MIT CENTER FOR INTERNATIONAL STUDIES

Internet Policy Research Initiative

KEEPING AMERICA SAFE:

TOWARD MORE SECURE NETWORKS FOR CRITICAL SECTORS

Cambridge, Massachusetts
March 2017

Joel Brenner
brennerj@mit.edu

Report on a Series of MIT Workshops, 2015-2016

With Recommendations for the New Administration

MIT Center for International Studies
https://cis.mit.edu

MIT Internet Policy Research Initiative
https://internetpolicy.mit.edu

Table of Contents

Executive Summary and Recommendations **3**

A History of Hesitancy **3**

Background: **17**

The Persistent Problem **17**
Expanding Operational Risk 18
Why Are Systems Insecure? 20
Coordinating Research Policy 24

The Workshop Plan **25**
The Sector-Specific Workshops 27
1. Electricity Sector Workshop 27
2. Financial Sector Workshop 33
3. Communications Sector Workshop 40
4. Oil-and-Natural-Gas Sector Workshop 45

Executive Summary and Recommendations

A History of Hesitancy

The digital systems that control critical infrastructure in the United States and most other countries are easily penetrated and architecturally weak, and we have known it for a long time. Yet Presidential leadership on infrastructure security has been hesitant and chiefly rhetorical, while system operators have tended to focus on short-term fixes and tactical improvements. Much effort has been devoted to developing better security standards,[1] but most standards are merely advisory. Key federal departments, notably but not exclusively homeland security, defense, and energy have devoted significant effort to improving infrastructure security. Examples would be too numerous to cite. But these efforts have not altered the strategic balance.

Offense remains dominant. To break this cycle, the nation will require a coordinated, multi-year effort to address deep strategic weaknesses in the architecture of critical systems, in how those systems are operated, and in the devices that connect to them. This effort must in part be technically directed, but it will also require a re-evaluation of the laws, regulations, and policies that govern our networks. The challenges we face are not merely technical. They are also economic, managerial, behavioral, political, and legal. Indeed the technical challenges may be the easiest to address. For example, aligning economic, tax, and liability incentives with the goal of higher security is not a technical challenge. Re-aligning incentives would be a daunting task, but our critical infrastructure cannot be made reasonably secure unless we do it.

This report identifies the most strategic of those challenges and proposes a policy and research agenda that has the potential to achieve significantly higher levels of security in critical networks over a five- to ten-year period. But the nation must begin now. *Our goal is action, both immediate and long-term.*

To address this task, CIS and IPRI jointly convened a series of workshops focused on four critical economic sectors, all of which are overwhelmingly or entirely in private hands: electricity, finance, communications, and oil-and-natural gas (ONG). We did not set out to write yet another description of the threat to our critical networks. In the wake of repeated, widely reported foreign intrusions into our power grid and banking system and the recent Russian interference in our national election, the threat is well known. Rather, we focused

[1] See, e.g., National Institute for Standards and Technology, "NIST Releases Update to Cybersecurity Framework," January 10, 2017, at https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework, accessed February 9, 2017.

on what to do about it.

The workshops were attended by experts[2] from leading enterprises in each sector, by academic experts in relevant fields, and by a few government officials. We expected commonalities across all four sectors, and we found many. Participants in each sector bemoaned the difficulty of quantifying network risk, for example; and each workshop expressed great interest in techniques of containing cascading failure. But we also encountered differences among sectors – in part because the sectors operate in different regulatory frameworks, and in part because two of these sectors – electricity and oil-and-natural-gas (ONG) – are heavily dependent on industrial operating technology (OT) as well as information technology (IT). Significant differences also exist within sectors as well as between them in their levels of investment in cybersecurity and ability to fend off attacks. We have preserved the essence of the individual workshops in summaries at the back of this report.

The Recommendations

This report makes both long- and short-term recommendations of broad applicability to critical infrastructure in the United States and, excepting certain legal and regulatory matters, to critical infrastructure globally. The report identifies eight strategic challenges to illuminate our predicament and guide our policy and research. Under each challenge, it makes findings that emerged from the workshops and recommendations to address them. The recommendations cover a wide range of issues, from the organization of cybersecurity in the Executive Office of the President to technical measures of network security and misaligned regulatory incentives. Each of the challenges is then followed by a series of research questions whose answers could help meet that challenge. The report therefore addresses three audiences: government officials, public and private institutions that fund research, and the researchers themselves. By changing and focusing the research environment, IPRI and CIS believe the nation could materially improve our long-term security environment. We emphasize the c*oordination* of funding, however; we do not propose budgetary measures.

