating interactions between Federal agencies, State and local governments, the private sector, academia, and international organizations
  - DHS's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems
  - DHS supports the DOJ in its mission to investigate and prosecute attacks in cyberspace
  - Commerce, in coordination with DHS, will work with the private sector, research, academic, and government organizations to improve technology for cyber systems
- A Critical Infrastructure Protection Policy Coordinating Committee will advise the Homeland Security Council on interagency policy related to cyber infrastructure protection

Sources: Homeland Security Presidential Directive 7, December 17, 2003; "Bush Expands Network Monitoring," Washington Post, January 26, 2008

The *National Security Strategy* and the *National Strategy for Homeland Security* provide the overall strategic framework for securing the United States

National Security Strategy ***March 2006***	▸ Founded upon two pillars: – Promote freedom, justice, and human dignity—working to end tyranny, to promote effective democracies, and to extend prosperity through free and fair trade and wise development policies – Confront the challenges of our time by leading a growing community of democracies
National Strategy for Homeland Security ***October 2007***	▸ Provides a common framework for the nation to focus its effort on the following goals: – Prevent and disrupt terrorist attacks – Protect the American people, critical infrastructure, and key resources – Respond to and recover from incidents that do occur – Continue to strengthen the foundation to ensure our long term success ▸ Leverages the unique strengths and capabilities of all levels of government, the private and non-profit sectors, communities, and individual citizens

Sources: National Security Strategy, March 2006; National Strategy for Homeland Security, October 2007

The *National Strategy for Information Sharing* aims to coordinate information about terrorist activity across all relevant government agencies and departments

National Strategy for Information Sharing

October 2007

- Developed with the understanding that homeland security information, terrorism information, and law enforcement information related to terrorism can come from multiple sources, all levels of government, as well as from private sector organizations and foreign sources
- Core Principles and Understandings:
  - Effective information sharing comes through strong partnerships
  - Information sharing must be woven into all aspects of counterterrorism activity
  - Information sharing must integrate existing technical capabilities and respect established authorities and responsibilities
  - Fusion centers represent a valuable information sharing resource
- Those responsible for combating terrorism must have access to timely and accurate information

Sources: National Strategy for Information Sharing, October 2007

The *Federal Information Security Management Act* requires federal agencies to implement an information security program

Federal Information Security Management Act

December 2002

- FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
- FISMA explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, the Office of Management and Budget (OMB) through *Circular A-130, Appendix III*, Security of Federal Automated Information Resources, requires executive agencies within the federal government to:
  - Plan for security
  - Ensure that appropriate officials are assigned security responsibility
  - Periodically review the security controls in their information systems
  - Authorize system processing prior to operations and periodically, thereafter

Source: "FISMA: Detailed Overview", http://csrc.nist.gov/groups/SMA/fisma/overview.html

The international community faces significant legal challenges when addressing cyber issues

- Still no universal agreement on application of Law of Armed Conflict (LOAC) to Cyber Operations
  - "Armed conflict" traditionally applied to physical confrontation
  - LOAC traditionally limited to domains of land, sea, air, and space
  - Characterization of combatants and non-combatants more complex
  - Proportionality issues and legality of use of cyber "weapons" are more complex
- Application of UN Charter to Cyber Operations also unclear
  - Article 2(4) proscribes "unlawful use of force"
  - Article 51 self defense is premised on "armed attack"
  - Both articles traditionally interpreted in physical terms
- Legal authorities largely stratified by fixed "lanes"
  - Laws are distinct for service providers, law enforcement, intelligence, and warfighters
  - Goals of each lane vary dramatically
  - Sharing and coordinating across lanes still challenging
  - May slow identification of "acts of war"
- Difficulty in attributing the source of an attack may pose a legal stumbling block
  - Attack sources easily spoofed, disguised
  - Some attribution techniques limited by law
  - Failure to link attack source to nation state may limit legality/appropriateness of response options
  - Duties of and protection of neutrals made more complex

