

# CYBER POLICY: A NATIONAL IMPERATIVE

Melissa Hathaway

Senior Advisor  
Belfer Center for Science and International Affairs  
Harvard University

1 March 2011



**HARVARD Kennedy School**

**BELFER CENTER** for Science and International Affairs

© 2011 Hathaway Global Strategies, LLC.

# Agenda

- ♦ CNCI and the Threat
- ♦ Cyberspace Policy Review
- ♦ Progress: Where We Stand Today
- ♦ Recommendations:
  - ♦ Legislative Branch
  - ♦ Executive Branch
- ♦ Summary

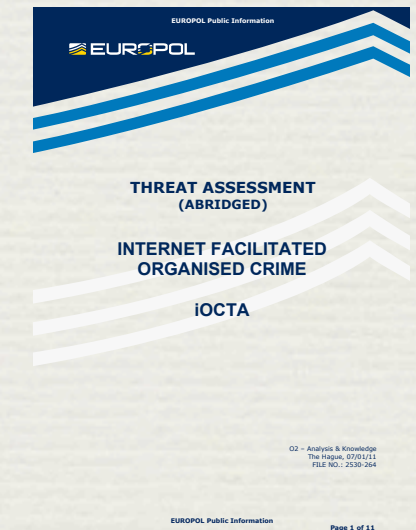
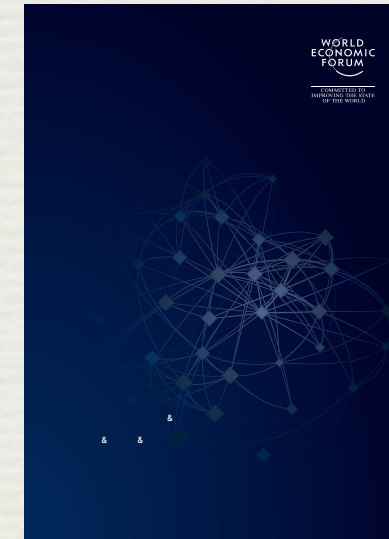
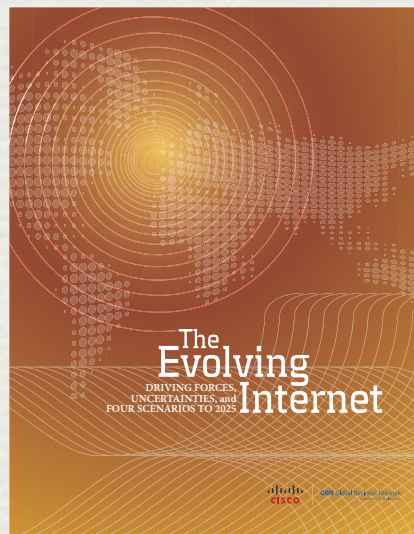
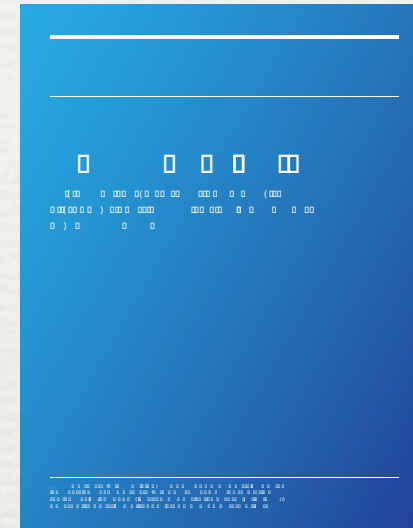
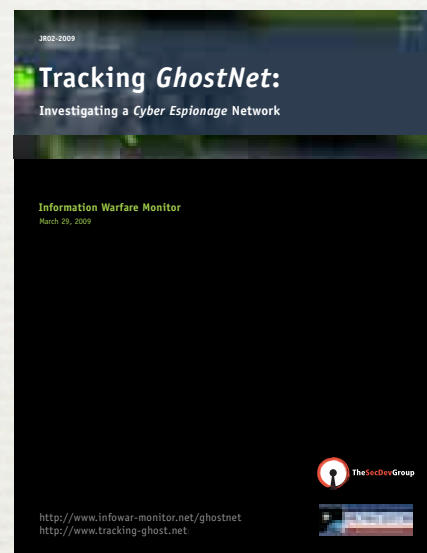
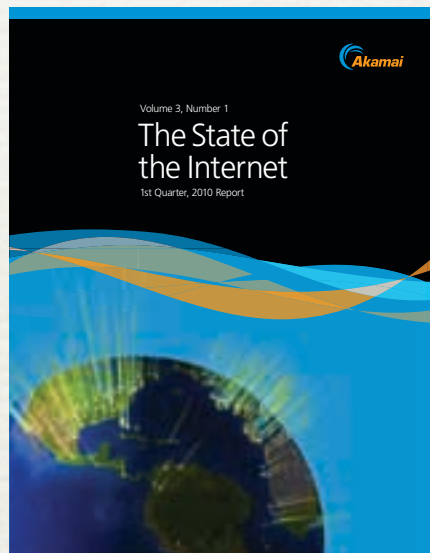


# 2007-2009: CNCI

- ♦ The Comprehensive National Cybersecurity Initiative (CNCI) provided a framework for unifying the government to address a multi-dimensional threat:
  - ♦ Insider: Unauthorized use or access to information, systems, and networks by otherwise trusted agents (employees).
  - ♦ Proximity: Gaining access to information or systems via deployment of technology in proximity to the target.
  - ♦ Remote: Accessing target information and/or systems through network-based technical means (Internet).
  - ♦ Supply Chain: Gaining advantage, control, and/or access to systems and the information they contain through manipulation by cooperative/witting vendors or unilaterally at any point in the supply chain between the manufacturer and end user.



