# Cyber Security
## An Economic and National Security Crisis

by Melissa E. Hathaway
Senior Advisor to the Director of National Intelligence
and Cyber Coordination Executive

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 an unprecedented scale by a growing array of state and non-state actors. Our corporate intellectual property is being stolen and no sector is without compromise (e.g., information technology, bio-technology, defense industrial base, financial, transportation, energy, etc.). Further, our government networks are being targeted to steal sensitive information and gain understanding of mission critical dependencies and vulnerabilities. Additionally, we are finding a persistent presence on these networks and we cannot say with assurance that a network that has been penetrated has not been infected with hidden software that could be triggered in a crisis to disrupt or destroy data or communications. Over the past year, this malicious activity has grown more sophisticated, more targeted, and more serious, and we expect these trends to continue. It is no longer sufficient for the U.S. government to discover cyber intrusions in its networks, clean up the damage, and take legal or political steps to deter further intrusions. The U.S. must take action to protect the critical components upon which our economy, government, and national security are based from potential exploitation, disruption or destruction.

## THE THREAT IS REAL AND GROWING

We face a dangerous combination of known and unknown vulnerabilities, strong adversary capabilities, and weak situational awareness. Both state and non-state adversaries are targeting our information systems and infrastructure for exploitation and potential disruption or destruction. The classes of adversaries include individuals, hacker groups, terrorist networks, organized criminal groups, rogue states, and advanced nation states. Each has its own technical sophistication. We must develop the capabilities to counter each. Nation states, including but certainly not limited to Russia and China, are targeting our government and private sector information networks to perform military style reconnaissance and gain competitive advantage for their commercial sectors. Terrorist groups, including Al-Qa'ida, Hamas, and Hizballah, have all expressed a desire to utilize cyber means to target the United States.[1] Criminal elements are showing a growing level of sophistication in technical capability and are performing myriad illicit cyber activities to include credit-card fraud and extortion. In fact, the cyber underground economy is growing at an unprecedented pace and is financing some terrorist and nation state activity.

The motives of these adversaries widely range from curiosity and prestige—at the hacker end of the spectrum—to industrial espionage and subversion of our national security interests by hostile nation states at the other end. We must be able to detect and prevent these intrusions from whatever the source before they can achieve significant damage. Information is a strategic asset, both for the government and our nation's commercial enterprises. It is clear that our adversaries are targeting this information as well as its related infrastructure.

### The Need for a National Approach that Embraces the Scale and Nature of the Threat

The exponential use and reliance upon electronic information and the Internet coupled with the threat posed by malicious state and non-state actors has reshaped our collective vulnerability. Undoubtedly policies and authorities for responding to those risks have not kept pace, and in fact may be falling further behind. The interconnectedness and interdependencies of the Internet allows for a number of individuals with a minimal budget, technical knowledge, and tools to inflict severe damage upon state powers by holding critical infrastructures at risk. The ability to shield one's identity by utilizing today's anonymous Internet technology means that a cyber intruder may be anything from a "lone gunman" to a well-financed nation state.

1. Director of National Intelligence. World-wide Threat Testimony. February 2008.

Some would say this is a strategic inflection point; we either change the path we are on—or lose.[2] Information is our strategic asset. We need an integrated response that builds upon a deep understanding of the technology and bridges our offensive and defensive missions to enhance our national and economic security for the long term.

An effective defense requires a good understanding of what the offense brings to the game: Attacks come over the Internet, via insiders, through the supply chain, and from almost any device used to import data or software into a system.[3] In a globalized IT market, our adversaries are exploiting our broad exposure and can: steal information from a target; corrupt the integrity of the information; deny the owner the use of the system; and/or destroy or deliberately insert erroneous data to render the system unreliable or inoperable. This latter threat –the inability to trust the integrity of our digital data-- is of increasing concern because of the potential impact on U.S. and the global systems should the perpetrator be successful.

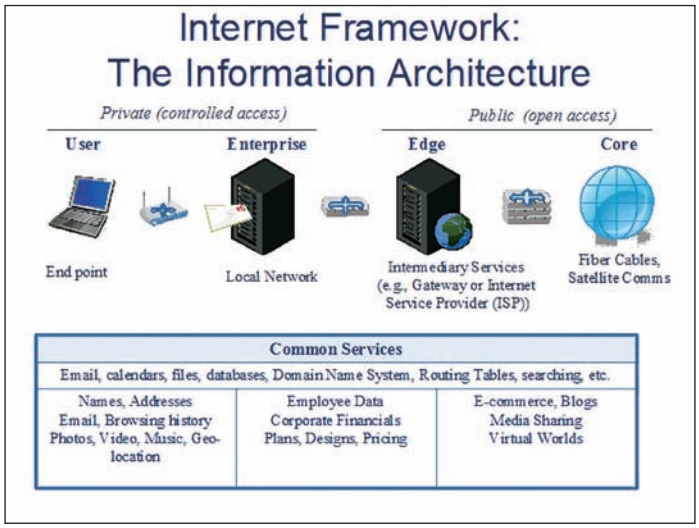


*Figure 1*: How a User Interfaces with Internet Technology.