Source: Booz Allen Analysis

Reference Material

The world that we operate in is becoming increasingly globalized and interconnected

- Our world today is driven by an evolving set of threats, with terrorist groups, health epidemics, natural disasters, and financial shocks conspiring, individually and collectively, to disrupt global markets, incite conflict, reduce prosperity, and impact our basic security
- Our increasingly globalized and interconnected world is creating issues that are too large for any one authority to solve alone—the situation calls for a new type of tri-sector leadership in which business, government, and nonprofits work together in a state of permanent negotiation and interaction
- *Bottom Line: In an era of global networks and interdependence, unilateral approaches are no longer adequate*

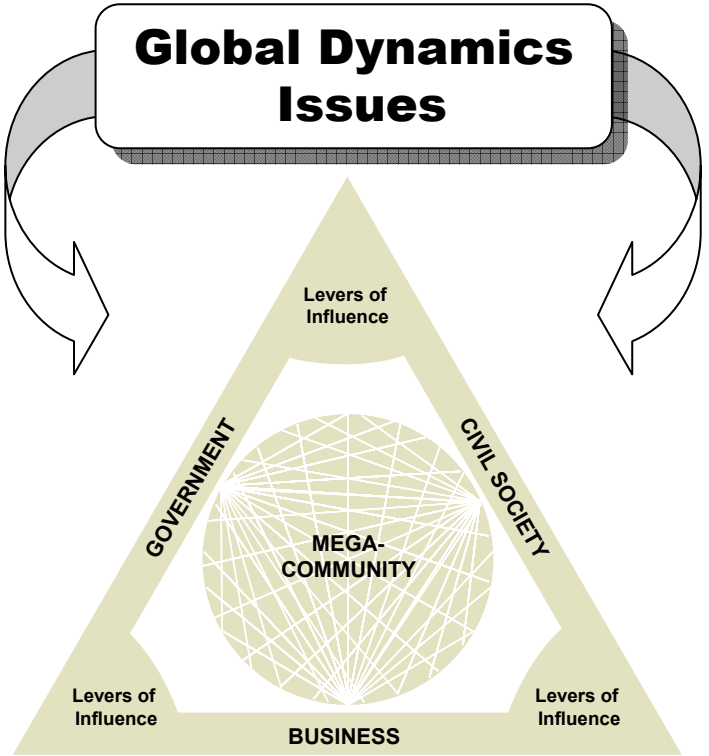
Global Dynamic Issues

To address these dynamic issues, leaders increasingly need to reach across traditional sector divisions to form collaborative "megacommunities"

Source: "Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together," Mark Gerencser, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly, (New York: Palgrave Macmillan 2008)

Megacommunity thinking offers a unique approach to introduce collaboration and system-level thinking to our most vexing problems