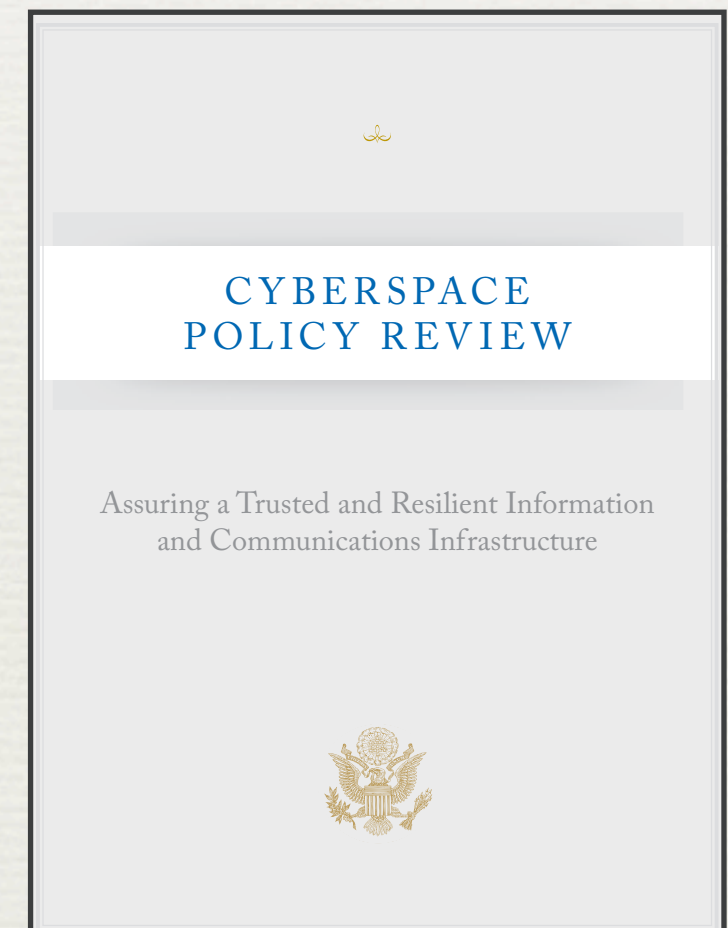
# Industry and Government are Being Targeted: The Tools are Common





# 2009: The Cyberspace Policy Review

- ♦ President Obama's Cyberspace Policy Review provides a National blue-print toward securing America and ensuring that cyberspace is sufficiently resilient and trustworthy to support U.S. goals of economic growth and national security.
- ♦ The report consisted of five chapters and seven annexes:
  - ♦ Leading from the Top
  - ♦ Building Capacity for a Digital Nation
  - ♦ Sharing Responsibility for Cybersecurity
  - ♦ Creating Effective Information Sharing and Incident Response
  - ♦ Encouraging Innovation
- ♦ It articulated 25 Near and Mid-Term Recommendations





# CPR Action Plans

CYBERSPACE POLICY REVIEW

TABLE 1: NEAR-TERM ACTION PLAN
1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.
6. Initiate a national public awareness and education campaign to promote cybersecurity.
7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement
9. In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
10. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

CYBERSPACE POLICY REVIEW

TABLE 3: MID-TERM ACTION PLAN
1. Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.
2. Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
3. Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
4. Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.
5. Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.
6. Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.
7. Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
8. Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
9. Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
10. Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
11. Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
12. Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.
13. Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
14. Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.

