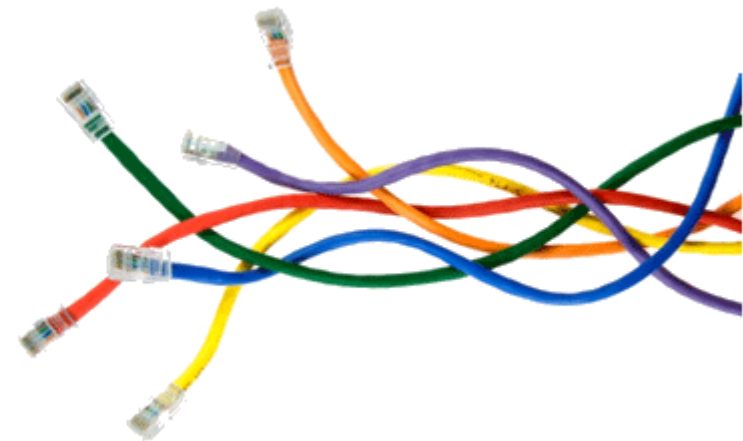




Succeeding in a Cyber World

Harry Raduege
Lieutenant General, USAF (Ret)
Chairman, Center for Cyber Innovation
November 2009



History of cyber warfare



Sources include "Some key events in the history of cyber warfare", By Amber Corrin, Federal Computer Week, Oct 15, 2009

The State of Cybersecurity – Pre January 2009

Some Examples:

- ✓ Russian cyber attacks followed by military invasion of Chechnya (2002) & Georgia (2008)
- ✓ Russian cyber attacks on Estonia (2007)
- ✓ Massive espionage being performed throughout U.S. government
- ✓ Identities lost (examples):
 - PA Public Welfare Dept. = 375,000 (9/07)
 - MA Div. of Professional Licensure = 450,000 (10/07)
 - U.S. Dept. of Veterans Affairs = 1,800,000 (11/07)
 - WI Dept. of Health & Family Services = 260,000 (1/08)
 - CO Div. of Motor Vehicles = 3,400,000 (7/08)
- ✓ Overall U.S. identities lost since Jan 2005 = > 250 Million
- ✓ Reported cyber attacks on U.S. government computer networks climbed 40%
- ✓ China became #1 user of Internet
- ✓ President's "Comprehensive National Cybersecurity Initiative" (1/08)

CSIS Cybersecurity Commission

Summary of Findings & Recommendations (Dec 08)

- ✓ Cybersecurity – now a major national security problem for the U.S.
- ✓ Decisions & actions must respect privacy & civil liberties
- ✓ Only a comprehensive national security strategy that embraces both domestic & international aspects of Cybersecurity will make us more secure

- Create a Comprehensive National Security Strategy for Cyberspace
- Organize for Cybersecurity
- Partner with Private Sector
- Regulate for Cybersecurity
- Secure Industrial Control Systems (ICS) & Supervisory Control and Data Acquisition (SCADA) Systems
- Use Acquisition Rules to Improve Security
- Manage Identities
- Modernize Authorities
- Revised Federal Information Security Management Act (FISMA)
- End Division Between Civilian & National Security Systems
- Conduct Training for Cyber Education & Workforce Development
- Conduct Research & Development for Cybersecurity

The State of Cybersecurity – Post January 2009

Some Examples:

- ✓ Estimated \$1 Trillion worth of data stolen (2008)
- ✓ Cybercrime up 53%
 - Topped \$20 Billion at financial institutions
- ✓ Cyber attack against Kyrgyzstan's ISPs (Directed Denial of Service, 18-31 Jan 09)
- ✓ Reported attacks on U.S. government computer networks climbed 40% last year
- ✓ Sensitive records of 45,000 FAA workers breached (Feb 09)
- ✓ Chinese stole design secrets of all U.S. nuclear weapons (Ms Van Cleave)
- ✓ U.S. nuclear weapons lab is missing 69 computers (Feb 09)
- ✓ U.S. moved from #4 to #17 in broadband connectivity
- ✓ \$4.5 Trillion moved daily via "Fedwire" (U.S. GDP = \$14.3 Trillion)
- ✓ "Cloud Computing" – the question of openness & savings versus security
- ✓ Cost to repair average 2008 data breach = \$6.6 Million
- ✓ Coordinated Cyber attack against U.S. government & South Korea (4 Jul 09)
- ✓ China has 338 Million Internet users – a 13.8% increase over 2008 (Nov 09)
- ✓ Today, there are 4,000 active terrorist activities on the Net

President's Cyberspace Policy Review

Assuring a Trusted and Resilient Information and Communications Infrastructure,

May 29, 2009

- U.S. is at a crossroads – “cyberspace” underpins almost every facet of society
- Status quo no longer acceptable – U.S. must lead with strong leadership & vision
- Federal government to initiate a national public awareness & education campaign
- U.S. should develop a globally competitive workforce
- Federal government should reinforce cybersecurity partnership with private sector
- U.S. needs a cybersecurity strategy addressing the international environment
- U.S. needs comprehensive framework to coordinate Federal, State, local, tribal, private sector, & international allies response to significant cyberspace events
- Federal, State, & local partners should identify procurement strategies to incentivize the market to make more secure products & services



