Strategic Advantage: Why America Should Care About Cybersecurity

BELFER CENTER
for Science and International Affairs
John F. Kennedy School of Government
Harvard University

Melissa E. Hathaway

Harvard Kennedy School
October 2009

Strategic Advantage: Why America Should Care About Cybersecurity

By Melissa E. Hathaway

The internet is an interconnected series of networks--where it is difficult to determine where private security threats end and public ones begin. These networks deliver power and water to our households and businesses, enable us to access our bank accounts from almost any city in the world, and transform the way our doctors provide healthcare. For all of these reasons, we need a safe Internet with a strong network infrastructure. Our nation needs to take prompt action to protect cyberspace for what we use it for today and will need in the future. I believe that we are at a strategic inflection point--and we must band together to understand the situation and ascertain the full extent of the vulnerabilities and interdependencies of this information and communications infrastructure that we depend upon. As I reflect on the situation, one of the key recurring questions is whether we really understand the intersections of our critical assets and networks and how we as entities interface with the communications infrastructure and the energy grid and other critical services that are provided on that backbone of interdependent networks.

This is a multi-dimensional problem and it is not just one network that is threatened. It is as if we are in the middle of the grand Chinese strategy game of Wei-Ch'i (or Go, as it is more commonly known in western world) and do not even realize it.[1] Using a 19x19 grid the rules of Wei-Ch'i are simple but the execution of the practical strategy can be extremely complex because the number of possible moves each turn can range from 150 to 250, and rarely falls

[1] The widely marketed game Othello, also known as Reversi, is a much simplified derivation of Wei-Ch'I, in which players use black and white playing pieces and attempt to engulf their competitor's pieces, thereby turning them into their possession. For more information on Othello, *see* http://en.wikipedia.org/wiki/Reversi.

below 50.[2] By way of comparison, the average number of possible moves in a typical game of chess is 37.[3] Many people consider Wei-Ch'i to be the world's greatest strategic skill game, far surpassing Chess in its complexity and scope. Wei-Ch'i means "surrounding game" or "surrounding chess" and the object is simply to capture territory by placing down stones on the board (in this case our networks) and control a larger portion of the board than the opponent. A stone or a group of stones is captured and removed if it has no empty adjacent intersections, the result of being completely surrounded by stones of the opposing color. Placing stones close together helps them support each other and avoid capture. On the other hand, placing stones far apart creates influence across more of the board. Part of the strategic difficulty of the game stems from the need to find a balance between these conflicting interests. Players strive to serve both defensive and offensive purposes and choose between tactical urgency and strategic plans.[4] The best of the Wei-Ch'i masters play multiple strategies on multiple boards--all at the same time.

The complexity and scope of the cybersecurity challenge mirrors the complexity of Wei-Ch'i, and requires that we partner to build more effective solutions and to develop and implement a sophisticated strategy. In this regard, government should work creatively and collaboratively with the private sector to tailor and scale solutions that take into account both the need to exchange information and protect public and private interests. These are some of the core tenets of the Obama Administration's 60-Day Cyberspace Policy Review—which set forth a blueprint

[2] *See* http://en.wikipedia.org/wiki/Go_(game).

[3] Raymond Keene and David Levy. How to Beat Your Chess Computer, Batsford Books (1991) at 85.

[4] To secure an area of the board, it is good to play moves close together; however, to cover the largest area, one needs to spread out, perhaps leaving weaknesses that can be exploited. Playing too low (close to the edge) secures insufficient territory and influence, yet playing too high (far from the edge) allows the opponent to invade. *See* http://en.wikipedia.org/wiki/Go_(game).

for the way forward for America. It outlines how we can move from operating with little situation awareness and in the red—to regaining our strategic initiative, moving America back into the black.

In a globalized IT market, our adversaries (Wei-Ch'i masters) are exploiting our broad exposure and they are stealing our information. These adversaries corrupt the integrity of our information, can deny the owner the use of the information or the system and can destroy or deliberately insert erroneous data to render the system unreliable or inoperable. Think of these as the counters on the boards. The threats are real and growing at a velocity and volume that keeps many of us awake at night. We have witnessed countless intrusions where criminals steal hundreds of millions of dollars and nation states steal intellectual property and sensitive military information.