[2] Participants were free to use any information received, but neither the identity nor the affiliation of any speaker or participant could be revealed. Industry participants came from ten private energy companies in the United States, Canada, France, and the United Kingdom, including two of the oil majors; four leading international banks, a major data processor for financial institutions, and a leading securities clearing organization; two tier-one communications providers; a leading computer chip manufacturer; a leading maker of commercial and consumer software; and representatives of the Government of Canada, the U.S. departments of homeland security and energy, and the Office of the Governor of Massachusetts. Participants from firms and governments in India and from another U.S. university were invited but did not attend. The views expressed in this report do not necessarily reflect those of individual workshop participants or of their enterprises and agencies.

Some of these research questions we pose are broad and technical (e.g., Can cyber risk be measured?); others are narrow and focus on non-technical impediments to adopting technically available security measures (e.g., What economic or other factors impede the adoption of secure connections between service providers?). Differences in generality were unavoidable if we were to describe the full range of technical and policy questions that must be answered, especially because many of the impediments are legal, economic, and political rather than technical. Taken together, these questions should form the basis of a focused, national agenda that must be adopted, coordinated, and funded if we are to escape from a twenty-five-year cycle of futile tactical measures and imprecise aspirational statements from a never-ending series of governmental and private groups.

The nation can no longer afford a pattern of uncoordinated executive action and scattershot research. Total security is not achievable. But a materially improved security environment for the infrastructure on which virtually all economic and social activity depend can be created with sufficient resources and political will. Achieving this goal will require a more determined and more directive approach from the highest levels of government and industry. It will also require more energetic and coordinated steps from the President than any of his predecessors has been willing to take.

FINDINGS AND RECOMMENDATIONS

FIRST CHALLENGE

Improve Coordination.

Finding:

> Critical infrastructure defense is insufficiently coordinated across the government. Changing the status quo will require a more directive effort from the White House.

Recommendation:

> **The President should elevate his cybersecurity advisor to the position of deputy national security advisor for cybersecurity. That official should be directed and empowered to work with the Office of Management and Budget (OMB) to focus long-term policy across the government on the substantive challenges identified below and to produce on an accelerated schedule a federal research agenda and budget for the cybersecurity of critical infrastructure focused on these same challenges. OMB should determine that funds are spent accordingly.**

SECOND CHALLENGE

Measure cyber risk and infrastructure fragility.

Finding:

> Quantifying risk in either absolute or relative terms is a difficult challenge that impedes cybersecurity investment in all sectors examined except certain financial institutions. The asserted inability to measure the rate of return on cybersecurity investment is a closely related problem[3] that affects overall investment levels and makes it difficult to target investment. Fragility of systems is a salient aspect of risk that concerned participants in all sectors. Absent assurances of confidentiality, candid participation by the private sector will not occur. However, the public should be informed of the general state of security of critical infrastructure.

[3] Most participants accepted the view that cyber risk, changes in cyber risk resulting from a specific security investment, and the rate of return on that kind of investment could not be measured. For the contrary view, see Douglas W. Hubbard and Richard Seiersen, *How to Measure Anything in Cybersecurity Risk* (New York, 2016).

Recommendation:

> **The President should direct the lead departmental secretary to convene on an accelerated schedule a meeting of representatives of the relevant national laboratories and other experts to assess impediments to measuring cyber risk and fragility and to recommend a national strategy to meet this challenge. The meeting should be closed to the public and its proceedings, though not the strategy, should be kept confidential.**

Research Questions:

1. Can cyber risk or network fragility be measured? Can changes in risk as the result of specific security investments be measured? If so, why are enterprises not doing it?

2. Would the answers to these questions produce more rational decision-making by enterprises? If not, why not?

3. Can simulation-based modeling be used to create cybersecurity stress-tests for critical sectors? In the electricity sector, could that type of modeling be used to test the ability to "cold start" electricity generation? Can the results of such modeling be protected from public disclosure? How, and at what level of generality, should the public be informed of vulnerabilities in critical systems?