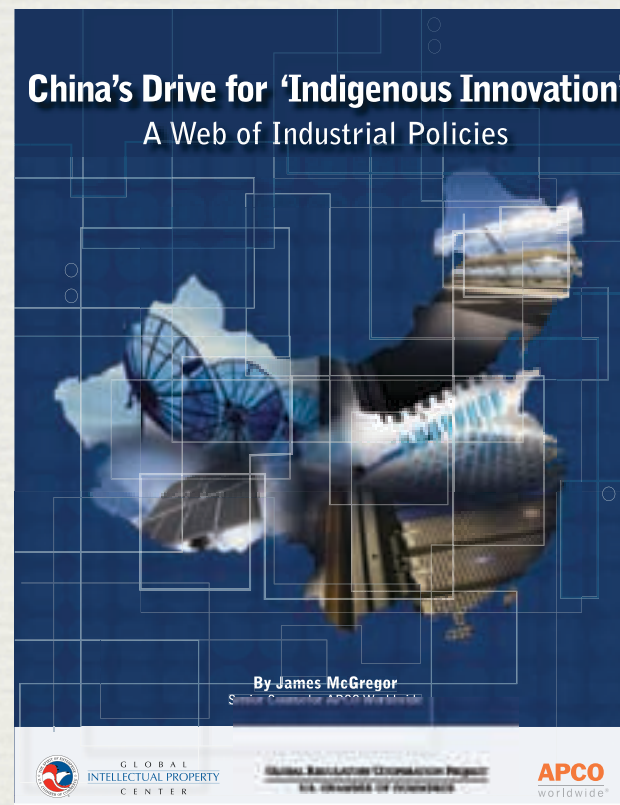
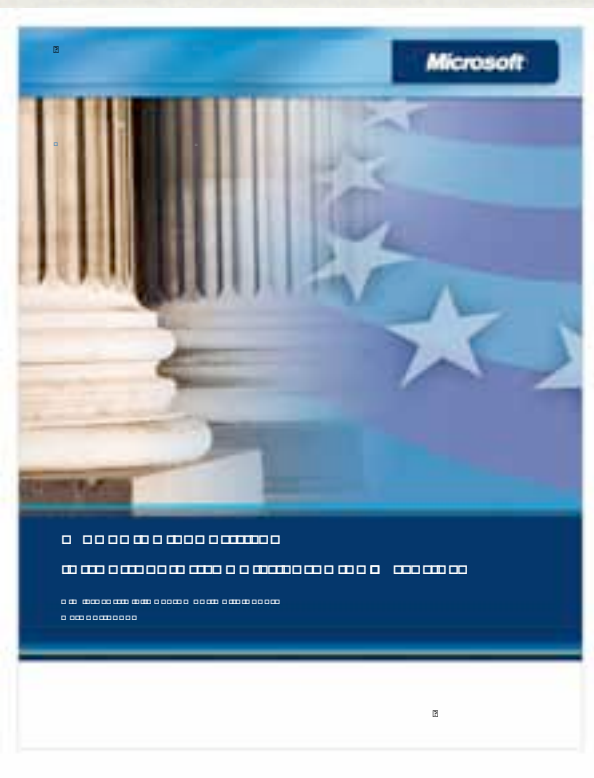
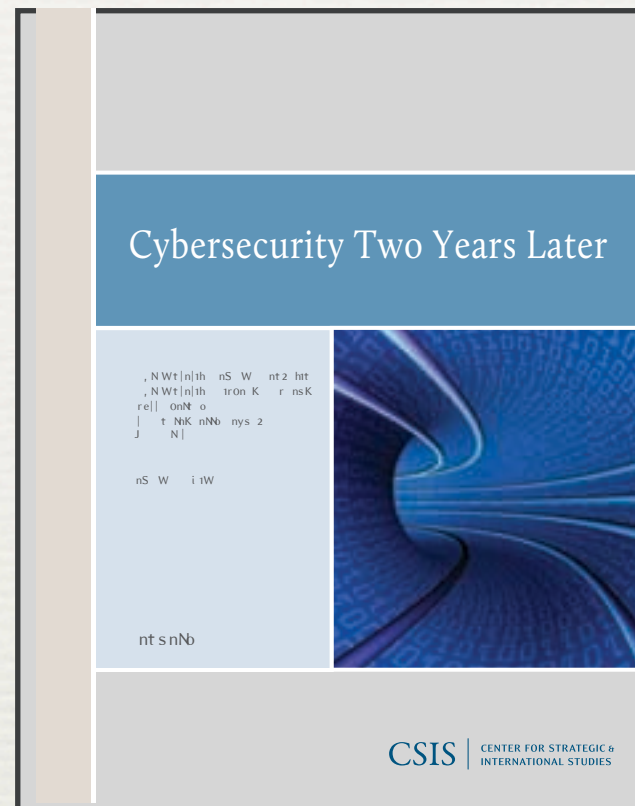
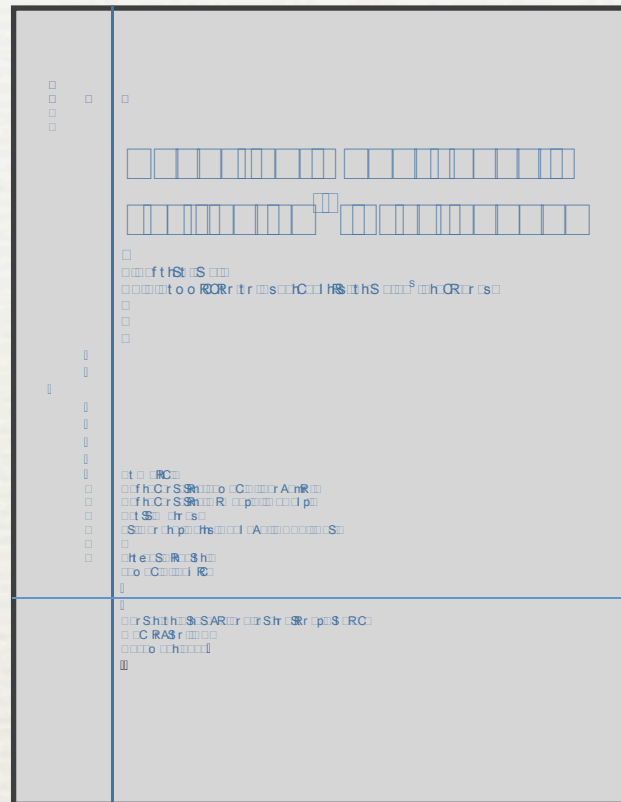