This paper highlights a few examples and strategy boards that I believe are being played in this very real world game of Wei-Ch'i.

Board One: The Government Networks

Government networks are being targeted by well-resourced and persistent adversaries who steal our sensitive information to gain a glimpse into our mission critical dependencies and vulnerabilities. As Secretary Gates has said publicly, our defense networks are "under cyber-attack virtually all the time, every day."[5] His deputy recently echoed that warning, stating that

[5] http://www.cbsnews.com/stories/2009/04/21/tech/main4959079.shtml.

our networks "are probed thousands of times every day. . . And the frequency and sophistication of attacks are increasing exponentially."[6]

As President Obama acknowledged in his groundbreaking speech on May 29, 2009, we experienced one of the most significant attacks on our military networks last year. Several thousand computers were infected by malicious software, forcing our troops and defense personnel to give up their external memory devices and thumb drives—changing the way they use their computers every day.

Earlier this year, our networks were threatened by the Conficker worm, a pervasive computer virus that has been described as "the largest computer worm infection since 2003."[7] Many companies across the United States participated in the *Conficker Cabal* to identify the vulnerabilities and prepare technical solutions (patches). The Conficker worm is a self-replicating program. It takes advantage of networks or computers that have not kept up to date with the security patches – largely for computers using *Windows* operating systems. It can infect machines from the Internet or hide on a USB stick, carrying data from one computer to another. Conficker could be triggered to steal data or turn control of infected computers over to amassing Zombies into a botnet.

The botnet armies are still growing and Conficker has not yet been resolved. It has been estimated that millions of machines worldwide are infected, and about one in five business computers still lack the patch for this *Windows* bug that first was detected in November 2008.

[6] http://www.defenselink.mil/speeches/speech.aspx?speechid=1365.
[7] http://en.wikipedia.org/wiki/Conficker.

And despite advanced warning and instructions on how networks could be protected, the government did not have a coordinated plan for agency responses had the Conficker worm been weaponized on April 1, 2009 as some had predicted.

More recently, during the July 4th holiday weekend, the United States and South Korea began suffering from a distributed denial of service attack against thousands of computers and websites. Industry self organized to help identify the origin and character of the threat. Internet service providers (ISPs) in five countries identified and shut down a number of control hosts. However, even as of the publication of this paper, we still do not know exactly who was behind the attacks—or even how many control hosts were driving the attacks against our infrastructures.

How is this relevant to Wei-Ch'i? We have no real process or procedure for pooling our information between industry and government, let alone across borders with our Allies. We are being surrounded and paralyzed by pretty simple tactics, and there is only a relatively small group of people who are loosely organized to address the problem. That clearly is not enough. One of the top ten recommendations set forth in the 60-Day Cyberspace Policy Review was to operationalize a public-private partnership to create an incident response plan that would incorporate a broad range of talent and experience to address these problems of lack of strategic warning and response. The planning is underway--and the government has begun to develop a wiki so that all can participate. Although long overdue, these efforts may lead to development of a collective strategy that can be used to address our opponents' tactics.

Board Two: Private Sector Networks

Our opponents are targeting our multinational and private corporations on at least three fronts: (1) through industrial espionage, they target corporate intellectual property and other proprietary data; (2) they attack other targets as mechanisms to reach yet other targets, sometimes through supply chains and sometimes to target relationships;[8] and (3) they target corporate infrastructure, by infecting networks or otherwise creating a persistent presence, as a means to allow for future targeting on either or both of the first two fronts.

More than 150 firms have been targeted for their corporate intellectual property and other proprietary data. This should be an alarming number, but what may be even more alarming is that, because the targeting is so sophisticated, the true number of targets simply is not known. Our opponents are seeking weapons designs, next generation telecommunications designs, and even proposals that may be used in the next international bid strategy to understand price points or win theme/strategy.

Like the example for DoD, some of this targeting comes via thumb drives (to allow an insider break-in). Other targeting is occurring through poor network security postures or procedures--and simple lack of understanding of the different/layered techniques that are being used to get to us. Perimeter defenses are not enough. For example, according to Symantec's April 2009 Internet security threat report, malware infections rose over 200 percent during 2008 in Europe, Middle East and Africa, and during that period there was a 47 percent surge in botnet activity.[9] Symantec further reported on risks from smartphones, which can be used to access backend

[8] In this regard, many corporations have been targeted due to their relationship with the Department of Defense, the Intelligence Community, or with other firms that have relationships with those organizations.