**The Business of America is conducted on the Network—and its security is being driven by Global IT companies. For the Government to be able to predict and mitigate nation state threats to our shared infrastructure requires an understanding of where industry is taking the technology**[4]

Sophisticated adversaries can take advantage of the global IT market to operationally introduce exploitable vulnerabilities into the critical systems of their target. Countering this requires understanding:

- Who are the technology leaders in the marketplace and what are their connections and dependencies on foreign governments?
- What technologies are achieving market dominance?
- What are the areas for technological innovation that can disrupt current market leadership or create game changing performance?
- What U.S. mission critical applications are using these technologies?
- Where is there foreign leverage in the life cycle of these products?
- Where are the opportunities to place strategic bets?

Addressing these questions requires a simple description of how people interface with the technology, an understanding of how technology is converging and a way to think about managing the inherent risks. For the purposes of this paper, a simplified model of the flow of information from the individual to the user to the Internet was developed to help convey these issues, as presented at left in *Figure 1*.[5]

There are at least three dimensions of the information architecture that must be considered. The first dimension is the functional and physical elements of the architecture. How does my information flow from end to end? What others systems am I connected to? What are those systems connected to? People consciously use networked devices like PCs, laptops, BlackBerries, PDAs, and cell phones. Less apparent technologies that people use that connect to the information enterprise include cable ready TVs, voice over Internet protocol (VoIP) phones, TiVos, and gaming consoles including Wii and Playstation. These devices transmit email, calendars, photos, music, employee data, and other common services and data.

2. Andrew S. Grove. *Only the Paranoid Survive*. New York, NY: Currency and Doubleday Publishing, 1999. Page 33.
3. James R. Gosler. "Digital Dimension," in *Transforming U.S. Intelligence*. Edts, J.E. Sims and B. Gerber, Washington, DC: Georgetown University Press, 2005. Pages 96-114.
4. Bruce Berkowitz. "Maintaining the American Advantage," *Foreign Policy Research Institute*, electronic subscription, June 2008.
5. The technology presentation was developed as part of a study conducted by the Office of the Director of National Intelligence, Integrated Concepts Development Office, completed in May 2008.

The information travels through local area networks, or the private wiring that connects your home, business, or mobile user to the Internet.

Once the data leaves the private network (home, business, or mobile user) it usually travels to the Internet via an Internet Service Provider (ISP). The connection can be wired (phone line, cable, fiber optic) or wireless (satellite, cellular, WiFi). The data now exists in a public area, possibly even in an international location. In order for the information to get to its end destination, it must also travel across the Internet backbone. This is the network of high speed fiber optic cables that span the world. Within the United States, there are a number of 'Tier 1' carriers, including, AT&T, Verizon, Sprint, Qwest, Global Crossing, Savvis, and Nortel. These global companies provide the highspeed optical cables that service the country's movement of data.