# 2010 Events Pique Awareness: The Threat is Real and Growing

- ✦ January 2010: Operation Aurora (Google) affected over 2000 companies, demonstrating ease of exploitation in a cloud-based infrastructure (Internet: espionage?)
- ✦ Summer 2010: Stuxnet affecting global critical infrastructures (power grid) using a combination of 5 propagation paths (supply chain: sabotage?)
- ✦ November 2010: Wiki-leaks demonstrating need for data-loss prevention, vulnerability of cloud-based infrastructures, and dependence upon the telecommunications infrastructure (DDoS affected AT&T and Verizon) (insider threat: Political Dissent?)

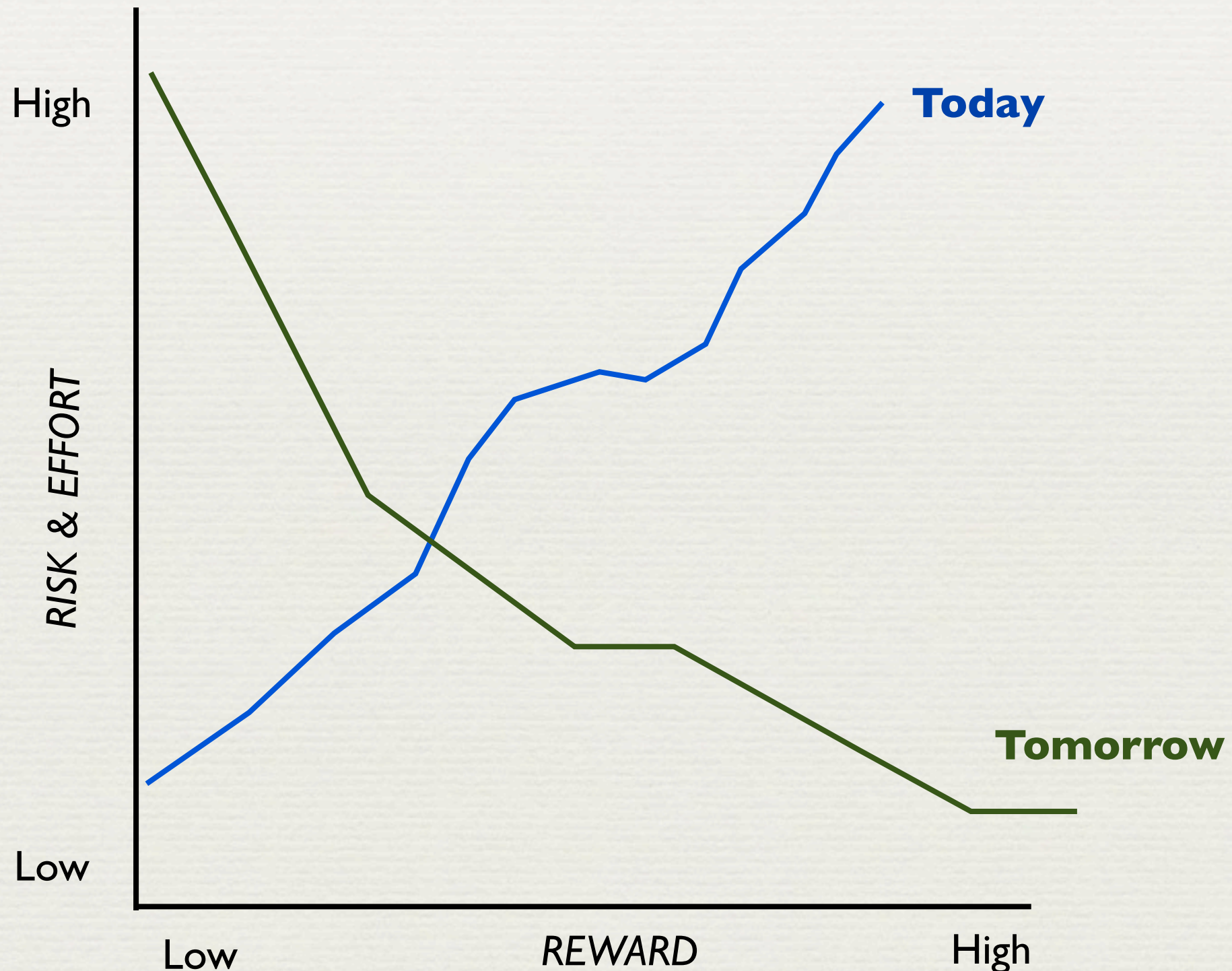


# Where We Stand Today





# Need to Reverse the Ease and Anonymity for the Attacker







# Leading from the Top



- ♦ **Anchor Leadership at the White House**

- ♦ Cybersecurity Coordinator does not have the positional authority required to catalyze change.