4. Should the answers to these questions have regulatory implications for some or all critical sectors?

5. Can the necessary de-identified[4] data be obtained to support research into these questions? Would legislation be appropriate to compel the production of that de-identified data in the interest of national security – but with an exemption from disclosure and under a legal privilege that would prevent its use for any other purpose?[5] How would the required data be defined, and who should hold it?

[4] De-identification means removing identifying aspects of data so that, practically speaking, it would be difficult and expensive to re-associate it with a particular person. Perfect anonymization of data is not possible in most circumstances.

[5] The National Infrastructure Protection Act, codified as 42 U.S.C. §§ 5195c et seq., does not clearly give the Department of Homeland Security power to require production of specific categories of data from private firms. See 42 U.S.C. § 5195c (d)(2)(A) and (B).

THIRD CHALLENGE

Review laws and regulations with the goals of reducing risk and optimizing security investment.

Finding:

Participants from all sectors overwhelmingly believed there was a material disconnection between mandatory compliance regimes and improvements in cybersecurity. Most participants from all sectors except finance believed that federal tax and regulatory incentives for higher levels of cybersecurity investment should be considered. Many participants from the electricity and telecommunications sectors believed that regulations either impeded or did not encourage higher levels of cybersecurity investment.

Recommendations:

The President should propose legislation at the earliest opportunity for the more favorable tax treatment of qualified cybersecurity investment in critical infrastructure and, potentially, throughout the economy, including investment necessary to convert to a more secure DNS and to more secure border gateway protocols. To qualify for favorable treatment, investments should be in products and services that are demonstrably compliant with the framework promulgated by the National Institute for Standards and Technology (NIST).[6]

The secretary of energy, state public utility commissioners, and the National Association of Regulated Utility Commissioners should forthwith examine the effect of utility regulation on cybersecurity with particular attention to (i) the effect of current regulations on cybersecurity investment and (ii) the usefulness of current compliance standards in achieving higher levels of security.

[6] National Institute for Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," version 1.0, February 12, 2014, at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, accessed February 20, 2017. For draft version 1.1 of the Framework, see https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, accessed February 20, 2017.

Research Questions:

1. How should liability rules and regulations be optimized to produce more secure behavior by vendors and by the owners and operators of infrastructure? A comparative study of state as well as federal regulatory models would be useful in addressing this question.

2. Can cybersecurity regulation be harmonized across government? Government regulates by sector. For example, the Federal Communications Commission regulates telecommunications; the Treasury Department, the Federal Reserve, and other agencies regulate banks; the Energy Department, the Environmental Protection Agency, and the states regulate energy, and so on. But as these "vertical" regulators have also begun to regulate cybersecurity, a complex of overlapping, expensive, and potentially inconsistent standards is emerging. Are these regulations driving greater security, or are they merely more elaborate and expensive compliance regimes?

3. The many competing compliance standards create confusion. Should the government make the NIST Framework, and only the NIST Framework, a single mandatory standard across government and for contractors dealing with the government?

4. Could the financial impact on insurers and re-insurers of the damage resulting from a successful attack on one or more critical sectors be absorbed by them? If not, what law and policy would be required to make it likely that such losses could be absorbed?

5. Can the necessary, de-identified data be obtained to support research into these questions? If not, would legislation be appropriate to compel the production of that de-identified data in any sector while protecting the rights of the enterprises that would produce the data? How would the required data be defined?

FOURTH CHALLENGE

Enable critical infrastructure operators to quickly identify and respond to cyber risk arising from cross-sector linkages as well as from their own networks.

Finding:

All sectors depend on electricity, and the financial sector's global platform supports transactions with energy and telecommunications. These and other linkages create possibilities for cascading failure that are insufficiently understood and not adequately illuminated by sector-specific simulations and other testing. Participants from all sectors stated emphatically that cooperation on pooling proprietary data and candor regarding the results of testing could not be achieved unless parties could be assured that the data and results would remain confidential and could not be used for other purposes.

Recommendation:

The President should direct the lead departmental secretary to convene on an accelerated schedule a meeting of representatives of the nation's leading industrial insurers and other experts to examine the steps necessary to enable more robust cross-sector simulations, including the sharing of data, and to make appropriate recommendations to the President. The meeting should be closed to the public and its proceedings kept confidential, but the resulting recommendations should be public.

