

**“Beyond Private-Public:
Making America’s Universities Full-Fledged Cyber-Security Partners”**

Written Testimony

prepared for a hearing of the

Subcommittee on Oversight, Investigations and Management
Committee on Homeland Security
U.S. House of Representatives

on

“America is Under Cyber Attack: Why Urgent Action is Needed”

by

Stephen E. Flynn, Ph.D.

Founding Co-Director

George J. Kostas Research Institute for Homeland Security &

Professor of Political Science

Northeastern University

s.flynn@neu.edu

Cannon House Office Building - Room 311
Washington, DC

2:00 p.m.
April 24, 2012

**“Beyond Private-Public:
Making America’s Universities Full-Fledged Cyber-Security Partners**
by
Stephen E. Flynn, Ph.D
Professor & Founding Co-Director, Kostas Research Institute
Northeastern University

Chairman McCaul, Ranking Member Keating, distinguished members of the Subcommittee, thank you for the opportunity to testify about the serious and growing cyber security threat facing consumers, industry and government at all levels in the United States. The significant vulnerability of critical infrastructure such as the electric grid and transportation infrastructure, information and financial systems, and everyday American consumers to cyber threats is why today’s hearing is so timely and why urgent action by Congress is so needed.

My name is Stephen Flynn. I am the founding Co-Director of the Kostas Research Institute for Homeland Security and professor of Political Science at Northeastern University in Boston, Massachusetts. I am also a member of the Homeland Security Project at the Bipartisan Policy Center that is led by 9/11 Commission co-chairs Governor Tom Kean and Congressman Lee Hamilton. The nation’s exposure to a growing array of cyber-security threats is one of deep concern to the co-chairs and all the members of our group of distinguished national security and homeland security leaders.

At the Kostas Institute, our mission is to help advance resilience in the face of 21st Century risks so that America can better withstand, nimbly respond, rapidly recover, and adapt to man-made and natural disruptions. As such, we are working with our Northeastern colleagues in the College of Computer & Information Science, College of Engineering, and College of Social Sciences and Humanities to make cyber security a primary area of focus. We are a particularly interested in better safeguarding industrial control systems that are key to the operation of much of the nation’s critical physical infrastructure.

The Kostas Institute is housed in a new 70,000 square foot research facility located in the heart of the metro-Boston high-technology corridor where it provides a secure environment for innovative translational research conducted by private-public-academic multidisciplinary research teams. Northeastern is also home to the Institute for Information Assurance, which is one of the National Security Agency’s (NSA) Centers of Excellence. In addition, the university is a member, along with MIT, Harvard, Boston University, and the University of Massachusetts, of the Advanced Cyber Security Center hosted at the MITRE Corporation in Bedford, Massachusetts. Given the historic leadership role that Northeastern, our neighboring universities, and the information technology industry that is concentrated in the metro-Boston area have played in high-tech development, we feel a special responsibility to help manage, stem and mitigate the growing risks to critical systems from cyber threats. To this end, we are committed to bringing together expert researchers and practitioners to identify risks and their potential consequences, to develop next-generation secure applications and computing architecture, and to promote best practices with our counterparts around the U.S. and globally.

Nature of the Cyber Security Threat

The cyber security threat is one of the most serious economic and national security challenges we face as a nation. Quite simply, the United States is at risk of becoming a victim of its own success. Our position as the world's dominant economic power can be attributed in no small part to the speed at which Americans have developed and embraced information technology systems and applications. But while we have been leading and benefiting from the information age, there has been too little consideration to the security implications of our growing reliance on information technologies.

A particularly worrisome vulnerability is the extent to which over the past decade, more and more Internet Protocol (IP) devices have been replacing proprietary hardware, software, and communications protocols for the nation's physical infrastructure. As industrial control systems (ICS) become increasingly accessible to the Internet, cyber attacks can be launched at the electrical power grid; water and waste management systems; oil pipelines, refineries, and power-generation plants; and transportation systems ranging from mass-transit to maritime port operations. An attack on these systems by a state or non-state actor, not only places at risk the continuity of service or the compromise of databases, but the potential for catastrophic loss of life and destruction of property. This is because computer hackers are not only able to infiltrate systems, but they are increasingly in a position to actually take control of such systems – turning off alarms or sending bad data that falsely triggers an alarm. Unfortunately, bad actors need not be terribly sophisticated in order to accomplish substantial harm. Because of the interconnectivity of our networks, successful disabling of just one critical system can generate cascading consequences across multiple systems.

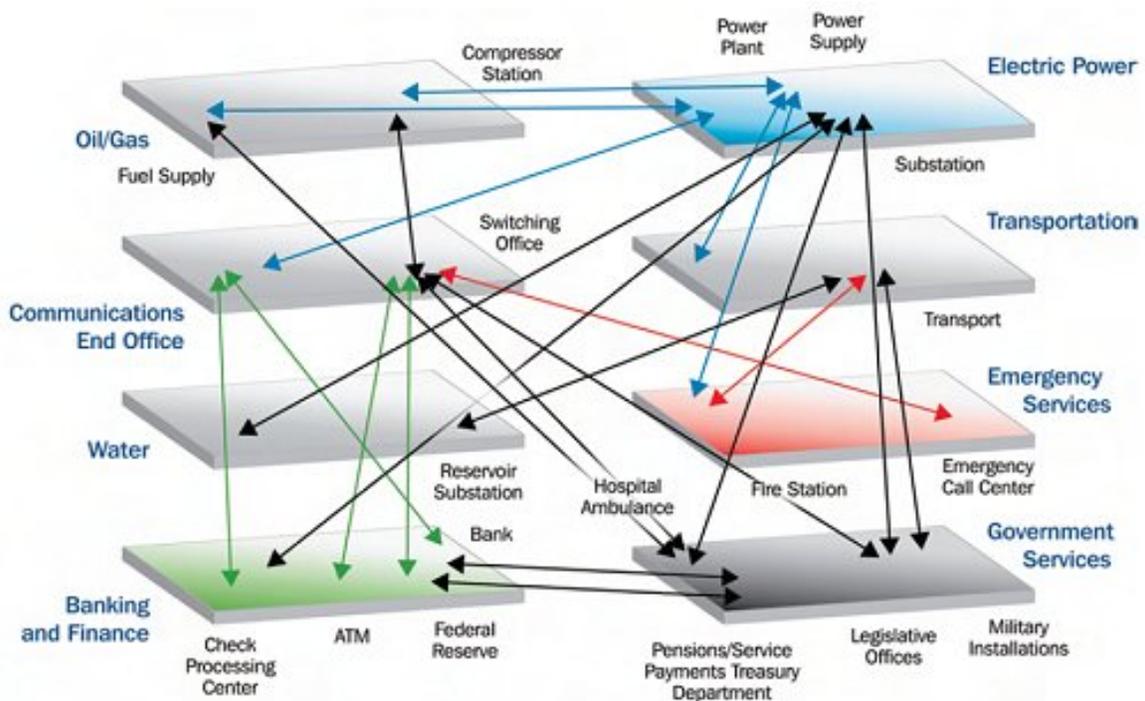
The U.S. power grid is particularly vulnerable to the risk of cyber attacks and given the reliance on power by all other sectors, it deserves special and urgent attention. As with other large and disbursed infrastructures that make up America's critical industrial landscape, managing the electric grid depends on the operation of supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). SCADA systems make it possible to control geographically dispersed assets remotely by acquiring status data and monitoring alarms. Based on the information received from the remote station control devices, automatic or operator-driven supervisory commands can be provided from a centralized location. These field devices can perform such functions as opening and closing breakers and operating the speed of motors based on the data received from sensor systems. Distributed control systems (DCS) are typically facility-centric and used to control localized industrial processes such as the flow of steam into turbines to support generation of power in an electric plant. DCS and SCADA systems are networked together so that the operation of a power generation facility can be well coordinated with the demand for transmission and distribution.¹

When most industrial control systems (ICS) were originally installed to help operate components of the power grid, they relied on logic functions that were executed by electrical hardware such as relays, switches, and mechanical timers. Security generally involved physically protecting access to the consoles that controlled the system. But, over time, microprocessors, personal computers, and networking technologies were

incorporated into ICS designs. Then in the late 1990's, more and more Internet Protocol (IP) devices were embraced so as to allow managers to gain better access to real-time systems data on their corporate networks. These networks are, in turn, often connected to the Internet. The inevitable result of this increased reliance on standard computers and operating systems is to make ICS more vulnerable to computer hackers.²

Tampering with DCS and SCADA systems can have serious personal safety consequences since industrial control systems directly control assets in the physical world. According to a June 2011 report by the National Institute of Standards and Technology (NIST), cyber security breaches of industrial control systems could include unauthorized changes to the instructions, commands, or alarm thresholds that result in disabling, damaging, or shutting down key components. Alternatively, false information about the status of systems can be sent that cause human operators to make adjustments or to take emergency actions that inadvertently cause harm. If a cyber attack leads to a power-generating unit being taken offline because of the loss of monitoring and control capabilities, it could result in a loss of power to a transmission substation, triggering failures across the power grid if other substations are not able to carry the added load. The resultant blackouts would affect oil and natural gas production, water treatment facilities, wastewater collection systems, refinery operations, and pipeline transport systems.³