- ♦ **Strengthen Federal Leadership and Accountability**

- ♦ The Joint Interagency Cyber Task Force and the quarterly reports regarding CNCI are coming to a sunset.
- ♦ Compliance does not equal security; the Federal Information Security Management Act of 2002 must be updated and a measure and reward system (report card) should hold leaders responsible.

- ♦ **Review the Laws and Policies**

- ♦ The Cyberspace Policy Review identified scores of legislation that needed to be updated for the digital environment in which we operate.
- ♦ Over 50 pieces of legislation relating to Cybersecurity were introduced in the 111th Congress.

- ♦ **Elevate State, Local, and Tribal Leadership**

- ♦ Three independent organizations are trying to improve the situation: National Association of State Chief Information Security Officers (NASCIO); Multi-State Information Sharing and Analysis Center (MS-ISAC); and the Center for Internet Security.



*Bipartisanship is Required*



# Building Capacity for a Digital Nation

## ◆ Increase Public Awareness

- ◆ Despite frequent media articles, a national conversation is not happening.
- ◆ Cybersecurity Awareness Month (October) is not enough.

## ◆ Increase Cybersecurity Education

- ◆ Of the more than 3000 colleges and universities within the U.S., the Federal Cyber Service, Scholarship for Service and National Centers of Academic Excellence in Information Assurance fund less than 5%.
- ◆ Cyber Competitions such as the Air Force Association, SANS Institute and the Defense Cyber Crimes Center need more visibility (similar to the science competitions/fairs of the 1960s).

## ◆ Expand Information Technology Workforce

- ◆ “There are about 1000 security people in the U.S. who have specialized security skills to operate effectively in cyberspace. We need 10-30,000 more.” (Jim Gosler). We actually need 100s of thousands of people trained to protect our networked infrastructures and business operations.
- ◆ The DoD Information Technology Exchange Program (ITEP) should be evaluated as a national program and may be a model that could accelerate knowledge exchange.

## ◆ Promote Cybersecurity as an Enterprise Leadership Responsibility

- ◆ We must address the gap between threat, innovation, and competitiveness and begin a serious conversation about the material risk (realized or ignored) to our multi-national corporations.



*A National Conversation is Needed*

0, r | nāSh DgNā nr( S22, DC

K | aē, So, DgN2 | ,  
8 8 gi i aCagn gn (t, DC, r6Dæ( NgD2 | , 2 | Q Cæ, nr(

1, oD C n2Sāf, Si, C1 SnW Tan  
1, oD C n2Sāf, a | S, ho r Seh  
8rg22 | SD, (

2, n, DSh SH 1 Se6, W  
8 Q 2

Si, C, l, aC

6H

CSIS | CENTER FOR STRATEGIC &  
INTERNATIONAL STUDIES



# Sharing Responsibility for Cybersecurity

## Improve Partnership between Private Sector and Government

- ✦ The government's relationship with the private sector is paternal and unilateral. Effective partnership requires mutual respect and benefit by both parties.


## Evaluate Potential Barriers Impeding Evolution of Private-Public Partnership; the full gambit of market levers are not being considered

- ✦ Requires building trust relationships: Public-Private; Private-Private; and Public-Public.
- ✦ Addressing perceived weakness of FOIA, especially when dealing with sensitive proprietary information and vulnerabilities such as network breaches.
- ✦ Sharing information (threat, vulnerability, etc.) among industry partners might be viewed as “collusive” or contrary to antitrust laws.
- ✦ Sharing information with global corporations in a consistent manner with our Allies.
- ✦ Recognize and respect the: cost to industry: time (Executive Bandwidth); money, opportunity loss; reputation; political capital; positional pairing.

## Partner Effectively with the International Community

- ✦ Military and Civilian policy makers need to begin working together to prioritize requirements and align agendas, especially in this fiscally constrained environment.



© 2011 Hathaway Global Strategies, LLC.

 Workshop on Addressing Security Challenges on a Global Scale  
Session 5.1:  
Global Cybersecurity Information Exchange Framework

### Challenges in Sharing Security Information


Ian Bryant, NEISAS Project

7 December 2010 ITU, Geneva, CH

© MS3i 2008-9, NEISAS 2009-10  
[IAP\_2010\_G\_057]

IFP/WKP/FGS(2011)3



MULTI-DISCIPLINARY ISSUES  
INTERNATIONAL FUTURES PROGRAMME

OECD/IFP Project on  
“Future Global Shocks”

### “Reducing Systemic Cybersecurity Risk”

*Peter Sommer, Information Systems and Innovation Group,  
London School of Economics*

*Ian Brown, Oxford Internet Institute, Oxford University*

Contact persons:  
Pierre-Alain Schieb: +33 (0)1 45 24 82 70, [pierre-alain.schieb@oecd.org](mailto:pierre-alain.schieb@oecd.org)  
Anita Gibson: +33 (0)1 45 24 96 27, [anita.gibson@oecd.org](mailto:anita.gibson@oecd.org)