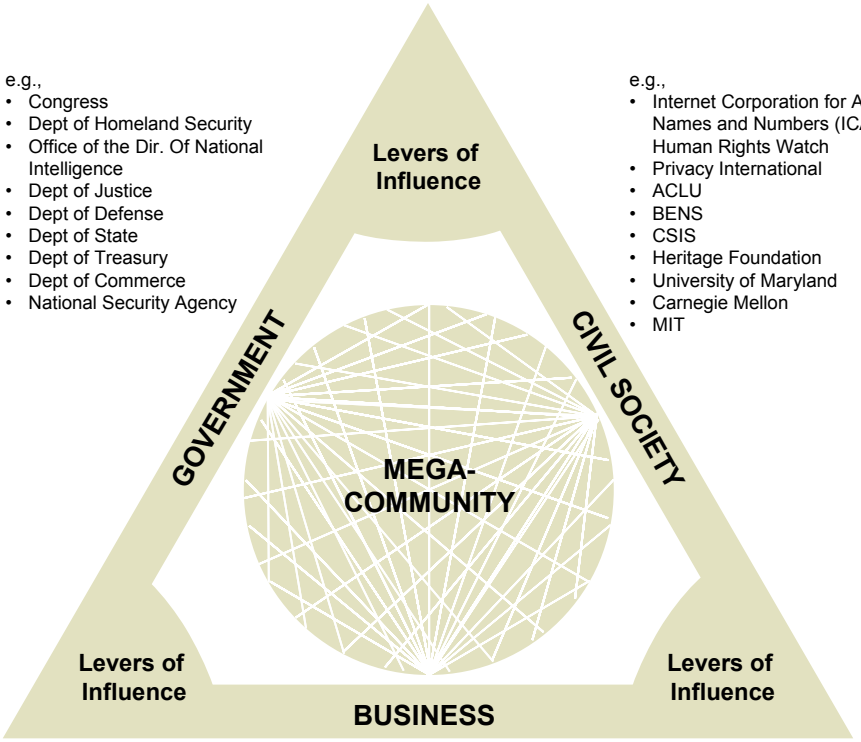
- Global Dynamics issues are the 'Gordian Knots' of our time—you can see them clearly, but they don't have any clear solution. Unfortunately, we cannot cleave them in two and call it quits. We need to attempt to solve them.
- Examining challenges like cyber through the Global Dynamics lens reveals the need for mutual leadership—activities that bring decision-makers from business, governments, and civil-sector institutions together to collaborate.
- By networking these communities together—creating Megacommunities—leaders will be able to share resources, talent, and innovative ideas in new ways that produce enduring solutions to the world's most significant problems.



The megacommunity concept provides an actionable collaborative framework to help our client's develop integrated solutions to the challenges posed by global dynamics

Source: "Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together," Mark Gerencser, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly, (New York: Palgrave Macmillan 2008)

Megacommunity thinking recognizes the necessity and power of business, government, and civil society working together on issues



A megacommunity relies on the dynamic tension that exists among all three sectors – each sector uses its levers of influence to interact with a different sector

Megacommunity is a new approach to problems which span business, government and the communities in which we live.

Megacommunities defined by five elements:

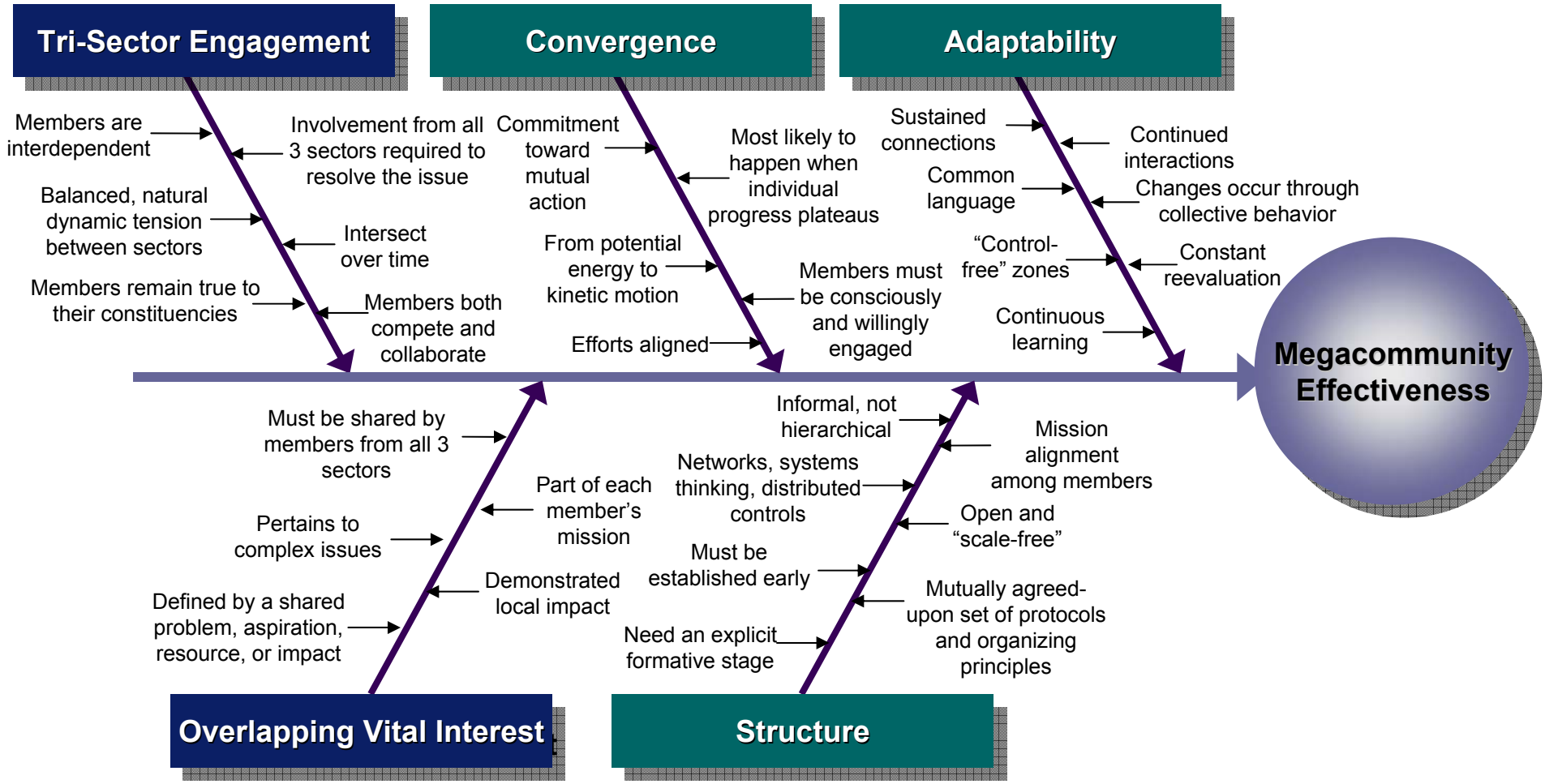
- ***Tri-Sector Engagement***
- ***Overlapping Vital Interests***
- ***Convergence***
- ***Structure***
- ***Adaptability***

We are caught in an inescapable network of mutuality, tied in a single garment of destiny. Whatever affects one directly, affects all indirectly.

Martin Luther King, Jr.

Source: "Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together," Mark Gerencser, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly, (New York: Palgrave Macmillan 2008)

Each element has several contributing factors which influence the effectiveness of the megacommunity



Source: "Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together," Mark Gerencser, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly, (New York: Palgrave Macmillan 2008)

Reference Material

Glossary

- **AIS: Automated Information Systems** – A combination of computers and networks configured to automatically process or transfer information quickly
- **ASD/HD: Assistant Secretary of Defense/Homeland Defense** – Office of the Secretary of Defense section focused on Homeland Defense matters
- **ASD/NII/DOD CIO: Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer** – Office of the Secretary of Defense section focused on network security, information integration, and information flow
- **CERT: Computer Emergency Readiness Center** – A team or trust of individuals set up to monitor, react, and respond to cyber incidents
- **CERT-CC: CERT Coordination Center** – Coordinates communication among experts during security emergencies and to help prevent future cybersecurity incidents
- **CHIP: Computer Hacking and Intellectual Property (units)** – A component of the Department of Justice, aimed at prosecuting high profile technology-focused incidents; also offers training to State, Federal and Local prosecutors to increase expertise

Glossary

- **CIA: Central Intelligence Agency**
- **CINS: Critical Infrastructure Notification System** – A component of the FS-ISAC that allows for rapid, simultaneous security alerts to multiple entities
- **CIP: Critical Infrastructure Protection**
- **CIPAC: Critical Infrastructure Partnership Advisory Council** – Facilitates coordination with Federal, State, Local, and Private infrastructure protection programs
- **CIPS: Critical Infrastructure Protection Standards**
- **CNA: Computer Network Attack**
- **CNCI: Comprehensive National Cybersecurity Initiative** – A component of PDD 54 aimed at facilitating Federal efforts to protect against cyber attacks
- **CNE: Computer Network Exploitation**
- **CONUS: Continental United States**

Glossary

- **COTS: Commercial Off the Shelf**
- **CSCC: Communications Sector Coordinating Council** – Facilitates the coordination of sector-wide activities and initiatives designed to improve physical and cyber security of the critical infrastructures
- **CSIA: Cyber Security Industry Alliance** – A public policy advocacy group that is dedicated to the privacy, reliability, and integrity of global information systems
- **CSIP: Cyber Security Incident Program** – A Department of State initiative aimed at enhancing the protection of its cyber infrastructure
- **CSIS: Center for Strategic and International Studies**
- **CS&C (Assistant Secretary of): Cyber Security and Communications** – An Assistant Secretary Position beneath the Undersecretary for National Protection and Programs (DHS) which coordinates the DHS cybersecurity mission
- **DARPA: Defense Advanced Research Projects Agency**
- **DBT: Design Basis Threat**

Glossary

- **DC3: DOD Cyber Crime Center** - Sets standards for digital evidence processing, analysis, and diagnostics for any DOD investigation; consists of the DCCI, DCITA, and DCFL
- **DCCI: Defense Cyber Crime Institute** – A component of DC3
- **DCFL: Defense Computer Forensics Laboratory**– A component of DC3
- **DCIOs: Defense Criminal Investigative Organizations**
- **DCITA: Defense Cyber Investigations Training Academy** – A component of DC3
- **DDSO/IO: Deputy Directorate for Strategic Operations/Information Operations**
- **DHS: Department of Homeland Security**
- **DIA: Defense Intelligence Agency**
- **DIOSS: Director for Operations and Strategic Studies** – Department of Defense

Glossary

- **DISA: Defense Information Systems Agency** – A DOD agency that supports the Office of the Secretary of Defense with part of its cyber component
- **DNI: Directorate of National Intelligence**
- **DOD: Department of Defense**
- **DOE: Department of Energy**
- **DOJ: Department of Justice**
- **DoS: Denial of Service (attack)** – A coordinated computer attack that restricts (denies) access (service) to the internet to a targeted set of individuals, agencies or geographic locales
- **EA: Electronic Attack**
- **EPA: Environmental Protection Agency**
- **ERO: Electronic Reliability Organization**

Glossary

- **FAA: Federal Aviation Administration**
- **FBI: Federal Bureau of Investigation**
- **FBIIC: Financial and Banking Information Infrastructure Committee**
- **FDCC: Federal Desktop Core Configuration** – A NIST initiative, and part of the CNCI that mandates agencies adopt a common security protocol for their desktop systems
- **FEMA: Federal Emergency Management Agency**
- **FERC: Federal Emergency Regulatory Commission**
- **FMC: Fixed Mobil Convergence**
- **FSCC: Financial Services Coordinating Council**
- **FS-ISACs: Financial Services Information Sharing and Analysis Centers**
- **GIG: Global Information Grid**
- **GPS: Global Positioning System**

Glossary

- **HHS: Health and Human Services**
- **HSPD: Homeland Security Presidential Directive**
- **ICANN: Internet Corporation of Assigned Names and Numbers** – Formed in 1998 through MOU with Department of Commerce, ICANN coordinates and manages unique identifiers (Domain Name Systems) that label websites across the world
- **IO: Information Operations**
- **IP: Internet Protocol** – A protocol used to locate and communicate across the internet
- **IRS: Internal Revenue Service**
- **ISAC: Information Sharing and Analysis Centers** – Multi-organization/agency entities aimed at protecting critical infrastructure from cyber and physical attacks
- **ITAA: Information Technology Association of America**
- **ITS: Intelligent Transportation Systems**

Glossary

- **JFCC-NW: Joint Functional Component Command Network Warfare** – A USSTRATCOM component that facilitates cooperation with other government entities in network defense, and executes offensive operations
- **JTF-GNO: Joint Task Force Global Network Operations** – A USSTRATCOM component that controls the GIG and ensures the availability and security of the systems and networks operated by the Services, Commands, and DOD civilian agencies
- **LANL: Los Alamos National Laboratories**
- **LE: Law Enforcement**
- **LOAC: Law of Armed Conflict**
- **NCS: National Communications System** – Assists Executive Branch and coordinating entities in the planning and provisioning of national security and emergency preparedness communications for the Federal Government
- **NCSC: National Cyber Security Center** – A DHS component overseeing the actions of the CNCI, and serving as the focus for improving Federal network defenses

Glossary

- **NGO: Non-Governmental Organization**
- **NIPC: National Infrastructure Protection Center** – A FBI component created under PDD 63 that serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement entity
- **NIST: National Institute of Standards in Technology**
- **NRC: Nuclear Regulatory Commission**
- **NSA: National Security Agency**
- **NSF: National Science Foundation**
- **OCONUS: Outside of the Continental United States**
- **OEC: Office of Emergency Communications**
- **OMB: Office of Management and Budget**
- **OSD: Office of the Secretary of Defense**

Glossary

- **P2P: Peer to Peer** – A form of communication between automated machines, wherein computers talk directly to one and another, rather than taking identical commands from a single, Command and Control machine or administrator
- **PDD: Presidential Decision Directive**
- **PIN: Personal Identification Number**
- **RFID: Radio Frequency Identification (Attacks)** – RFID technologies remotely read sensors over radio frequencies, linking the sensors to a particular ID
- **SANS: SystemAdmin, Audit, Network, Security, Institute**
- **SCADA: Supervisory Control and Data Acquisition (systems)** – Systems used to monitor critical infrastructure components – a ubiquitous part of most of the nation's critical infrastructure
- **SEI: Software Engineering Institute**
- **SIGINT: Signals Intelligence**

Glossary

- **SMS: Short Message Service** – A common form of communication using short messaging to text from phone to phone
- **TIC: Trusted Internet Connections** – An integral component of the CNCI, TICs are designed to drastically reduce the number of gateway connections between agencies and the internet
- **TFI: (Department of the Treasury Office of) Terrorism and Financial Intelligence**
- **UN: United Nations**
- **USB: Universal Serial Bus** – Often associated with "Flash" drives, USB is a standard and easily accessible interface with most computers, enabling rapid transfer of files
- **US-CCU: US Cyber Consequence Unit** – An independent, non-profit, non-governmental research institute that provides the US government and its allies with the concepts and information necessary for making sound security decisions
- **US-CERT: US Computer Emergency Readiness Team** – DHS's 24/7 watch and warning center for the Federal Government's Internet infrastructure

Glossary

- **USD AT&L: Under Secretary of Defense, Acquisitions, Technology, and Logistics**
- **USD-I: Under Secretary of Defense, Intelligence**
- **USD-P: Under Secretary of Defense, Policy**
- **USNORTHCOM: US Northern Command** – A DOD Combatant Command (COCOM) established in 2002 to provide command and control oversight of DOD's homeland defense efforts, as well as coordinate defense support of civil authorities
- **USSTRATCOM: US Strategic Command** – A COCOM that among other things, is focused on deterring attacks against US vital interests in space and cyberspace
- **VoIP: Voice over Internet Protocol** – A system of technologies that enables delivery of voice communications over the internet
- **WiFi: Wireless Fidelity** – A remote and wireless means of connecting to the internet, which only requires proximity to a properly configured network hub
- **Web 2.0** – Changing trends in the use of World Wide Web technology and web design that aim to enhance creativity, communications, secure information sharing, collaboration and functionality of the web