President's Cyberspace Policy Review

Near-Term Action Plan

1. Appoint NSC/NEC dual-hatted cybersecurity policy official & establish NSC directorate
2. Prepare cybersecurity national strategy
3. Designate cybersecurity as a Presidential key management priority with metrics
4. Designate a privacy & civil liberties official to the NSC cybersecurity directorate
5. Formulate policy – clarify roles, responsibilities, & agency authorities
6. Initiate national public awareness & education campaign
7. Develop an international cybersecurity policy framework & strengthen international partnerships
8. Prepare cybersecurity incident response plan; enhance public-private partnerships
9. Develop framework for research & development (R&D) strategies focusing on game-changing technologies
10. Build a cybersecurity-based identity management vision and strategy that addresses privacy & civil liberties, leveraging privacy-enhancing technologies

President's Cyberspace Policy Review

Mid-term Action Plan

1. Improve process for resolving interagency disagreements
2. Use performance-based budgeting, using OMB program assessment framework
3. Expand key information age education programs and R&D
4. Expand & train the workforce
5. Determine best mechanisms to obtain strategic warning, maintain situational awareness, & inform incident response capabilities.
6. Develop a set of threat scenarios & metrics for risk management, recovery planning, and R&D prioritization
7. Develop a process between government & private sector for preventing, detecting, & responding to cyber incidents
8. Develop mechanisms for information sharing that address privacy & proprietary information & make information sharing mutually beneficial
9. Develop solutions for emergency communications
10. Expand information sharing with key allies about network incidents & vulnerabilities

President's Cyberspace Policy Review (May 09)

Mid-Term Action Plan (cont'd)

11. Encourage collaboration between academic & industrial laboratories
12. Define goals for national & international standards bodies
13. Implement an "opt-in" array of interoperable identity management systems to build trust for on-line transactions to enhance privacy
14. Refine government procurement strategies & improve market incentives for secure & resilient hardware & software products, new security innovation, & secure managed services



We've had our Cyber Wake-up Call

Security experts say financial motives often are behind modern *cyber-attacks*. ...
CNN, August 6, 2009

Federal agencies are facing a severe shortage of computer specialists, even as a growing wave of coordinated cyberattacks ... *WSJ, July 22, 2009*

Russian hackers hijacked American identities and U.S. software tools and used them in an attack ...
WSJ, August 17, 2009

A Brooklyn man used his job as a computer technician to appropriate the identities of more than 150 employees of the Bank of New York Mellon and steal more than \$1.1 million from an array of nonprofit groups and other institutions, *NYT, October 2009*

House leaders called for an "immediate and comprehensive assessment" of congressional cybersecurity policies, a day after an embarrassing data breach that led to the disclosure of details of confidential ethics investigations. *Washington Post, October 2009*

The number of security incidents reported by federal agencies to the U.S.-CERT has dramatically increased in the past three years, rising from 5,503 incidents in fiscal year 2006 to 16,843 in FY 2008, a 206 percent increase.
Gregory Wilshusen, GAO

[Cyveillance] identified more than 175,000 distinct phishing attacks from June through August of this year, "one of the highest three-month volumes ever detected."

Government Computer News, October 2009

"They predominantly use spear-phishing attacks which they have socially engineered" to deliver client-side application exploits."

Rob Lee, Sans Institute, September 2009

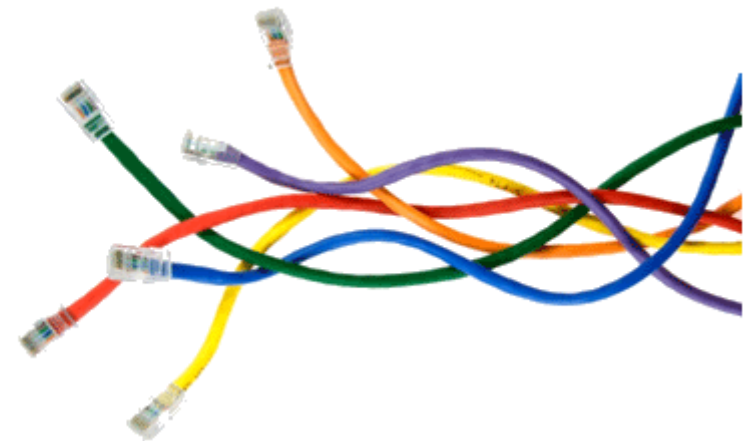
CSIS Cybersecurity Commission (Phase 2)

Beginning 24 Jun 09

- “ ... we will continue the Commission's work to identify sound policies that address the critical issues for Cyberspace. We will build a national community of experts to engage in this vital task. Our goal is to fulfill the Commission's vision for a secure Cyberspace while adhering to the bipartisan and independent principles that guided our report.”
- *Work-plan & topics for Phase 2 more detailed efforts:*
 - ✓ Vision for a “National Cyberspace Strategy”
 - ✓ Authorities & Doctrine
 - ✓ Network Health & Situational Awareness
 - ✓ Authentication of Identity
 - ✓ Privacy & Civil Liberties as a Foundation for Cybersecurity
 - ✓ Innovation
 - ✓ International Engagement
 - ✓ Plan for Moving Forward

CSIS Cybersecurity Conclusion

- The effort to improve Cybersecurity offers the opportunity to rethink how government & industry operate and to build collaboration across organizational boundaries
- The goal should not be the best defense, but government & industry that can:
 - Securely take full advantage of Cyberspace
 - Enable and assure essential services in Cyberspace
 - Create opportunities for collaboration, growth, & national advantage



Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. [v.l.1]