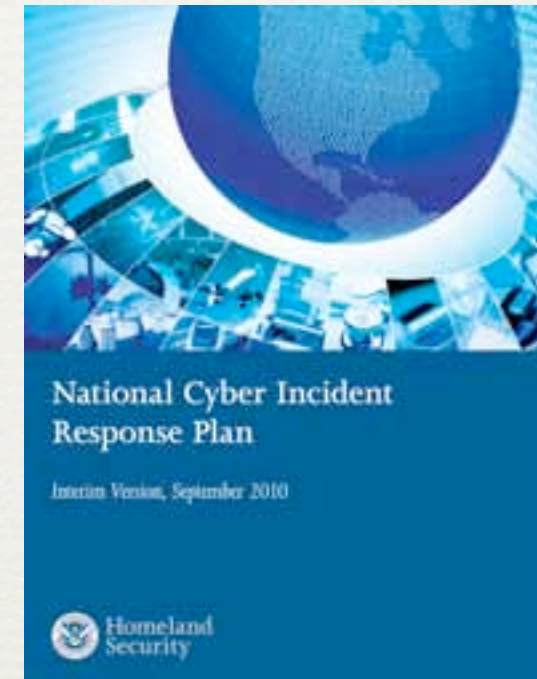
14th January 2011



# Creating Effective Information Sharing and Incident Response

## ♦ Build a Framework for Incident Response

- ♦ The NCIRP was developed with minimal private sector participation and is still in draft form. An Eligible Receiver like exercise may be required to understand the full requirements of an Incident Response Plan.
- ♦ Incident response requires engaging in a thoughtful discussion that develops a transnational approach to infrastructure protection that minimizes the dangers of attack and is inclusive of the private entities that will likely be called upon to take action against the perpetrators causing the disruption, degradation, or destruction.



## ♦ Enhance Information Sharing to Improve Incident Response Capabilities

- ♦ Tear lines are required to enable a useful information sharing partnership (Classified information and proprietary information; FS-ISAC/NSTAC recent pilot).
- ♦ Evaluate existing success models in the private-public partnership: Center for Disease Control, Amnesty International, International Civil Aviation Organization.



## ♦ Improve Cybersecurity Across All Infrastructures

- ♦ Regulatory CIP Standards need to be streamlined but appear to have positive affect.
- ♦ NIST needs to be pro-active and anticipatory of needs prior to spending resources (e.g., Smart Grid--American Recovery and Reinvestment Act of 2009).

Conficker Working Group:  
Lessons Learned

June 2010 (Published January 2011)



# Encouraging Innovation

## ✦ Link R&D Frameworks to Infrastructure Development

- ✦ Despite R&D \$585M plus up in FY 2010 budget, cyber R&D lacks direct link to infrastructure upgrades (Broadband to America, Smart Grid, NexGen Air Traffic Control, etc).

## ✦ Establish Identity Management as an Option

- ✦ A Draft National Strategy for Trusted Identities in Cyberspace is published and a new program office is being established at Department of Commerce, but it is unclear the regulatory authorities or approach that the government is adopting.

## ✦ Integrate Globalization Policy with Supply Chain Security

- ✦ The United States' ability to project power is wholly reliant on the strength of our IT sector. Other countries (China and Russia) are pursuing strategies that support their IT industry leadership, recognizing the importance to their overall national economic health. The United States needs to find equivalent market levers to shore up our indigenous IT companies and help drive focused R&D for the next generations of innovation with the goal toward building out a more secure resilient infrastructure.

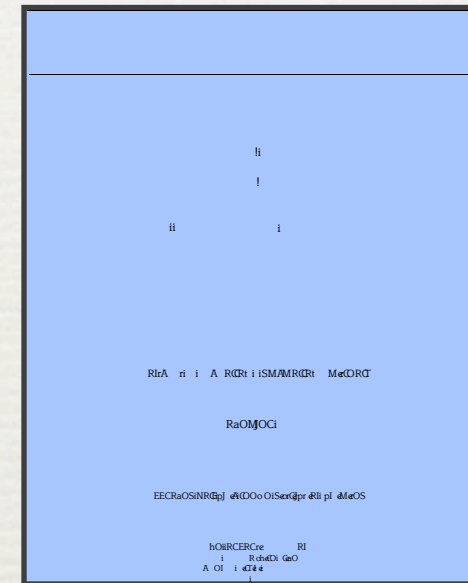
## ✦ Maintain National Security/Emergency Preparedness (NS/EP) Capabilities

- ✦ The rapid adoption of technology and growing migration of essential services to be delivered on Internet based infrastructure demands that the FCC or the law be modified to classify broadband and other Internet services as core telecommunications providers. This is important because as the communications infrastructure continues to converge and migrates from older to newer technologies, services like energy (Smart Grid) and public safety (voice over IP), will be carried over a communications network that may or may not be built to the same standards for which the traditional voice telephone system was built. Whether wireline or wireless, the FCC or the law needs to take a stance and assure that the carriers contribute to the security and resiliency of our communications infrastructure. After all, it is their pledge that they will deliver reliable service to their customers.