Research Questions:

1. What steps would increase the likelihood of early detection of a slow-moving strategic attack on a critical sector or across critical sectors? How will detection techniques be affected by the anticipated move to IPv6?[7]

2. How would such an attack affect critical backup systems?

3. Can simulation-based modeling be used to create better cross-sector stress tests?

4. Can simulated cyber disasters help determine how communications should be prioritized in the event of a national emergency?

5. Can efforts to use big data and fast processing to quickly detect intrusions in critical networks be accelerated?

6. What, if anything, prevents the effective use of identity management tools across the full range of steps necessary to execute a successful exploit or attack?

[7] IPv6 is an Internet addressing protocol that would expand the number of IP addresses available under the current protocol, called IPv4, by a factor of 7.9 x 10^{28}. It could therefore render ineffective current techniques for scanning systems for malware because the address space to be scanned would be exponentially larger.

FIFTH CHALLENGE

Reduce component complexity and the vulnerabilities inherent in them.

Finding:

Participants from the electricity and energy and oil-and-natural gas (ONG) sectors believed that unduly complex, and insufficiently secure, hardware, software, and industrial controls were a significant source of cyber vulnerabilities that created physical danger as well as risk to information. Participants from the ONG sector were emphatic on this point. Both energy sectors are highly dependent on industrial operating technology. This is a significant supply chain risk created by commercial, not technological, factors. Suppliers find it profitable to market cheap, general purpose hardware and software for multiple uses, regardless of differing security tolerations in different sectors and uses.

Recommendation:

The President should direct the lead departmental secretary to report to him on an accelerated schedule on the feasibility, timeline, and expense of supporting and otherwise incentivizing the production and use of more secure and less complex hardware, software, and controls for use in critical infrastructure.

Research Questions:

1. Can the technical, economic, and regulatory obstacles to reducing complexity in both information technology and industrial operating technology be identified?

2. Field programmable gate arrays (multipurpose computer chips) are cheap, so they are used for many purposes including commercial routers and industrial controls used in critical infrastructure operations, but their complexity and superfluous functionality increase risk. The same may be said of general purpose processing units, operating systems, and software systems.

    a. Can standards be established to reduce the vulnerabilities in logic processors and the software and firmware that control them?

    b. Can standards be established, or incentives created, to phase out design tools that permit hardware and software designers to make the same basic errors repeatedly, such as allowing buffer overflows?

c. What steps would be necessary to establish a certification system for hardware and software, possibly modeled on the Underwriters Laboratory for electrical products?

d. Can microchips be designed so that entire sectors of those chips can be cheaply, reliably, and verifiably disabled so that functionality matches task requirements?

3. What incentives should be in place to induce controls manufacturers and Internet service providers to use less vulnerable chips?

4. Are the departments of defense, energy, and homeland security optimizing their role in creating and supporting a market for simpler and more secure commercial devices in critical infrastructure? For example, can these departments jointly establish metrics for complexity and standards for controls, and use their procurement decisions to favor less complex and more secure hardware and software?

5. Can simpler firmware and operating systems be cost-effectively developed and marketed for use in critical infrastructure?

Sixth Challenge

Address fundamental issues of system architecture.

Findings:

1. The Internet is a legacy system designed for non-commercial uses with little or no need for security. Security has chiefly been an option for end points, which frequently ignore it in favor of speed-to-market and low costs. Hardware and software that run on the Internet display wide differences in security, and the tools for creating hardware and software enable many of the same security errors to be repeated over many years, without liability.

2. Security professionals from all sectors overwhelmingly believed that certain aspects of their systems could not otherwise be made reasonably secure unless isolated from public networks. There are significant differences of opinion about appropriate degrees of isolation.

Recommendations:

1. The President should direct the secretaries of energy and homeland security:

a. in consultation with the Federal Energy Regulatory Commission (FERC), to explore the feasibility, expense, and timelines of isolating from public networks[8] all controls and operations of activities within FERC's jurisdiction,[9] to define acceptable degrees of isolation, and to report to the President on an accelerated schedule; an

b. in coordination with the FERC and the North American Electric Reliability Corporation (NERC),[10] to convene at the earliest practical time a conference of state electricity regulators to explore the feasibility and expense of isolating key elements of electricity generation and delivery from public networks.