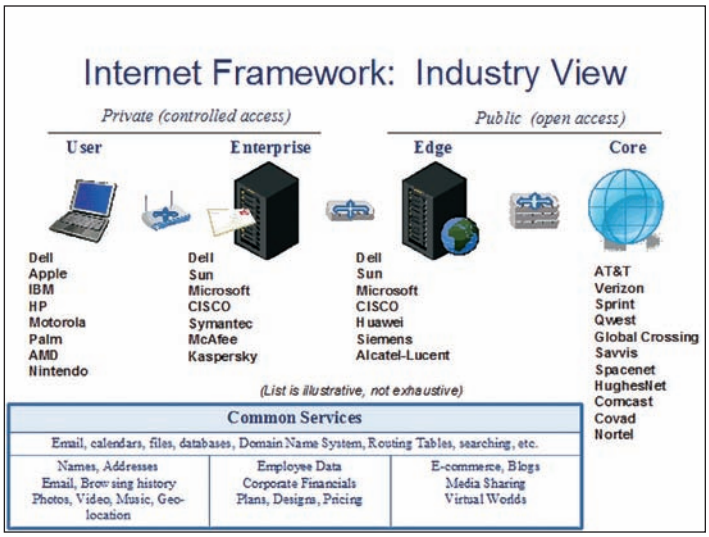


*Figure 2*: Private Sector Provider of Services within Information Architecture

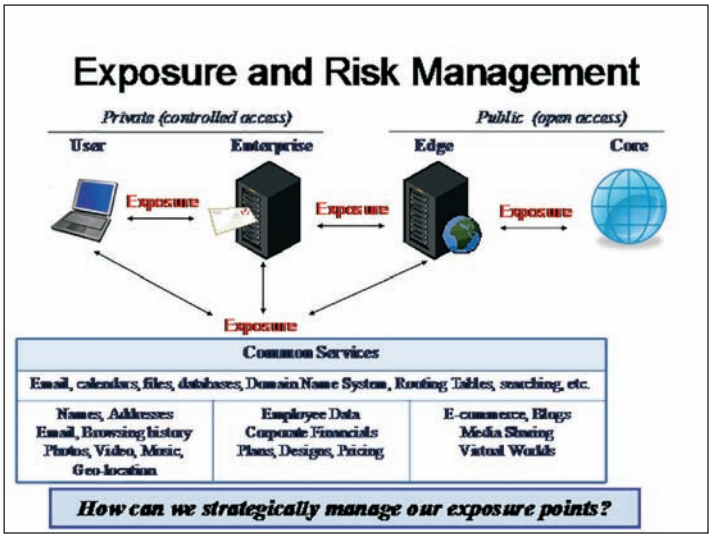


*Figure 3*: Understanding Risk and Exposure Across the Information Architecture

The second dimension of understanding the information architecture requires understanding the market view, both from a corporate and international perspective. We need to understand: Who designed the technology? Who built the technology? Who operates and maintains the technology? Who upgrades the technology? Who retires the technology? We need this understanding because each of these points of interface of the device with the hardware, software, and technology design, presents an opportunity to introduce or exploit vulnerability. Often, technology dominance reinforces the power of the industry leader, however we are increasingly seeing government influence to help disrupt current market forces to gain competitive and economic advantage – and potentially introduce or exploit cyber vulnerabilities. Figure 2 helps illustrate the plethora of market vendors of software and hardware who move the information between the user and the Internet.

The third dimension of understanding the information architecture requires understanding the organizational and governance approaches to risk management. Specifically, this requires understanding relationships within and across the information architecture. Risk is a function of multiple components: threat, vulnerability, and consequences.[6] Today, risk is distributed across all dimensions of the information architecture, and we must recognize how and where vulnerabilities and exposure exist in order to maintain a better defensive posture. *Figure 3* depicts exposure points within the information architecture.

Information technology and the Internet have become the fabric of our way of life. Our communications, commerce, transportation, banking, healthcare, emergency response, disaster relief, defense, utilities and more depend on it. A growing array of state and non-state actors are using the Internet and the information technology to project power to meet varying objectives. Whether for economic advantage or national security purposes, our government and private sector networks and information are being exploited at unprecedented scale. And we are not alone. Malicious activity in cyberspace is a threat to everyone. All of us have been victims of cyber attacks affecting our critical information and infrastructures

6. Brian Contos, William Crowell, Colby DeRodeff, Dan Dunkel, and Eric Cole. *Physical and Logical Security Convergence: Powered by Enterprise Security Management*. Elsevier, Inc., 2007. Page 57.

over the past several years, some of which have been very costly.

### Information Theft: Espionage and Competitiveness

The most common threat involves stealing information from a target personal device, system or network. The examples of such theft increase daily and the effects are economic, competitive, and personal. For example, TJX, the operator of discount chains T.J. Maxx and Marshalls, indicated its computers were compromised via interception of the wireless signal from its point of sale credit card terminals. Data compromised between 2003-2006 may have affected as many as 95 million consumers.[7] More recently, during a four-month period, Hannaford Food suffered a malicious code-induced security breach which compromised personal identifying information (credit cards and medical records) of 4.2 million customers. This breach, which is now linked to over 1,800 cases of fraud, occurred despite the company's adherence to industry standard data security practices.[8] In another example, a disgruntled employee was charged with the theft of 320,000+ sensitive company files using a thumb drive to move the files out of the corporate system and devices. Boeing estimated that if the stolen documents were given to competitors, it could have cost the company between $5 billion and $15 billion in lost revenue.[9] Finally, one of the most sophisticated exploitations of computer data is believed to have been enabled via deliberate alteration of the product somewhere in the supply chain prior to marketplace use. Additional unauthorized circuitry was added to Personal Identification Number (PIN) keypads used in Point of Sale transactions in British stores. When consumers entered their PIN's (which are encrypted on bank or credit cards) to complete purchases, the 'plain text' version of the PIN along with their account number was captured, hidden in encrypted form on the compromised hardware, and sent electronically to a computer server. The information was used to skim from or even drain the victims' bank accounts. The attack may have taken over a year to plan and execute and was likely executed by well-funded organized criminals.[10]