Homeland  
Security

November 2009



### National Strategy for Trusted Identities in Cyberspace

Creating Options for Enhanced  
Online Security and Privacy

June 25, 2010

Draft



# Recommendations

- ♦ The 112th Congress should champion transparency and discourse on cybersecurity by holding public briefings and hearings encouraging a dialogue about what is really needed to address the problem comprehensively.
  - ♦ Address the shortfalls in our current laws and consider providing government assistance to address the gap between threat, innovation, and competitiveness
  - ♦ Drive a new legislative conversation
- ♦ Examine how the Executive Branch's three Independent Agencies could serve as a catalyst for change and boost our national cyber defense immediately.
- ♦ Enlist and incentivize the private sector to understand and address the vulnerabilities and innovate our way through a solution.
- ♦ Develop and implement a broad-based awareness and education campaign for the U.S. population and other like-minded nations.



# Align Interests

Strategic Vision and Process  
Must Span Private and Public Sectors





# Options for Congress:

## Update and Leverage Existing Laws

Empower the Government	Assist Industry	Facilitate a Strategic Posture
Federal Information Security Management Act of 2002	Economic Espionage Act of 1996	National Defense Production Act of 1950
Electronic Communications and Privacy Act of 1986	Broader Application of [Rights and Property] Provider Exception	
Stored Communications Act of 1986	Telecommunications Act of 1996	
Computer Fraud and Abuse Act of 1986	Securities Exchange Act of 1934	



# Computer Fraud and Abuse Act of 1986

## ♦ **What Needs to Change:**

- ♦ The definition of a protected computer is too narrow and should be expanded to include any public sector or private sector computer. Ideally, protected computers would include all of our corporate computers as well (defense industrial base). “Protected computers” is a term used in Title 18, Section 1030, which prohibits a number of different kinds of conduct, generally involving unauthorized access to, or damage to the data stored on, “protected computers”.
- ♦ Additionally, CFAA should be amended to criminalize the creation and distribution of malware. Finally, Congress should increase the penalties (monetary and prison sentences) associated with activities that disrupt or damage protected computers (the activities outlined in the statute).

## ♦ **Why Now?**

- ♦ Why does existing law treat “federal computers” and “financial systems” differently than others? The Congress should provide that hacking is illegal, regardless of domain, and that the *effects* are what bears out the penalties, not the location, path taken (interstate) or victim (government entity, financial institution, etc). It is time that the government declares that all entities (.mil, .gov, .com, .edu, etc.) are “interconnected” and establish stiffer penalties to better deter this malicious behavior.



# Economic Espionage Act of 1996

- ♦ **What Needs to Change:**

- ♦ The definition of trade secret is consistent with the Uniform Trade Secrets Act, which states that the information is subject to reasonable measures to preserve its secrecy and derives independent economic value from not being generally known to or ascertainable by the public. But the threshold for protection is too high because it requires that industry at the onset of the development of information or idea protect it as a trade secret. Addressing the broad-based economic industrial espionage that we are observing on our corporate networks requires that the government lower the threshold for a trade secret or add a threshold around proprietary information.

- ♦ **Why Now?**

- ♦ No matter what name we have for it: illegal copying of information, stealing data, cyber espionage, it should be deemed illegal and have a penalty associated with it. If this law were coupled with changes to the CFAA, it would enhance our deterrence posture.



# National Defense Production Act

## ♦ **What Needs to Change:**

- ♦ Leverage the authorities contained in the NDPA to help subsidize and accelerate government access to commercial production technologies and capacity because the pace of innovation and marketplace dynamics are threatening U.S. leadership in communications, computing, networking and security technologies.
- ♦ The NDPA also provides for anti-trust protection for voluntary agreements among business competitors to enable cooperation to plan and coordinate measures to increase the supply of materials and services needed for national economic and defense purposes. It also authorizes the establishment of the National Defense Executive Reserve (NDER) (some would call the Civilian Cyber Reserve Corps), a cadre of persons with recognized expertise for employment in executive positions in the Federal government in the event of an emergency. One could argue that the information technology exchange program (ITEP) initiative could be the long-term pipeline for this NDER.
- ♦ The government should consider protecting our national telecommunications infrastructure and recognize that it is vital to U.S. interests. The discussion should include the primary and subsidiary providers and suppliers. Furthermore, the government should consider a broad definition of the IT environment to include current and future converged communications infrastructures and services. It may be wise to draw upon the Electronic Communications and Privacy Act (ECPA) definition: “including voice over Internet-Protocol communications; by the aid of wire, cable, or other like connection including wireless connections such as mobile phones, satellites, and fiber-optic cables.”

## ♦ **Why Now?**

- ♦ The United States’ ability to project power is wholly reliant on the strength of our IT sector. Other countries (China and Russia) are pursuing strategies that support their IT industry leadership, recognizing the importance to their overall national economic health. The United States needs to find equivalent market levers to shore up our indigenous IT companies and help drive focused R&D for the next generations of innovation with the goal toward building out a more secure resilient infrastructure.