2. The President should direct the lead departmental secretary to consult with key stakeholders, including vendors, users, the public, and the insurance industry, about the desirability and feasibility of (i) establishing legally binding standards of care in the manufacture of hardware and software for critical infrastructure, and (ii) the establishment of a privately owned and managed accreditation bureau for such hardware and software, and to report to the President on an accelerated schedule.

Research Questions:

1. Should some operations of some or all critical sectors be isolated from the Internet? If so, which ones? How should "isolation" be defined? What level of isolation would be appropriate for particular systems in critical applications? Who should determine that?

[8] This is not a recommendation to create a single non-public energy network. Isolation from public networks does not imply isolation from efficient, digital operating systems that produce real-time, or near real-time, information about those systems. Non-public information and operating systems based on TCP/IP protocols are available or can be created.

[9] FERC has jurisdiction over the interstate transmission of electric power. Power generation and delivery are regulated by the states and territories.

[10] NERC is composed of the owners and operators of the grid and has been named by FERC as the "Electric Reliability Organization." It is charged by Congress to "establish and enforce reliability standards for the bulk-power system," subject to FERC's oversight.

2. Can block chain or other technology be used to verify accounts in a timely fashion to reduce the risk of corrupted backup systems and wiped accounts?

3. What changes to security architectures would let us more efficiently manage system accesses and identities for devices, people, applications, and data, both internally and externally?

4. Can a system be designed so that its failure would be immediately transparent to its operator? Can the state of the system's algorithms be made understandable to humans? Would it be cost-effective to impose audit requirements on that kind of system? (E.g., if a driverless car ran off a bridge, could its control algorithm be made to explain why it did that?) If so, why don't we mandate that kind of auditability in critical sectors?

5. What economic, regulatory, or other factors impede the more rapid phasing out of legacy components of electronic systems in favor of components that are not merely newer but are demonstrably more secure?

6. What economic or other factors impede the adoption in the private sector of the existing but largely unused secure domain name system or an alternative security architecture? What incentives could accelerate the adoption of a more secure domain name system?

7. In the communications sector, what economic or other factors impede the adoption of secure border gateway protocols that would make it impossible, or substantially more difficult, to divert network traffic? What incentives could accelerate the adoption of that type of control?

8. Companies have differing interests. Academics make a living by disagreeing with one another and often prefer the notional perfect to the achievable good. Universal agreement on a domain name system and border gateway controls is therefore not achievable. Is there a point, short of war, when the Congress should make these choices?

9. The Internet of Things makes attack surface management geometrically more difficult. What aspects of insecure devices matter most in this respect? Should enhanced security be applied at the device level or only at higher levels within networks?

10. Would it be feasible and efficient in a virtual network to segregate or at least identify all executable code, thus making unauthorized executables more readily discoverable?

SEVENTH CHALLENGE

Formulate an effective deterrence strategy for the nation.

Findings:

> The cybersecurity postures and capabilities of the United States and its peer or near-peer competitors in cyberspace have served to deter outright attacks against one another's critical infrastructure, but have been unsuccessful in deterring lower-level but increasingly harmful cyber operations across our economy, society, and political system. Hostile acts are systematically carried out below the level of armed conflict that have the potential to gradually reduce this nation's stature and security and its ability to lead free and open democracies around the globe. In this gray space between war and peace, the United States does not have an effective deterrence strategy against either nation-states or transnational groups bent on terror or other forms of disruption of our critical infrastructure.

Recommendation:

> **The President should direct his national security advisor to review the nation's deterrence strategy. That strategy should include, but not be limited to, (i) hardening critical American systems and infrastructure; (ii) raising the price for attacking them; (iii) constructing a diplomatic strategy for achieving verifiable cybersecurity agreements with potential adversaries; and (iv) evaluating the nation's ability in the long term to maintain offensive dominance in cyberspace and the stabilizing or destabilizing effect of attempting to do so.**

Research Questions:

1. In view of the demonstrated ability of certain nation-states to exploit critical networks for economic, political, and potentially military advantage, would a more directive policy toward hardening critical networks be justified? Would that course of action be politically acceptable in the United States and among other nations involved in global transactions and telecommunications?

2. Cyber network operations by capable nation-states and their proxies are difficult or impossible to prevent, yet we expect critical infrastructure operators to defend themselves against these attacks. Is this the right public policy? If not, what policy should replace it?

3. Will the pursuit of offensive dominance in cyberspace continue to be feasible in the next five to ten years? Will its pursuit be inconsistent with order and stability in cyberspace, as it proved to be in the strategic nuclear relationship with the Soviet Union? What are the implications of the answers to these questions for American diplomatic strategy in cyberspace?

   Is the President receiving robust counter-strike options, both military and non-military, for cyber intrusions, including those that do not rise to the level of armed conflict under international law?

4. Is any department of government conducting realistic simulations and other exercises to explore the consequences of non-military counter-strikes in response to a cyberattack? Does the President's understand and approve of the assumptions that underlie these exercises?

EIGHTH CHALLENGE

Accelerate and improve the training of cybersecurity professionals.

Findings:

There is a serious dearth of cybersecurity expertise in the United States, especially at advanced levels. The nation does not produce enough graduates with advanced cybersecurity skills or with skills in both cybersecurity and in the operation of industrial operating systems.

Recommendation:

The President should appoint a blue-ribbon commission on the feasibility of increasing the supply of highly trained computer scientists and engineers and developing model curricula for training computer scientists and engineers in the defense of critical systems. The commission should report to the President within 180 days.

Research Questions:

1. Adm. Hyman Rickover created a rigorous model for selecting and training nuclear submariners. Should government or industry adopt his model for the cyber defense of critical infrastructure?

2. Can effective network defense skills be taught without also teaching high-level offensive skills? If not, given the risk of teaching those skills to a wider cadre, who should be eligible to receive that instruction? Should qualified trainers, in defined circumstances, be granted liability protection for teaching offensive tactics?

3. Are different core curricula appropriate to train people to operate and defend the networks of different critical infrastructures? If so, who should develop them?

4. Should people in cybersecurity disciplines be subject to specialized training and certifications, as in other professional disciplines?

This is a time for action. It is also a time for calm, long-term strategic thinking, based on sound research, into the underlying causes of cyber insecurity and how to address them.

Background:

The Persistent Problem

In the United States, Presidential Directives to address infrastructure risk have emerged from the White House like clockwork for more than twenty-five years. In 1990, President George H.W. Bush announced to the country what intelligence officials, but not many others, already understood: “Telecommunications and information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the foreign intelligence threat. . . . “

In 1998, as enterprises were beginning to shift both information systems and operations to the Internet, President Clinton warned of the insecurities created by cyber-based systems. In 1998 he directed that “no later than five years from today the United States *shall have achieved and shall maintain* the ability to protect the nation’s critical infrastructures from intentional acts that would significantly diminish” our security. Five years later would have been 2003.

In 2003, President George W. Bush implicitly recognized that this goal had not been met. He stated that his cybersecurity objectives were to "[p]revent cyber attacks against America's critical infrastructure; [r]educe national vulnerability to cyber attacks; and [m]inimize damage and recovery time from cyber attacks that do occur." Meanwhile, virtually all commercial and operational activity was migrating to the Internet, which remained insecure.

By 2009, concerns about critical infrastructure had become acute. President Obama said:

> The architecture of the Nation's digital infrastructure, based largely on the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat ….

By 2013 – fifteen years after President Clinton had said the country's critical infrastructure should be secure from malicious disruption by 2003 -- President Obama acknowledged that the goal had not been met: "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." The view at the enterprise level is much the same. Trend Micro, a leading Internet security firm, reported in 2015 that critical infrastructure operators throughout the Western hemisphere "painted a picture that depicts the threat [to their networks] as being severe, while some perceived the future of securing these infrastructures as bleak."

The question the nation faces is therefore this: Are we condemned to remain in this unstable and insecure condition, in which the best we can do is to repeat urgent but futile warnings from high places and, at the operational level, merely to refine our tactics in a losing game of Whac-A-Mole? To find an answer, we gathered experts from industry, government, and academia, to imagine – in President Obama's phrase – "a *significant change in how [systems] are constructed or operated."* This meant going beyond the intense and difficult day-to-day tactical challenges that critical sector operators face, important as they are, to imagine a better security environment in five to ten years and to understand what keeps us from getting there.

Expanding Operational Risk

For the owners and operators of critical infrastructure, the prime concern is risk to continuity of operations rather than theft of information, though that, too, is a serious risk. An intruder who can steal massive amounts of data from a system remotely can also corrupt the information on the system, or wipe information from it, or shut it down.