POTENTIAL CASCADING EFFECTS OF ELECTRIC POWER FAILURE



Source: Department of Homeland Security⁴

A possible scenario hypothesized by the NIST is illustrative:

Using war dialers—simple computer programs that dial consecutive phone numbers looking for modems—an adversary finds modems connected to the programmable breakers of the electric power transmission control system, cracks the passwords that control access to the breakers, and changes the control settings to cause local power outages and damage equipment. The adversary lowers the settings from 500 Ampere (A) to 200 A on some circuit breakers, taking those lines out of service and diverting power to neighboring lines. At the same time, the adversary raises the settings on neighboring lines to 900 A, preventing the circuit breakers from tripping, thus overloading the lines. This causes significant damage to transformers and other critical equipment, resulting in lengthy repair outages.⁵

When transformers fail, so too will water distribution, transportation, communications, and many emergency and government services. Given the 12-month lead time typically required to replace a damaged transformer with a new one,⁶ the local and regional economic and societal disruption caused by a cyber attacks that that disable or destroy the mechanical functioning of key components of the power grid would be devastating.

Beyond this exposure of long-standing industrial infrastructure to cyber threats, there is a serious risk to the emerging computing environment as well. As mobile devices, from smart phones to iPads have proliferated, so too has mobile malware reflecting the painful reality that security still receives insufficient attention by the private sector responsible for rushing to market new informational technology tools and applications. According to a March 2012 company survey conducted at a major IT conference, 68 percent of security professionals reported currently having no way of identifying known mobile device vulnerabilities that could be affecting their networks.⁷ Mobile devices are being targeted to steal users' authentication credentials and financial information. Moreover, as new social networks emerge, users tend not to appreciate the permanent availability of data, which can facilitate hackers' identity theft and identity cloning efforts. It is these growing ubiquitous links on the Internet that makes all Americans vulnerable to cyber threats that can damage very practical aspects of our lives.

The Case for Making Universities Full-Fledged Cyber Security Partners

The potential contribution of American universities and academic institutions in advancing cyber-security has been largely overlooked by the executive branch. There are three reasons why this oversight must be redressed.

- (1) The need for expertise and for an honest-broker to support public-private partnerships. Universities can help bridge the expertise and trust gap between the public sector and private sector in developing standards, and—when appropriate—regulations. Universities can play this role by serving as neutral conveners between the public and private sectors and as arbiters of technical issues. Serving in this capacity should be seen as attractive to both the private sector and public sector, given the unique challenges for each associated with advancing cyber-security.

The private sector, left largely on its own, has struggled to establish and enforce cyber-security standards. In some instances this is because the information asymmetry associated with *moral hazard*; i.e., the developer of technologies and applications pass along risks because the costs will be disproportionately or wholly borne by the IT users that are attracted to the benefits of the tool, but lack an understanding of their resultant exposure to cyber threats and the associated consequences. There is also the *tragedy of the commons* dilemma arising from the fact that an entire system or network can be compromised by an attack on its weakest link. If compliance with a security standard is only voluntary, the vigilant company must worry that one or more of its competitors will find irresistible the temptation to forego the added cost of adopting the measure in a bid to boost market share or profits. As a result, the system remains vulnerable to disruption even if the vigilant company places itself at a competitive disadvantage by investing in the security measure.

The traditional way to deal with the problem associated with *moral hazard* and the *tragedy of the commons* dilemma is by adopting regulations that are well enforced. But, effective regulations largely depend on the public sector having the requisite expertise to develop and oversee them. Unfortunately, in the case of cyber security, the federal government continues to face significant challenges with recruiting and retaining personnel with the appropriate technical background. This is particularly true of the Department of Homeland Security and other federal agencies outside the Department of Defense, the National Security Agency, and the intelligence community.

Universities and the academic community should be enlisted to assist in addressing this deficit. Universities can help the private sector identify reasonable security options that can be embedded into critical infrastructures without causing undue disruption to dynamic and complex systems. Universities can also provide the public sector with the expertise that government policy makers and officials need to keep up with the rapid pace and the growing complexity of information technologies and applications. Beyond the Office of University Programs within the DHS Science and Technology Directorate, Secretary Janet Napolitano has embraced the need for such coordination with the university community by recently establishing a Homeland Security Academic Advisory Council (HSAAC). HSAAC has been created so that the Department has a structured way to receive advice and input from university leaders who voluntarily serve on the Council, including Northeastern University's President, Joseph E. Aoun. In 2011, Secretary Napolitano has also created an Office for Academic Engagement and appointed an Executive Director to serve within her office.

- (2) The imperative to “bake-in” cyber security. Universities have been and will continue to be incubators for information technology and applications. The time for thinking about incorporating safeguards is when they are under development, not after they are being widely used by consumers and industry. When security measures are an afterthought, they often end up being costly and suboptimal. Developing and

maintaining standards that can mitigate cyber threats, vulnerabilities, and consequences, and help to sustain or rapidly recover essential functions and trust need to become an organic part of critical infrastructures, systems and networks. Academic institutions need to be made an active partner in that effort.

- (3) The need to develop a culture of cyber security. Cyber security needs to be embedded in our information-age culture. Everyone needs to have a better understanding of cyber risks. This will require collaborative efforts that actively engage civil society, not just companies and government agencies. There's no better way to develop this culture than by starting with young people who are attending academic institutions. An important way to advance this is to integrate cyber security within and across academic curriculums. Universities should be assigned a prominent role in conducting research, developing courses, and teaching as many informational technology users and providers as possible about the cyber dangers that we face and the security strategies and tactics that we need to embrace. The goal should be to create a new generation of students with the sophisticated skills to harness the opportunities of the information age without becoming victims of its dark side.

The Need for A Coordinated Research & Development Strategy

While pockets of knowledge exist about new and emerging cyber threats and the techniques for better safeguarding systems from attack, too many owners and operators of critical infrastructure continue to embrace information age tools, including wireless and mobile devices, without adequately understanding the associated vulnerabilities and consequences. Faced with significant resource constraints, the federal government is largely trapped in the present, racing to respond to known threats to critical assets, often at the expense of developing the means to better anticipate new threats, to map out the associated risks, and to devise appropriate responses. There is also a national security imperative to develop offensive capabilities to deter or respond to attacks by state actors. It's in these areas that academic partners working together with industry and governments at all levels can be particularly helpful.

I applaud Chairman Dan Lungren and the efforts by Ranking Member Keating to introduce legislation that recognizes that preparing for and combatting cyber warfare requires robust academic, industry and federal research partnerships to design and implement secure systems for critical infrastructure. Yet, to date, the nation's cyber-security leaders have not yet fully engaged the academic research community in this effort. Meanwhile, industry is focused more on the near- and medium-term tasks of developing new products and applications. As the National Academies have noted, it largely falls to the federal government to play the indispensable role in sponsoring fundamental research that is key to developing the information technology talent that is used by industry and other parts of the economy. Chairman Lungren's proposed legislation appropriately recognizes the vital importance of a coordinated federal program of research and development to advance cyber security.

In 2010, the DoD-commissioned JASON Report, *Science of Cyber-security*, outlined the need to establish cyber security science-based centers within universities and other research institutions.⁸ These federally-funded centers would provide government sponsors with access to the regional clusters of innovative ideas and academic experts while concurrently facilitating exposure by researchers to agency experience and expertise in managing cyber threats to government networks. One priority should be to map the risk and potential cascading consequences associated with cyber-attacks on critical physical infrastructure. A second priority should be to advance research that can support the development of technology and automated approaches to detect and mitigate attacks. And another priority should be to enrich our understanding of the human and social aspects of managing cyber vulnerabilities since advancing cyber security involves much more than technical problems.

Regional University-Based Cyber-Security Research Centers

Since information and communications networks are largely owned and operated by the private sector, regional university-based cyber-security research centers should be assigned the task of facilitating an exchange among industry, government, and academic partners to test data and transition new ideas into the rapid adoption of research and technology development innovations. Regional university-based centers should be assigned as their primary mission, developing strategies to improve the security and resilience of information infrastructure and reducing the vulnerability, mitigating the consequences, and speeding the recovery of critical infrastructure in the face of cyber attacks.