# Proposed Focus Areas for the 112th Congress

- ✦ What is the national security threat to industry?
- ✦ Should the Economic Espionage Act of 1996 be reviewed due to the significant quantity of information being stolen or illegally copied from our companies that has reached a qualitatively unacceptable threshold?
- ✦ Should we consider a new statute that criminalizes the creation and distribution of malware?
- ✦ Is it time to review the need for an industrial policy that helps our companies maintain global competitiveness and continue to grow jobs in the United States by repatriating their foreign source income?
- ✦ Would strengthening the regulatory oversight of the SEC, FCC, FERC, or FTC help or hurt the situation? How are these regulatory bodies using their current authorities to address the situation? Are these regulatory bodies working together?
- ✦ As we continue to invest in digitizing our infrastructures and everything behind it, what are the attendant investment requirements needed to assure its integrity and security?
- ✦ Should Internet Service Providers assume more responsibility for providing enhanced security services to their customers and report all security incidents to an appropriate government entity?
- ✦ What are other countries doing to strengthen their information and communications infrastructures and posture?



# Options for the Executive Branch: Turn to the Independent Agencies

- ♦ **Securities and Exchange Commission (SEC)**: Ask the Securities and Exchange Commission (SEC) to examine and evaluate requiring Chief Executive Officers (CEOs) to attest to the integrity of their company's information infrastructure. The SEC could open a dialogue with industry, through an administrative notice to industry informing them that the SEC will consider making a rule regarding the thresholds of materiality risk in the area of information security. This notice would inform registrant's that the SEC would like an assessment by management of the effectiveness of the registrants controls over the protection of proprietary and confidential personal data, mission critical systems and in the event of an incident, what is the registrant's incident response and remediation capability.
- ♦ **Federal Communications Commission (FCC)**: Enlist private sector talent and requiring the core telecommunications and ISPs to shoulder a broader burden of protecting our infrastructure. The major telecommunications providers and ISPs, collectively, have unparalleled visibility into global networks which enable them with the proper tools to detect cyber intrusions and attacks as they are forming and transiting towards their targets.
- ♦ **Federal Trade Commission (FTC)**: Consider a more proactive initiative and require all e-commerce transactions carry a warning banner or label that informs consumers that they should recognize that they are assuming a risk by conducting e-transactions and that their transaction may not be secure and in fact could lead to compromised credentials. This can be compared to the tobacco label of "smoking is hazardous to your health" or the warning label on your bottle of wine that says "consumption of alcohol may cause health problems."

More information: <http://www.acus.org/publication/creating-demand-curve-cybersecurity>



# Summary

- ♦ Begin an honest conversation about what is happening in the United States to our long-term strategic posture (denial will not lead to recovery).
- ♦ Reconcile the tension between economic recovery and national security needs.
- ♦ Retard the quick-to-adopt movement of all critical infrastructures to rely on Internet based protocols and technology.
- ♦ Enlist and incentivize the private sector to understand and address the vulnerabilities and innovate our way through a solution.
- ♦ Congress should clarify jurisdictional responsibility and legislate new authorities.
- ♦ Review regulatory authorities (FCC, FTC, SEC, FERC) and demand coordination across Internet jurisdictional overlap; Legislation has not kept pace with technology, making regulation difficult.
- ♦ State U.S. policy of what is tolerable (crime, espionage, and armed aggression) and impose costs if threshold is crossed.



# Recent Hathaway Publications and Speeches

- ✦ [http://belfercenter.ksg.harvard.edu/experts/2132/melissa\\_hathaway.html](http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html)
- ✦ [http://media.techtarget.com/searchSecurity/downloads/F\\_1009\\_ISM\\_eM.pdf](http://media.techtarget.com/searchSecurity/downloads/F_1009_ISM_eM.pdf)
- ✦ <http://www.washingtontimes.com/news/2009/nov/25/a-safe-harbor-for-our-foes/>
- ✦ <http://blog.executivebiz.com/five-myths-about-cybersecurity/6102>
- ✦ <http://www.thenewnewinternet.com/2010/05/07/why-successful-partnerships-are-critical-for-promoting-cybersecurity/>
- ✦ <http://belfercenter.org/publication/20133/cybersecurity.html>
- ✦ <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/28/AR2010052803698.html>
- ✦ [http://www.govinfosecurity.com/articles.php?art\\_id=2627](http://www.govinfosecurity.com/articles.php?art_id=2627)
- ✦ <http://www.govconexec.com/2010/06/13/your-organizations-it-security-reflects-on-you/>
- ✦ <http://www.federalnewsradio.com/?nid=17&sid=2042610>
- ✦ <http://www.scientificamerican.com/article.cfm?id=power-hackers>
- ✦ <http://www.sais-jhu.edu/publications/saisreview/current/hathaway.html>
- ✦ <http://www.acus.org/publication/creating-demand-curve-cybersecurity>
- ✦ <http://www.umuc.edu/orkandlecture/>
- ✦ <http://news.bbc.co.uk/2/hi/programmes/newsnight/9393765.stm>