### Information Disruption: Corrupt the integrity of the information

While information theft is occurring daily, information disruption and the corruption of data integrity is also being seen around the world. For example, in 2000, a disgruntled contractor used a wireless access point to launch a series of Supervisory Control And Data Acquisition (SCADA) attacks against the municipal water treatment system in Maroochy Shire, Australia, causing the spillage of millions of liters of raw sewage into local rivers, parks, and the grounds of a luxury hotel.[11] The intruder chose to target sewage disposal, but could as easily have altered production of potable water to produce unsafe—or even poisonous—drinking water. The United States Navy faced a similar problem in 2006 when a disgruntled contractor inserted malicious code into five computers at the U.S. Navy's European Planning and Operations Command Center in Naples, Italy. Two of the computers were rendered inoperable by the action; had the program been run on the other three infected machines, the result would have the shutdown of the network that tracks the locations of U.S. and NATO naval ships and submarines in the Mediterranean Sea and helps prevent military and commercial vessels from colliding.[12] And as recently as this spring, a low-level trader at French bank Societe Generale circumvented IT security by stealing computer passwords, sending fake e-mail messages, and illegally accessed the bank's computer system to exceed trading limits and cover up his actions. The unauthorized trading positions he built up totaled $73 billion, and cost the bank $7.2 billion.[13] This action also caused instability on the United States New York Stock exchange.

It is not just information integrity that is being challenged. We are also observing counterfeit technology being introduced into the marketplace, which may be introducing further vulnerabilities into our information systems and architectures. For example, counterfeit Cisco network products have been purchased

7. Paul F. Roberts. "Retailer TJX reports massive data breach" *http://www.infoworld.com/article/07/01/17/HNtjxbreach_1.html*
8. Christina Vieders. "Standards Not Enough in Hannaford Bros. Data Breach" *Supermarket News*. 14 April 2008. Also in March 19, 2008 (Computerworld)
9. Sharon Gaudin, *Information Week*. July 11, 2007 URL: *http://www.informationweek.com/story/showArticle.jhtml?articleID=201000820*
10. Zjan Shirinian. "Supermarket shoppers fleeced in debit card fraud." *Barking and Dagenham Recorder*. 15 May 2008 Discussions with Stephen Spoonamore Spring 2008.
11. Tony Smith. "Hacker jailed for revenge sewage attacks." *The Register*. 31 October 2001. *http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/*
12. Tim McGlone. "Navy contractor charged with sabotaging computer system" *The Virginian-Pilot*. 27 June 2006.
13. Julia Werdigier. "Trading scandal diverts attention from Société Générale's subprime losses." *The International Herald Tribune*. 29 January 2008.

by unwitting U.S. government and private sector customers. The counterfeit products have been linked to the crash of mission-critical networks, and may also contain hidden "backdoors" enabling network security to be bypassed and sensitive data accessed. As of February 2008, the Federal Bureau of Investigation and its foreign partners have conducted over 400 seizures of counterfeit Cisco network hardware with an estimated retail value of more than $76 million.[14]

### Information Denial: Deny the Owner the Use of the Information or System

One of the most famous examples of denying information and use of a system is the Estonia case of distributed denial of service. On 27 April 2007, pro-Russian nationalists launched a distributed denial of service attack[15] against Estonia. Using botnets,[16] the attack denied users access to key institutions including banks, the networks of the Estonian president and Parliament, virtually all government ministries, political parties, news organizations, Internet providers, mobile phone networks and Estonian cyber response services.[17] This attack was technically meager, and one of this scale could be mounted by hiring criminal hackers for a few hundred, or thousand, dollars. A denial-of-service attack on the London Stock Exchange web site in 2007 succeeded in disrupting services alerting investors of major announcements and changes in stock values for almost 48 hours.[18]

South America, Southwest Asia and other regions have been targeted and suffered compromise of key infrastructures. Internet-based attacks on SCADA systems, aimed at extorting money, have resulted in electrical power blackouts abroad.[19] Consequences of a cyber attack on U.S. SCADA systems could vary widely, given the way such systems are integrated into our critical national infrastructure, but could be long lasting if critical components were physically damaged or destroyed.