As a stepping-off point, these regional university-based research centers should be tasked with working with U.S. national research laboratories to develop a detailed profile of the physical-cyber risk to the electric grid and developing options for mitigating that risk. Understanding the technical elements of the cyber threat to the power grid is a complex, multi-disciplinary challenge, that requires an understanding of networking and protocols, software and machine architecture, formal methods and high-performance computing, nanotechnology, and quantum and compressive imaging, to name a few. Implementing potential solutions will involve an intricate array of not just technical tools, but appropriate procedural protocols, public policy, and regulations. To accomplish this task, the Department of Energy and the Department of Defense should actively support a directed research program that involves a collaborative effort amongst the U.S. national research laboratories, electric utilities, and the university-based cyber security research community to simulate real-life conditions, systems and infrastructure, that would lead to the discovery, testing, and analysis of state-of-the-art tools, technologies and software in a scientifically rigorous manner. Concurrently, the research program should identify policy guidelines and incentives for quickly integrating those tools, technologies, and software into the power grid to bolster its resilience in the face of the cyber threat. This effort should be undertaken with close collaboration with Canada given the interconnected nature of the regional grids in the East and West with the provinces of Canada.

Economic Drivers

Advances in networking and information technology are key economic drivers, crucial to maintaining America's global competitive position in energy and transportation, food and manufacturing, education and life-long learning, healthcare, and national and homeland security. If the recent past is a guide, these advances will also accelerate the pace of discovery in nearly all other fields. In the end, capitalizing on America's peerless standing in higher education by creating regional university-based centers to advance cyber-security, will provide a rich return on investment for the nation.

Conclusion

Beyond the risk of a detonation of a weapon of mass destruction on U.S. soil, no security challenge is currently more serious to the United States than the ongoing risk of cyber attacks. The security of our public and private cyber networks is vital to assuring the reliability of the electric grid, transportation systems, and banking and financial systems, and consumers. Continued research collaboration with academic and industry partners is an important function for the federal government and vital to improving homeland security. Such partnerships provide an important return on investment as government receives solutions tailored to its security needs, university partners employ some of their best researchers and students in an effort to develop new technologies, and the next generation of STEM professionals get the skills and training they need to enter into homeland security careers that benefit the nation. I strongly recommend that this Subcommittee direct the Department of Homeland Security to build on Secretary Napolitano's recent academic engagement efforts by more actively incorporate university partners, including establishing regional university-based cyber-security research centers, to support the DHS's efforts to develop public-private approaches to preventing, responding, and recovering from future cyber attacks.

Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

*Dr. Stephen Flynn is a Professor of Political Science and the Founding Co-Director of the George J. Kostas Research Institute for Homeland Security at Northeastern University. Before arriving at Northeastern in November 2011, he served as President of the Center for National Policy and spent a decade as a senior fellow for National Security Studies at the Council on Foreign Relations. Dr. Flynn served in the Coast Guard on active duty for 20 years, including two tours as commanding officer at sea. He is the author of **The Edge of Disaster: Rebuilding a Resilient Nation** (Random House, 2007), and **America the Vulnerable** (HarperCollins 2004). He is a Senior Research Fellow at the Wharton School's Risk Management and Decision Processes Center at the University of Pennsylvania and serves as a member of the Bipartisan Policy Center's Homeland Security Project, co-chaired by former 9/11 commissioners, Governor Tom Kean and Congressman Lee Hamilton. Flynn holds the M.A.L.D. and Ph.D. degrees from the Fletcher School of Law and Diplomacy, Tufts University. He is the principal for Stephen E. Flynn Associates LLC, where he provides independent advisory services on improving enterprise resiliency and critical infrastructure protection, and transportation and maritime security.*

¹ U.S. Department of Commerce. Guide to Industrial Control Systems (ICS) Security, (Special Publication 800-82, Jun. 2011) by K. Stouffer, J. Falco and K. Scarfone.

² Ibid

³ Ibid

⁴ National Aeronautics and Space Administration. NASA Science News. Severe Space Weather – Social and Economic Impacts. June 2009 at http://science.nasa.gov/science-news/science-at-nasa/2009/21jan_severespaceweather/

⁵ U.S. Department of Commerce. Guide to Industrial Control Systems (ICS) Security, (Special Publication 800-82, Jun. 2011) by K. Stouffer, J. Falco and K. Scarfone. 3-17.

⁶ National Aeronautics and Space Administration. NASA Science News. Solar Shield-Protecting the North American Power Grid. October 26, 2010 at http://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield/

⁷ “Mobile Device Vulnerability Management Flagged as Top Concern for Security Professionals in 2012,” Press Release by Tenable Press Security (Apr 2, 2012)
<http://finance.yahoo.com/news/mobile-device-vulnerability-management-flagged-140900613.html>

⁸ “Science of Cyber-Security” JASON, The MITRE Corp. JSR-10-102 (Nov 2010)
<http://www.fas.org/irp/agency/dod/jason/cyber.pdf>