[9] Symantec Global Internet Security Threat Report Trends for 2008. Volume XIV, Published April 2009

systems where corporate proprietary data is increasingly being stored. Considering the number of botnets right now – the upstream targeting coming over the core Internet or ISPs – can provide an early warning. The ISPs know who is infected; who has a botnet on their computer, being a relay point to target another entity, or is being targeted for exploitation or disruption. But right now, because of privacy concerns, as well as liability issues, the information is not disclosed.

To further refine the point, many multinational corporations take precautions in the design, development, and manufacturing stages of their supply chains. But what about the managed service updates and upgrades? What about the retirement of the technology? One corporation found its corporate proprietary data had been stolen after its asset-disposal vendor took possession of the units. Despite the fact that they have a detailed asset-disposal procedure in place, what most would claim are sophisticated safeguards, it is becoming clearer that no company can inoculate itself completely against the targeting that is underway.[10]

The unvarnished truth is that no sector is without compromise. We are attempting to build trusted networks out of untrusted components, within untrusted environments, using untrusted supply chains, and untrusted vendors, all of which ultimately comes to rest in the hands of employees, some of whom cannot be trusted to observe well-established security rules.

How is this relevant to Wei-Ch'i? Corporate America is being targeted and its brand integrity is increasingly at stake. We could say that a “brand” is trust with the customer, trust with the marketplace, or even “trust monetized.” We work constantly to protect the integrity of this trust

[10] “Under Cyberthreat: Defense Contractors,” Business Week Special Report, 6 July 2009. http://www.businessweek.com/technology/content/jul2009/tc2009076_873512.htm?chan=technology_technology+index+page_top+stories

relationship, which is perhaps a company's most valuable asset. But that trust is being compromised through the targeting techniques described above.[11] As more of our networks are compromised, or intellectual property is stolen, corporate America will continue to lose market advantage and begin to be displaced. A government cannot develop a strategy independent of private sector insight and cooperation. Rather, the government will depend on the private sector and its capabilities to identify the next zero day exploit and create the patch for all of our systems.

The 60 Day Cyberspace Policy Review highlighted the need to communicate and share information as a "top 10" priority. First with a communication strategy, beginning with a national dialogue on cybersecurity -- what is happening to America and what it means to our family, friends, businesses, and future. Second, the review addressed the need for greater information sharing from the government to the private sector on what is being targeted, how, and why it is important to protect yourself (personally, professionally, corporately, nationally). The partnership on the research and development agenda is critical to move our collective security posture from red to black. Third, the review reiterated the need to revisit the National Intelligence Priority Frameworks (NIPF), the methodology that prioritizes our collection posture. The government's highest collection priorities are deemed "Band-A" topics and countries and therefore receive the most resources (funding, technology, people). We must consider looking at the countries that are emerging as Information Communications Technology (ICT) leaders and rank them as equal to those other Band A countries. And while threats to our critical infrastructure may be considered a Band-A topic, our government views these threats in a

[11] Stephen M. R. Covey. Speed of Trust: The One Thing that Changes Everything. Free Press, New York, NY: 2006. Page 263.

traditional country versus country lens, not from an emerging market or business intelligence context. Why should the United States change its approach? By viewing the countries that are creating relationships with ICT leaders or who are emerging as ICT leaders in the markets, we may see early targeting of corporate America. It may also be where we observe early market behavior for displacement technologies and new partnerships that may affect our supply chains.

Finally, the United States may need to retool its approach to the various international venues and negotiations. There are at least twenty international venues that are deciding the future of the information communications infrastructure. Whether it is the technical standards of that infrastructure, and whether it is corporations or the government representing the national interests (or the two going abroad together because there are different forums), we need to determine what we collectively need and want to then be able to find ways to amplify the common/shared goals. Additionally, the United States will need to find new ways to share information and boldly. In this regard, we may need to retool our intelligence and diplomatic communities -- as we did for arms control negotiations--to collect the information on positions, stances, alliances, necessary to meet our objectives.

Board Three: Personal Computers

Heartland Payment Systems disclosed in January 2009 that intruders hacked into the computers it uses to process 100 million payment card transactions per month for 175,000 merchants. [12] Robert Baldwin, Heartland's president and CFO, said that the intruders had access to Heartland's system for "longer than weeks" in late 2008. It discovered the hack after Visa and MasterCard

[12] Byron Acohido. "Hackers breach Heartland Payment credit card system**,"** USA TODAY.
http://www.usatoday.com/money/perfi/credit/2009-01-20-heartland-credit-card-security-breach_N.htm

notified it of suspicious transactions stemming from accounts linked to Heartland's systems. Investigators then found the data-stealing program planted by the thieves. Heartland is just one of many payment clearinghouses that is being targeted for personal credit-card data.[13] When was the last time you looked at your credit card bill and noticed an extra penny to a transaction? How about a quarter or dollar? It can be a very lucrative business for organized criminals and presents a sophisticated, albeit illicit; process to raise money for other purposes (e.g., buying weapons, further pursuing industrial espionage, or funding counterfeit operations).

More recently, there was an attack on United Kingdom based web hosting provider Vaserv that destroyed data on about 100,000 websites. [14] The attackers appear to have exploited a zero-day vulnerability in a virtualization application called HyberVM. The flaw allowed the intruders to gain root access to the system, allowing them to "execute sensitive Unix commands to force a recursive delete of all files. Half of Vaserv's customers had contracted for service that did not include data back-up."[15] For the ever growing number of users of Internet based email accounts, who host their data in a cloud somewhere, attacks like this pose major risks. For those who have not backed up their personal data or contracted for that service, the risk is even higher.

How is this relevant to Wei-Ch'i? Individually, we are all participating on the board. Our home computers are operating as part of botnet armies that are targeting our own credit cards and our governments. Unknowingly, in many ways we are facilitating the loss of America's economic

[13] At least three individuals responsible for the attack on Heartland and others were indicted by a federal grand jury in August 2009. *See* http://www.usdoj.gov/opa/pr/2009/August/09-crm-810.html.

[14] Dan Goodin. The Register. "Webhost hack wipes out data for 100,000 sites." 8 June 2009. http://www.theregister.co.uk/2009/06/08/webhost_attack/

[15] *Id.*

and security posture. Ultimately, this strategy has the potential to undermine our confidence in the information systems that underlie our economic and national security interests.

The 60-Day Cyberspace Review discussed the importance of building capacity as a digital nation and the immediate need for a national dialogue. This dialogue began with the May 29, 2009 publication of the review and President Obama's detailed speech on cybersecurity. Many people who heard that speech were surprised to hear the President use terms like botnet, phishing, pharming, spyware, and malware. But he is a 21st Century President who has children that are young like mine, and who use technology daily. He uses the technology and many of his transformational initiatives are dependent upon securing the global infrastructure that is driving the global economy.

Although many of us have become quite comfortable with technology and our dependence on digital infrastructure, at bottom we are all digital infants with much to learn. So how do we increase our digital maturity going forward to understand how to move forward as a nation and as a workforce? How do we stay safe online? What is our responsibility as a digital citizen operating in a digital age on the digital infrastructure? In his recent book, *Showing Up for Life*, Bill Gates, Sr. states, "The solutions to the problems confronting education in America require fundamental changes and drastic action. Getting it right will not be easy or comfortable. And getting it done will take broad engagement and support --from me and from you." He further goes on to say, that this change will require every person’s individual, deliberate acts of citizenship. Whether we join a club, read the newspaper, sign a petition, write a letter or vote. "If those clubs and newspapers and petitions and letters and votes and contributions and arguments predominantly point in the same direction, that's public will. Public will is manifest when the right thing to do becomes consensus and people generally start expressing the convictions they share in everything they do."[16]

We need to get the public to understand what is at stake--and why we must increase our digital maturity, and hence security, at a rapid pace.

Board Four: Electric Grid

Peggy Noonan recently wrote a book intended to inform the election, titled Patriotic Grace. At the end of the book she points out that everything in America runs on electricity:

> Communications--the phone, the TV, the radio, the Internet. The lights, the heat, the ATM, the bank, the pump, the refrigerator. The machines in the operating room, the lights on the runway. As I type I listen to music that is plugged in, on a machine that is plugged in, under lights that are plugged in. I received word from people I care about through two machines that are, at the moment, plugged in and being recharged. If something bad happens we will get information, instructions, inspiration, and help from things that are plugged in. And we will be largely without information, instruction, data, assistance and inspiration if the grid goes down.[17]

I can certainly relate to this, as I recently managed three blackberries and a pager, not to mention the multiple computers that I used to prepare this paper.

[16] Bill Gates Sr. Showing Up for Life: Thoughts on the Gifts of a Lifetime Broadway Books, New York, NY: 2009.
[17] Peggy Noonan. Patriotic Grace: What It Is and Why We Need It. Hapers Collins Publishers, New York, NY: 2008. Page 184.

One of my colleagues has reported and speaks publicly about the cyber attacks that have been used to disrupt power and equipment in several regions outside the United States.[18] In at least one case, it disrupted power and created outages that affected multiple cities for multiple days. We do not know who executed those attacks, but we do know that the intrusions are enabled through the Internet and can bring down the infrastructure. These are some of the things that may be keeping the President up at night; they certainly kept me and the 60-Day Cyberspace Policy Review team up at night.

How is this relevant to Wei-Ch'i? During the last decade and a half the United States has been seduced by phenomenal business and economic growth enabled by the effectiveness and efficiency of high performance global networked environments. The United States has been one of the key global leaders on embedding technology into our day to day life, transforming the global economy and connecting people in ways never imagined. However, we have not invested in the resilience necessary to ensure that our businesses can operate in a degraded environment. Our reliance on the conveniences of remote access and the ability of our networked control systems to reduce costs and manpower needs have led to weaknesses that are being exploited by our opponents on multiple boards. The United States and our allies have become asymmetrically vulnerable because we have more to lose than our adversaries. Our vulnerabilities have increased year after year, while at the same time becoming less transparent to systems owners and systems users. Finally, our technological defenses have not kept pace with the threat, and it remains easier today -- and I suspect for some time to come -- for our adversaries to create an offense than for us to create a defense. If we lose power for a day, a

[18] Thomas Donahue. SANS SCADA Security Conference, New Orleans, LA. January 2008.

week, or longer it will be a digital disaster that we are unprepared to address. In the game of Wei-Ch'i we lose; it is the end game or the Achilles heel.

The 60-Day Cyberspace Policy Review addressed the importance of innovation and the process by which governments, industry and citizens must work together toward building the next generation’s infrastructure standards that we need to have collectively – whether it is for the communications and information infrastructure or the next-generation energy grid or the next-generation FAA systems, all of which run on the same digital infrastructure that carries our data. We need to cultivate a public-private partnership and action plan that identifies the requirements for that future architecture, hardware, software, services. We need to work together to address the linkages to national essential functions and how we hold each other accountable toward our shared vision. We also need to develop the processes and procedures to measure government and industry progress and build in the agility along the way to change our course when we are off the path.

There is an annex to the 60-Day Cyberspace Policy Review that discusses the last 150 years of the growth of modern communications technology infrastructure.   It describes how we got to where we are today, from the telegraph to the telephone, to satellite communications, to today's wireless communications and Internet communications. It articulates how the development of a new technology led to new vested authority within a department and agency which then leads to concerns from civil liberties and privacy perspectives, and then perpetuates another new law. The cycle has continued as each new technology has developed, and the annex highlights the patchwork of laws and authorities that have developed over time as a result. Understanding this history is very educational and can help inform the debate. Why do I raise this, and how does it relate to the electric grid? Today, there are at least eleven pieces of legislation pending in Congress that, if not coordinated properly, will further complicate what is already a very complex and murky situation.

* * * *

We are losing territory every day in this digital game of Wei-Ch'i. Stones are being placed everywhere--on all of the boards. We must develop the situational awareness and find a way to share information so we can mount a successful defense. We need multiple players maneuvering on multiple boards. Together, we must make multiple, independent actions that get us to our goal. We need a shared vision with a trust that we are all in this together because there is a lot at stake. To move us toward our collective vision, we must mobilize everyone to defend what we hold dear to ourselves, to each other, and for future generations. We need to strive for a common result for the common good--a safe, secure, and resilient infrastructure that can continue to support our daily lives, our national security, and the global economy. We need to get America out of the red, both literally and figuratively. We have been invaded and our corporate bottom lines and competitive future are at stake.

Recognizing the challenges and opportunities, President Obama identified cybersecurity as one of the top priorities for his Administration and I had the privilege to lead the 60-Day Cyberspace Policy Review for him. It addressed all missions and activities associated with the digital infrastructure. It included the missions of computer network defense, law enforcement investigations, military and intelligence activities, and the intersection thereof with information assurance, counter intelligence, counter terrorism, telecommunications policies, and general critical infrastructure protection. The President adopted the vision, blueprint and all of the recommendations in total and directed that work begin immediately to address these issues.

It is our collective responsibility to get America back in the black by moving together toward the vision of making us strong again. It is not enough for just one person to lead. As we develop a counterstrategy in this game of Wei-Ch'i, we must recognize that we are all players and although we are all placing stones (making moves) independently, together we can achieve the strategic objective of protecting our digital infrastructure as a strategic national asset. This requires that we abandon institutional prerogatives to get to the common good of our country. We need to marshal all of our resources to protect this infrastructure as a national security priority. This requires all of us ensure that these networks are secure, trustworthy and resilient. It further requires all of us to work together and trust each other to deter, prevent, detect and defend against attacks and recover quickly from any disruptions or damage.

We need to work together to ensure our highest performance, by placing our stones close together and sharing information to help support each other and avoid capture. We also need to be placing stones far apart, using our reach as global companies and a strong nation to create influence across more of the boards. We need to harness America's ingenuity and innovation and downright determination to win. We cannot afford to have parochialism interfere with what must be done.   We must act together, or we will fail.

There is a verse in the Book of Psalms that says "your word is a lamp to my feet and a light to my path." The promise in that verse is that we are given enough information, knowledge, or wisdom to take the next step. While it may make us more comfortable to have a set of high beam halogen headlights that illuminate the next two miles of the road, all we have is a lamp that lights the next few steps of our path. Remember that the terrain is complex and all encompassing. Advancing into unchartered territory is about taking one step at a time. Our strategy must harness our collective vision and be tempered by patience and endurance. Because navigating the jurisdictional purview of individual departments and agencies, the laws that may inhibit our ability to share information and communicating the urgency of the situation while at the same time keeping our eyes on the horizon in addition to our bottom line will not be easy. To be competitive requires that we amplify our common interests and place our stones with serious people. None of us can see everything that is ahead of us down the road. What we do have is the opportunity to operate from how we are when we are at our best and to draw on those characteristics to create the outcomes that matter most. That is what moving to the next level, no matter what the terrain may be, is all about.

Why use Wei-Ch'i as an example? Unlike chess, no computer program has yet been written which has been able to compete with the best of players.[19] Whether it is a lighthouse on the shore, a lamp along the path, a candle in the night, or a flashlight in our hands, we must all be working together to light and walk this path.

[19] Scot Eblin. The Next Level: What Insiders Know About Executive Success. Page 193

MELISSA E. HATHAWAY
melissa_hathaway@verizon.net

August 2009 - Present: President, Hathaway Global Strategies, LLC
Ms. Hathaway brings a multi-disciplinary and multi-institutional perspective to strategic consulting and strategy formulation for public and private sector clients. She is raising public awareness by writing and speaking publicly about current real-world problems and is building information and research bridges among academic, industrial and government stakeholders.

February 2009 - August 2009: Acting Senior Director for Cyberspace, National Security Council
At the request of the Assistant to the President for National Security Affairs, Ms. Hathaway was asked to lead the 60-Day Cyberspace Policy Review for President Obama. She assembled a team of experienced government cyber experts, inventoried relevant presidential policy directives, executive orders, national strategies and studies from government advisory boards and private sector entities, identified over 250 needs, tasks, and recommendations and engaged in more than 40 meetings with industry, academia, the civil liberties and privacy communities, State governments, international partners, the Legislative Branch, and the Executive Branch. Her outreach resulted in receiving more than 100 papers that informed the recommendations. She produced a comprehensive report that contained multiple annexes and twenty-five near term and mid-term recommendations.

In May 2009, President Obama presented the elegant blueprint of the Cyberspace Policy Review and announced cybersecurity as one of his Administration's priorities. He recognized Ms. Hathaway's leadership and noted that there are, as the President said, "opportunities for everyone—academia, industry, and governments—to work together to build a trusted and resilient communications and information infrastructure."

Ms. Hathaway stood-up the Cybersecurity Office within the National Security Staff, convened the policy meetings that began work against each of the top ten recommendations contained in the Cyberspace Policy Review, and set the expectation and pace to move the United States toward a stronger more resilient information and communications infrastructure.

March 2007 - February 2009: Cyber Coordination Executive and Director, Joint Interagency Cyber Task Force, Office of the Director of National Intelligence

Ms Hathaway built a broad coalition from within the Executive Branch for two Presidents, developing a cybersecurity strategy covering unprecedented scope and scale that will now facilitate revolutionary improvements for the United States to secure and defend our critical national infrastructures.

She developed and created a unified cross-agency budget submission for FY 2008 and for 2009-13, assembling disparate funding sources into a coherent, integrated program. One of the single largest intelligence programs of the Bush administration, the Comprehensive National Cybersecurity Initiative has been carried forward by the Obama administration.

Her holistic, integrated vision of cyber issues that spans computer network defense, law enforcement investigations, military and intelligence activities, and the intersection thereof with information assurance, counter intelligence, counter terrorism, telecommunications policies, and general critical infrastructure protection was evaluated against the growing velocity and volume of threat vectors. These ranged from attacks coming over the Internet, to threats posed by insiders, to the deliberate manipulation and corruption of the supply chain. They involved almost any device used to import data or software into a system. Her vision is the centerpiece of President Obama's 60-Day Cyberspace Policy Review.

She established a partnership with Congress and obtained bipartisan support by presenting unified, objective cyber threat and U.S. government operational activities in Congressional briefings and Statements for the Record which earned respect from Committee leadership and the private sector. She garnered trust in Congress through her exhaustive interaction (more than 150 testimonies and briefings) with both members and staff during the course of the 110th and now 111th Congress.

June 1993 - February 2007: Principal, Booz Allen & Hamilton, Inc.

Ms. Hathaway's responsibilities focused on leading two primary business units: information operations and long range strategy and policy support. Her consulting efforts supported key offices within the Department of Defense and Intelligence Community, including United States Strategic Command, United States Pacific Command, the Office of the Under Secretary of Defense for Intelligence, the Office of the Secretary of Defense for Net Assessment, the Central Intelligence Agency, the Defense Intelligence Agency and the Office of the Director of National Intelligence. Her work included the design and development of novel techniques for mapping social, business process, and infrastructure relationships. She also led the design and development of a methodology for evaluating new force options across the electromagnetic spectrum. Some of the more significant long range strategy and policy studies on which Ms. Hathaway worked focused on biotechnology, power projection, Asia, and other national security issues.

June 1990 - June 1993: Associate, Evidence Based Research, Inc.
Ms. Hathaway performed research and developed databases to track economic and political issues in Eastern Europe and the former Soviet Union, developed a model to detect the routes and modes and to estimate the quantities of cocaine movement into the United States, and studied other key issues in support of the Intelligence Community.

September 1989 - May 1990: The American Foreign Service Association.
Ms. Hathaway coordinated international conferences for the business community held at the Department of State. Topics included investment opportunities in Eastern Europe, the European Community, and the GATT Uruguay Round.

Education
Ms. Hathaway has a B.A. degree from The American University in Washington, D.C. She has completed graduate studies in international economics and technology transfer policy, and is a graduate of the US Armed Forces Staff College, with a special certificate in Information Operations.

Publications
Cyber Security: An Economic and National Security Crisis. The Intelligencer: Journal of U.S. Intelligence Studies. Volume 16, Number 2, Fall 2008.

Safeguarding Our Cyber Borders. Miami Herald. 9 October 2008.

Information Operations Workshop Summary. Phalanx: Military Operations Research Journal. September 2002.

Tactical Decision Exercises - Preparing the Joint Task Force-Computer Network Operations for Mission Readiness, Information Assurance and Technical Analysis Center (IATAC) Newsletter. Summer 2001.