### Information Destruction: There is No Greater Threat to Our Sovereignty

Some adversaries have ambition to destroy or, perhaps worse, deliberately insert erroneous data to render systems inoperable and information unusable. This is an increasing concern because of the potential impact on U.S. and global systems should the perpetrator be successful. How does a nation attribute and deter such behavior? How long does it take to recover from the effects of the following scenarios? What if:

- Financial records (bank accounts etc.) were altered or destroyed?
- Medical records were damaged or destroyed?
- DoD logistics were rendered ineffective?
- Air traffic control systems were corrupted?
- Pipeline or rail control was interrupted or corrupted?

Our risks are increasing dramatically and the trend is likely to continue as our information architecture is increasingly being interconnected to improve efficiency, response time and information sharing. But as the private sector drives the architectural IT security that increasingly provides the foundation for critical operations in both business and government, there is no single governing body that has cognizance over the end-to-end architecture, and therefore no one entity is responsible or accountable for managing the risk and exposure. Our vulnerability in this regard also is being exacerbated through globalization. Through acquisitions, off-shore development driven by inexpensive labor, and multinational growth, our exposure to foreign influences continues to increase.

### A Strategic Partnership is Required to Close the Gap

The U.S. government needs to generate and share with the private sector an operational understanding of how adversaries create and exploit our cyber vulnerabilities. We must disclose the extent and reach of their capabilities. We need to inform the private sector what is being targeted by our adversaries (usually intellectual property) and to the extent we know, why. Finally, the government must begin to share the extent of resources at risk, the risk-reward construct of inaction vs. action, and what other partners may be involved. This shared understanding and dialogue should influence our defensive strategy and collective resource allocation.

The U.S. government, as well as the private sector,

14. "FBI: China may use counterfeit Cisco routers to penetrate U.S. networks" *World Tribune*. 15 May 2008.
15. Distributed Denial of Service: Repeated communication attempts targeting a network resulting in degradation of communication ability if not shutting down the targeted computer.
16. BOTNET: A network of surreptitiously compromised computers that can be remotely manipulated.
17. Joshua Davis. "Hackers Take Down the Most Wired Country in Europe." *Wired Magazine* Issue 15.09. 21 August 2007.
18. Tom Young, London Stock Exchange cyber attack *Computing, 20 June 2007.*
19. Andy Greenberg. "Hackers Cut Cities' Power." *Forbes*. 18 January 2008.

needs to change the way it does business, and recognize that a vulnerability to one affects us all. Private sector risk models are inadequate for national security and critical systems—and therefore the government must define higher standards and specifications. The government must also incubate and create incentives for game-changing technological innovation. Industry, which often leads the government in technical advice and advancement, needs to rise to the challenge of producing innovative, game-changing technologies that enable us to operate safely in cyberspace. Together, we must look toward creative partnerships to explore technology development, enhance product development, and build trust into a system created from untrustable components. Security and risk understanding must be built into our collective next-generation information architectures. Only in partnership will we be able to foster our economic competitiveness and retain consumers' freedom to "mix and match" vendors and products while maintaining security of our information and information systems.

Internationally, we should look toward invigorating our traditional alliances and creating new ones that share the responsibility for securing cyberspace and enhancing our global competitiveness. While industry must invest to mitigate the risk and cost of crime, nations must invest to mitigate the risk and cost of nation-state activity against sovereign territory and assets. We need to bring action, accountability, and unprecedented public-private partnerships and international alliances to bear to solve this problem for the long-term.

We are late in addressing this critical national need and our response must be focused, aggressive, and well-resourced. Consequently, an enduring strategic framework must become a long-term national priority.

Melissa E. Hathaway is Senior Advisor to the Director of National Intelligence (DNI) and Cyber Coordination Executive. She chairs the National Cyber Study Group (NCSG), a senior-level interagency body instrumental in developing the Comprehensive National Cybersecurity Initiative (CNCI). In January 2008, Hathaway was appointed Director of the Joint Interagency Cyber Task Force (JIACTF), to coordinate and monitor the CNCI. Prior to her appointment as Senior Advisor, Ms. Hathaway was a Principal with Booz Allen Hamilton, focused on information operations and long range strategy and policy support. She supported key offices within DOD and the Intelligence Community, including U.S. Strategic Command, U.S. Pacific Command, the Office of the Under Secretary of Defense for Intelligence, CIA, DIA and the ODNI. Her work included the design and development of novel techniques for mapping social, business process, and infrastructure relationships as well as evaluating new force options across the electromagnetic spectrum.

Pretexting: pretending to be someone you're not, to get something you shouldn't have, to use against the giver or others.

Social engineering: a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim.