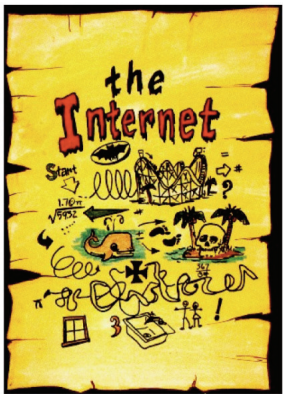
"In one year, five years, ten years, and twenty-five years, will we look back and see this as a time when normal market behavior and normal government actions failed to achieve our common goals? Or, will we see this as the period when goals were met through new ideas, expanded thinking, and the combined efforts of industry and government working as one?"

—MELISSA E. HATHAWAY

Falling Prey to Cybercrime:
Implications for Business and the Economy

Melissa E. Hathaway
President
Hathaway Global Strategies LLC

Espionage, "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company"[1] is pervasive in the United States. Foreign governments and criminal networks are stealing our ideas, counterfeiting our goods, and putting our future economic well-being at risk. The number of businesses falling victim to these crimes increases daily, and no sector is without compromise. Secretary of Commerce Gary Locke recently stated that, "every year, American companies in fields as diverse as energy, technology, entertainment and pharmaceuticals lose between $200-$250 billion to counterfeiting and piracy."[2] But it is not just about counterfeiting and piracy; companies and governments regularly face attempts by others to gain unauthorized access through the Internet to their data and information technology systems by, for example, masquerading as authorized users or through the surreptitious introduction of malicious software.



We did not arrive at this place overnight. The Internet, born with its first transmission on October 29, 1969, was never conceived as the backbone of global commerce. Rather, it evolved into this role through a series of events including: (1) the first virtual data communication with Europe in 1973; (2) the first cellular portable telephone in 1973; (3) the first automated commercial cellular network in 1979; (4) the advent of the personal computer in 1981; (5) the introduction of top-level-domains (for example., .mil, .com, .edu, .gov) in 1985; (6) the creation of hyper-text mark-up language (HTML) in 1990, which enabled expanded and user-friendly information sharing on the Internet—which ultimately became the World Wide Web; (7) the relaxation of export controls for encryption

products to foster global electronic commerce in 1996; (8) international adoption of the domain name system (DNS) to enable a framework for global electronic commerce; and (9) the widespread adoption of new technologies like voice over Internet protocol (1996), WiFi (1997), wikipedia (2001), the Google search engine (1997), social networking technology (2002), and voice and video over Internet with Skype (2003). The private sector is driving innovation and adoption of technology with the promise of lower costs, increased productivity, and consumer usability without much discussion of security. In contrast, and very much the reality we face, this same technology and attendant services are being exploited for crime and conflict.

In 1988, the release and propagation of the Morris Worm affected 10 percent of the Internet's computers and disrupted Internet services for days.[3] As one of the first major "infections" experienced by both governments and businesses, it inspired the information security commodity market. Digital Equipment Corporation developed the first packet filter firewall in 1988 and so began the evolution of security products to protect us from the insecurity of doing business on the Internet.

Over the course of the next twenty years, we experienced breaches to our banks (Citibank in 1984), theft of our passwords and credit card information (AOL in 1995), penetration of the Department of Defense unclassified networks (Solar Sunrise in 1998), theft of our personal identifiable information (Choice Point in 2005), illegal copying of defense industrial base critical program information (weapon system designs in 2007 and ongoing), penetration of the Department of Defense classified networks (Buckshot Yankee in 2008), and targeting of our children (Sony 2011). These and other cyberattacks on Internet commerce, vital business sectors, and government agencies have grown exponentially. Some estimates suggest that in the first quarter of 2011 security experts were seeing almost 67,000 new malware threats on the Internet every day. This means more than forty-five new viruses, worms, spyware, and other threats were being created every minute—more than double the number in January 2009. As these threats grow, security policy, technology, and procedures need to evolve even faster to stay ahead of the threats."[4] A recent Symantec report indicates that these trends will continue.[5] From 2010 to 2011 the differences are discouraging. In fact: There were 286 million unique variants of malware that exposed and potentially exfiltrated our personal, confidential, and proprietary data; each data breach exposed, on average, 260,000 identities; there was a 93 percent increase in web-based attacks (compromised/hijacked websites that would infect individuals' computers if visited); the underground economy paid anywhere from $.07 to $100 for our stolen credit card numbers; and realizing that mobile payments

and mobile platforms (like smart phones and the iPad) would be the newest vector of technology adoption, there was a 42 percent increase in mobile operating system vulnerabilities and subsequent exploitation.

As American businesses, inventors, and artists market, sell, and distribute their products worldwide via the Internet, the threat from criminals and criminal organizations who want to profit illegally from their hard work grows. The threat from other nations wanting to jump start their industries without making the intellectual investment is even more disturbing. This fleecing of America must stop. We can no longer afford complacency and silence—we must find and use as many market levers as possible to change the path we are on.

This chapter discusses three different approaches to addressing the problem. First, it is possible to apply tax incentives to businesses for innovation and consumers to patch the problem. While this may not be a fiscally responsible approach given the current debt crisis and constrained economic environment, it should nonetheless be considered. Second, Congress could consider reviewing the applicability of the National Defense Production Act to provide our IT industry a fighting chance against the predatory pricing and industrial espionage being practiced by other nations. Finally, this chapter will discuss four unique private-public partnerships that deserve attention as regional and potentially national agents of change.

Use Tax Incentives

It is estimated that the G-20 economies have lost 2.5 million jobs to counterfeiting and piracy, and that governments and consumers lose $125 billion annually, including losses in tax revenue.[6] The underground economy makes it easy for anyone to get started in cybercrime. The tools and services are readily available to take advantage of the average consumer and exploit the industry's latest product. So why can't we help our information security industry innovate as fast as the criminals? The research and experimentation credit under section 41 of the Internal Revenue Code provides a tax credit for incremental investment in research, which could be applied to address this innovation gap. There is a 20 percent credit for incremental research over a base period, or an alternative simplified credit of 14 percent for incremental research over the previous three years. Originally enacted in 1986, the research credit is a temporary provision that must be extended regularly. In its FY2012 budget proposal, the Obama administration proposed to make the research credit permanent, and to increase the credit percentage on the alternative simplified credit to 17 percent.[7]

The research credit is not specific to any particular type of research or industry, but is available for any research that is technological in nature. So, just as the Digital Equipment Corporation introduced some of the first technology (the firewall) to address exploitation of our systems, our industry could apply its research toward monetizing products that begin to close the gap between criminal exploitation and successful protection. The innovation agenda could also be applied to data correlation, detection of network and system anomalies, and identification and evidence gathering of criminal "fingerprints."

Because the research credit is focused on basic research, it serves as an incentive for companies to develop new ideas that can be deployed in their business. However, the credit does not extend to purchases of products or technologies that are used in a business. If an incentive is needed to encourage companies to acquire tools that can be used to enhance their cybersecurity, the research credit will not suffice. Rather, Congress could consider tax incentives to encourage taxpayers to acquire and deploy new security tools by providing an investment credit to encourage such investments. For example, since 1992, Congress has provided incentives for taxpayers to invest in renewable energy through the energy investment credit under section 48 of the Internal Revenue Code and through the renewable energy production credit under section 45. These incentives have helped to encourage taxpayers to deploy resources to develop wind, solar, geothermal, and other types of renewable energy. Similar programs could be implemented to assist in the development of new tools to protect the security of our information and communications infrastructure.

While tax credits can help incentivize taxpayers to focus investment on favored items, a tax credit is only useful to a taxpayer with positive taxable income who can use the credit to shelter the tax burden on that income. For companies in depressed markets, with net operating losses, a tax credit has no value and will not provide any incentive for new investment. In recognition of this problem, in 2009 Congress provided a temporary program for grants in lieu of the low-income housing and energy credits.[8] A similar type of temporary grant program might be appropriate to kick start intensive investment in technology to improve cybersecurity.

Whether a credit or a grant program is established, key drafting considerations would need to ensure that the benefits are provided only for new investment in the type of technology that Congress wants to incentivize, that the investment is made in the United States, and that research and manufacturing relating to the favored products is conducted in the United States. In addition, to ensure that the benefits are used solely for innovation, the provisions should be drafted to ensure that only the

taxpayers who invest in and deploy the technology can receive the benefits provided. This would stand in contrast to the low-income housing and energy credit programs that have been developed over the years to permit financial investors to take advantage of their benefits.

Offering a similar incentive to the average consumer may also go a long way toward improving the nation's security posture. Because consumers may not keep pace with the latest technology improvements or band-aids in security, Congress also should consider providing targeted incentives for consumers to invest in securing their personal computers and home networks. Again, the energy sector provides a useful precedent: Section 25C of the Internal Revenue Code provides a credit of up to $500 per year for individual investments in residential energy efficiency improvements. This credit has encouraged investments in energy-efficient appliances, HVAC systems, and windows and doors. Separately, section 25D provides a 30 percent investment credit for investments in residential solar, wind, and geothermal systems. And over the past decade the hybrid vehicle industry has flourished in the United States, in large part due to the tax credits provided to incentivize these purchases. In the case of cyber investments in the home, the average dollar cost per household is relatively small, so tax credits may not impact the economic decision as much as in the case of the energy examples described above. Nevertheless, a credit of even $25 per taxpayer who purchases new security software each year could help further proliferate these important safeguards.

Leverage the Authorities in the National Defense Production Act (NDPA)

In addition to using taxes as a market incentive, Congress should also consider applying the NDPA to counter the broad based espionage being conducted against our defense industrial base coupled with the predatory pricing and acquisition strategies of our core telecommunications technologies by foreign corporations. Foreign companies are gaining an ever-increasing share of the U.S. commercial technology market, while at the same time our national security networks, critical infrastructure, and weapons systems are growing more reliant on products and services from that market. This is further complicated by the fact that China is our largest supplier of telecommunications imports (42 percent) and is our eighth largest export market for U.S.-based telecommunications technologies. The NDPA could be applied in the absence of industrial policy or market levers that can shore-up the competitive position of U.S.-based information and communications technology (ICT) companies.

In response to the start of the Korean War, the NDPA was enacted in 1950 as part of a broad civil defense and war mobilization effort in the context of the Cold War. The act contained seven sections, of which three major sections remain active today. The first (Title I: Priorities and Allocations) authorizes the president to require businesses to sign contracts or fulfill orders deemed necessary for national defense. The second (Title III: Expansion of Productive Capacity and Supply) authorizes the president to establish mechanisms (such as regulations, orders, and agencies), to develop, modernize, and expand defense productive capacity. The third area (Title VII: General Provisions) provides antitrust protection for voluntary industry agreements serving defense interests, and established a voluntary reserve of trained private sector executives available for emergency federal employment.[9] Beginning in the 1980s, the Department of Defense (DoD) began using the contracting and spending provisions of the NDPA to provide seed money to develop new technologies. Using the NDPA, DoD assisted in the development of a number of new technologies and materials, including silicon carbide ceramics, indium phosphide and gallium arsenide semiconductors, microwave power tubes, radiation-hardened microelectronics, superconducting wire, and metal composites.

In the late 1980s and early 1990s, U.S. industry faced fierce competition in the area of micro-electronics, specifically with semiconductors from Japan. The U.S. government co-invested with industry to establish Sematech to upgrade the production environment and improve quality and yield of product to market. New technologies create new opportunities and one could argue these investments led to many of the micro-electronics that are part of the American household today, including cell phones, netbooks, and iPads, among others.

The information technology industry is critical to the economic and national security of the nation, much as the aerospace industry was crucial to our security posture during the 1960s. The pace of innovation and marketplace dynamics are threatening U.S. leadership in communications, computing, networking, and security technologies, and it may be time to provide government assistance to enhance the competitiveness and preserve the leadership of this critical sector. For example, Congress could leverage the special authorities contained in the NDPA to help subsidize and accelerate DoD access to commercial production technologies and capacity. 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. The NDPA also authorizes the establishment of the National Defense Executive Reserve (NDER) (what some would call the Civilian Cyber Reserve Corps), a cadre of persons with recognized expertise who could step into executive positions in the Federal government in the event of an emergency. One could argue that the Department of Defense information technology exchange program (ITEP) initiative could be the long-term pipeline for this NDER. The government should recognize that our national telecommunications infrastructure is vital to U.S. interests and consider better protecting it. Any discussion of government protection of the industry 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."[10]

It is desirable to use Title III authorities to upgrade suppliers' production capabilities to improve quality and yield on new technologies that would enhance the security of our critical infrastructures, networks, and mobile devices while at the same time making our IT corporations more competitive. Example areas for technology investments include: systems architectures that permit the secure use of commercial-off-the-shelf (COTS) computers, software, and networks; mechanisms, including intelligent agents, for locating and retrieving information from complex database structures; automated systems for reverse engineering based on scanning of an actual part; design of interruption-free connector systems for ultra-high-speed data rates; high performance computing (HPC) and advanced visualization of petabyte data sets; advanced visualization; and environments to perform at scale network simulations and rapid prototype testing.[11]

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

Accelerate and Seed Private-Private and Private-Public Initiatives

Finally, as discussed above, the proposed tax incentives coupled with the NDPA could enhance emerging private sector initiated partnerships and innovation to close the security gap. These grassroots efforts are being initiated by businesses who can no longer tolerate being victimized by criminals and foreign governments alike. Each program aspires to reduce the overall incidence and harm caused by cyber incidents and each program is improving collaboration and operational information-sharing while simultaneously protecting sensitive data and ensuring the security of the broader community. Four initiatives—the Cyber Accelerator, the Network Security Innovation Center, the Advanced Cybersecurity Center, and the National Economic Security Grid—are discussed in detail below.

The Cyber Accelerator is a structured consortium that uses DoD's transaction authority to invert the acquisition model from pull- to push-sourcing and repurposes private sector innovation to meet DoD's needs. The government enters into a technology investment agreement (TIA) with the non-profit consortium lead to assist in research and development of commercial technologies to apply to DoD use cases and defense technology allowing tech transfer of intellectual property to commercial entities. The goal of the effort is to expand integration of innovative technologies within the commercial marketplace (for example Google, Intel, McAfee, and VMware) to add value beyond the large-scale system (weapon system) integrators (Lockheed Martin, General Dynamics, and Northrop Grumman). The Cyber Accelerator seeks to lower the private sector barrier to working with the DoD while simultaneously providing the DoD with shorter product cycles, lower life cycle costs, and privileged access to commercial innovation.

Two benefits converge to open up a new set of vendors and new innovation for the government. First, identifying and funding the development of "dual-use" capabilities attracts private sector investment and at the same time addresses an operational and technical shortfall in DoD. Second, it attracts companies that are reticent to deal with DoD by protecting their intellectual property and seeding capability development that leads to both company and investor profits and DoD operational needs.

The work of the consortium follows an agreed upon multi-year technology roadmap with an annual funding plan that complies with authorities and appropriations. Some technology initiatives that this effort will explore include: (1) enhanced authentication (endpoint, application, and data); (2) identity and behavior recognition (correlating user behavior across multiple personas, devices, and

accounts); (3) trusted data provenance (tied to identity for source, application, and user roles); and (4) automated learning for remediation and response.

Lessons learned from these dual-use product initiatives will provide the government with insight for future acquisition reform and potential innovative models. It also provides a mechanism to use market incentives for rapid innovation and deployment.

The Network Security Innovation Center (NSIC) is an industry driven initiative based out of Silicon Valley to create a government, academic, and industry partnership to foster innovation and information-sharing in cybersecurity. The NSIC brings together the talent of the largest IT companies and entrepreneurs of the Bay Area with the computational capacity and unique capabilities of the FFRDC (Federally Funded Research and Development Center) status of Lawrence Livermore National Lab (LLNL). This initiative is striving for "extreme security innovation," says Jacques Francoeur, executive director of the Bay Area CSO Council, who played an instrumental role in bringing industry stakeholders to the table, using intellectual power, computational power, and most importantly industry power.[12] In a recent speech at the center, Gary Terrell, Adobe's chief information security officer, described the top strategic initiatives businesses must launch to meet the growing threats of worldwide cybercrime, stating that, "security leadership needs to fundamentally change its perspective and, in many cases, make a 180-degree turn to protect their digital assets, and the time is now." [13]

The NSIC has two "anchor" IT firms initiating focused collaborative R&D projects. These projects are indicative of what the center could offer, as an incubator and a direct path for moving R&D results to sustainable innovative products. For example, McAfee, which has an Internet threat sensor network collecting data in 120 countries, and LLNL are jointly working on probability models for dynamics on graphs. They are trying to run analytics to winnow out critical threats from this massive data set (of 100 billion queries per month), to see if they can find interesting patterns with significantly greater computing capacity. By partnering with LLNL, McAfee gains access to the lab's supercomputing and highly specialized scientific resources, allowing it to handle large data analysis requirements and potentially enabling McAfee to develop new technologies to counter advanced threat techniques, profile hackers, and insider threats. Cisco is also partnering with LLNL on a focused project regarding network simulation and virtualization. The goal of this project is to simulate large-scale exploits without disrupting operational networks in order to discover the second-order effects of exploits with the aim of developing techniques for early detection. By having a large-scale network simulator that has access to large

volumes of real world data (provided by the Cisco IOS platform that is currently operating on millions of active systems, ranging from the small home office router to the core systems of the world's largest service provider networks), it may be possible to create an environment and technology that can lead to attacker attribution. The simulation creates flexible honeypots and "hacker treadmills" to keep adversaries engaged while allowing the time and interactions required to gain attribution.

The NSIC is working to become fully operational in the next six months. It is currently in the process of defining a governance framework and intellectual property rights model that meets the needs of all parties. The NSIC shows great promise as an innovation engine that addresses some of our toughest cybersecurity problems, especially around big-data and malicious behavior analysis.

The Advanced Cybersecurity Center (ACSC) was created to establish Massachusetts—and the New England region more broadly—as a leader in the development of next generation cybersecurity R&D and education programs. This industry-driven initiative brings together university and government entities to address advanced cyber threats by sharing insights on attacks and mitigation strategies and cultivating the next generation of talent for employment in the region. The ACSC supports a collaborative, cross-sector research environment (and facility) using the region's unparalleled university, research, and industrial resources to focus on areas not addressed by commercial security solutions and thereby strengthen members' defensive capabilities. The ACSC has formed working groups to drive the Center's collaborations across a range of initiatives including: (1) threat evaluation and data sharing, (2) university-industry partnerships, and (3) policy and legal challenges. Specific technology projects seek to enable trusted collaborations in the pre-competitive space and foster innovations and improvements in predictive analytics, incident monitoring and analysis, intrusion detection and eradication, and deployment, incident scenarios and response strategies.

As the ACSC becomes operational it intends to establish federal and national partnerships to extend the region's influence and enhance coordination with key resources, becoming a vital component in protecting the region's and nation's key assets.

Finally, the National Economic Security Grid (NESG)[14] is a grassroots-based independent non-profit organization established in 2010 as a resource for metropolitan area public and private sector entities. The NESG is committed to dedicating resources and capability to local small and medium enterprises (SMEs) in each of

the metropolitan areas across the country and providing them with information, processes, proven practices, and solutions to the risk, threats, and hazards they face every day. The goal is to establish NESG operations in every metropolitan area in every state across the country to truly create a "National Economic Security Grid."

NESG selected metropolitan Los Angeles as its inaugural site after LA County Sheriff Leroy Baca expressed a strong desire to launch this grassroots initiative as a means of strengthening the local partnership between the public and private sectors, with a focus on safeguarding the economic security of the city. As such, the NESG will collect "intelligence" data on a broad range of external and internal risks, threats, and hazards that may affect the local SME community and will turn this data into tailored actionable information for delivery to online secure escrow accounts accessible by SME members. It also plans to establish a Risk Solution Center that provides tested and vetted risk mitigation solutions to SMEs.

While not yet fully operational, the NESG intends to make a difference by: (1) establishing strong local partnerships between SMEs, local law enforcement, prosecutors, politicians, and other community-based support groups to focus on the stability, viability, and resiliency of the local community and its economic environment; (2) providing actionable information to SMEs on the real world risks and threats they face every day; and (3) identifying sound and affordable risk mitigation solutions to ensure high survivability of SMEs, which ultimately improves the economic conditions of the community.

Conclusion

Notwithstanding all of the efforts made to date by many well-intended professionals and organizations, and despite significant advances in technology, we are still struggling to stay on top of the cybersecurity problem. Indeed, the problem is growing faster than the solution and we cannot afford to be faced with strategic surprise as we falter in addressing it. The national economic security agenda for the United States needs disruptive ideas that reinvigorate our innovation engine, our intellectual creativity, and our law enforcement capability and capacity.

We need to expand our options, and to do so quickly. In one year, five years, ten years, and twenty-five years, will we look back and see this as a time when normal market behavior and normal government actions failed to achieve our common goals? Or, will we see this as the period when goals were met through new ideas, expanded thinking, and the combined efforts of industry and government working as one?

We cannot continue along the current path and expect to make adequate progress to confront the cybersecurity dilemma. Our country has at its disposal market levers, unique authorities, advanced technology, public-private partnerships, and a culture of innovation and creativity. The full gambit of market levers—especially incentives-based levers—is needed to advance research and development, drive innovation, and close the gap between adversary successes and industry defenses. We need a more secure resilient infrastructure. Can we find the wherewithal to stop the fleecing of America?

Melissa Hathaway is President of Hathaway Global Strategies LLC and a Senior Advisor at Harvard Kennedy School's Belfer Center. Ms. Hathaway served in the Obama administration as Acting Senior Director for Cyberspace at the National Security Council and led the Cyberspace Policy Review. During the last two years of the administration of George W. Bush, Ms. Hathaway served as Cyber Coordination Executive and Director of the Joint Interagency Cyber Task Force in the Office of the Director of National Intelligence where she led the development of the Comprehensive National Cybersecurity Initiative (CNCI). At the conclusion of her government service she received the National Intelligence Reform Medal in recognition of her achievements. Previously, Ms. Hathaway was a Principal with Booz Allen & Hamilton, Inc., where she led two primary business units: information operations and long range strategy and policy support, supporting key offices within the Department of Defense and intelligence community. Earlier in her career she worked with Evidence Based Research, Inc. and the American Foreign Service Association. Ms. Hathaway is a frequent keynote speaker on cybersecurity matters, and regularly publishes papers and commentary in this field.

[1] *Merriam-Webster's Dictionary*, 11th ed..

[2] Secretary of Commerce Gary Locke (Remarks at the Washington International Trade Association, Washington, D.C., July 22, 2009).

[3] Eugene H. Spafford, "The Internet Worm Program: An Analysis," *Purdue Technical Report* CSD-TR-823 (West Lafayette, IN: Purdue University, 1988).

[4] United States Department of Commerce, Internet Policy Task Force, Cybersecurity Green Paper (Washington, D.C.: Government Printing Office, June 2011), ii.

[5] Symantec Internet Security Threat Report, *Trends for 2010*, (April 2011).

[6] Frontier Economics, *Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy* (February 2011).

[7] Joint Committee on Taxation, *Description of Revenue Provisions Contained in the President's Fiscal Year 2012 Budget Proposal (JCS-3-2011)* (June 2011).

[8] Sections 1602 and 1603 of the American Recovery and Reinvestment Act of 2009.

[9] Congressional Research Service, *Defense Production Act: Purpose and Scope* (May 14, 2009).

[10] 18 U.S.C. § 2510(1) (2006) and Nicholas Matlach, "Who Let the Katz Out? How the ECPA and the SCA Fail to Apply to Modern Digital Communications and How Returning to the Principles in Katz v. United States Will Fix It, 449 *Commlaw Conspectus*, Vol. 18 No. 2 (2010), 443.

[11] National Research Council, *Defense Manufacturing in 2010 and Beyond: Meeting the Changing Needs of National Defense* (Washington, D.C.: National Academies Press, 1999), 45.

[12] Author interview with Jacques Francoeur, July 28, 2011.

[13] Quoted in Brian D. Johnson, "Network security innovation center kicks off lecture series," on the Lawrence Livermore National Lab website, July 18, 2011.

[14] Information presented here is derived from discussions with the founder, Lynn Mattice.