Information technology and industrial operating technology have largely converged. A decade ago, researchers at the Idaho National Laboratory proved they could physically destroy a diesel-electric generator using only a keyboard and a mouse.[11] Real-world examples soon followed.

In 2010, the centrifuges used to enrich uranium gas at Iran's Natanz nuclear facility started failing rapidly. The Iranians were baffled – until researchers in Germany diagnosed the Stuxnet virus, now widely attributed to the intelligence services of the United States and Israel.[12] In 2012, cyber attacks from Iran wiped all information from thirty thousand computers at the world's largest oil refiner, Saudi Aramco.[13] In 2014, an unidentified intruder used a spear-phishing ruse to gain access to the network of a German steel mill, then caused multiple components of the industrial control system to fail, resulting in massive physical damage.[14] Meanwhile, starting in 2011, a Russian operation known as "Dragonfly/Energetic Bear" began targeting North American aviation companies before shifting to U.S. and European energy firms. Its targets included "energy grid operators, major electricity generation firms, petroleum pipeline operators, and Energy industry industrial control system (ICS) equipment manufacturers. Most of the victims were in the United States, Spain, France, Italy, Germany, Turkey, and Poland."[15] There were no reports of damage from these penetrations; they appeared to be reconnoitering exercises that could facilitate damaging attacks on the systems later, if the intruder chose to attack. In 2015 the prospect that an attacker might launch a damaging attack on an adversary's energy grid became reality when portions of Ukraine's power grid were disabled for several hours in a coordinated attack on three energy firms. This was the first publicly acknowledged attack on a power grid. The Ukraine government immediately blamed Russia. The attackers employed a range of sophisticated tools, but in the view of several analysts, "the strongest capability of the attackers was not in their choice of tools or in their expertise, but in their capability to perform long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multisite attack."[16]

[11] "The experiment used a computer program to rapidly open and close a diesel generator's circuit breakers out of phase from the rest of the grid and cause it to explode." Wikipedia, "Aurora Generator Test," at https://en.wikipedia.org/wiki/Aurora_Generator_Test, accessed January 6, 2017.

[12] Wikipedia, "Stuxnet," at https://en.wikipedia.org/wiki/Stuxnet, accessed November 16, 2016.

[13] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012, at http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html, accessed December 23, 2016.

[14] R.M. Lee et al., "German Steel Mill Attack," SANS Institute, ICS Defense Use Case, December 30, 2014, at https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf, accessed December 23, 2016.

[15]June 30, 2014, at https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat, accessed December 6, 2016.

[16] Lee et al., "Analysis of the Cyberattck on the Ukrainian Power Grid," SANS Institute, ICS Defense Use Case, March 18, 2016, at http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf, accessed December 23, 2016.

This is the offense-dominant environment that critical infrastructure operators now live in. Network defense has certainly gotten better in the last fifteen years in absolute terms, but so has the offense. Relative to the increased resources and sophistication of criminal and nation-state attackers, it is doubtful the defense has improved at all. Attacks are still easy and cheap to launch and difficult and expensive to defend against.

The offense continues to enjoy inherent advantages owing to human fallibility, architectural flaws in the Internet and the devices connected to it, massive data aggregation, and pervasive interconnectivity. And the attacker must succeed only once, while the defense must succeed thousands or millions of times. Connecting geographically dispersed operating equipment to the Internet has brought undoubted efficiencies to electricity generators and other industries, but it has also created dangerous vulnerabilities in the systems that keep the lights on and power the economy. In late 2016, the recently retired chief security officer of AT&T said it was "inevitable that significant, large-scale cyber attacks will be launched against our critical infrastructure [in the coming four years]. These attacks will shift from the theft of intellectual property to destructive attacks aimed at disrupting our ability to live as free American citizens. I do not know of a single cyber security expert in our country who would disagree with this view."[17] We concur.

Why Are Systems Insecure?

When the Internet was being designed in the early 1970s, it was not initially clear what the important security issues were. Its initial purposes were to assure communications in the event of a nuclear attack through packet-switched routing, and then to serve as the basis for collaboration among geographically dispersed scientists working for the Department of Defense. The relatively few people having access to the original network were a trusted group for whom security was not an issue. Insofar as the network's sponsors in the Department of Defense and the intelligence community thought about security, they preferred that security challenges be pushed onto the attached end-nodes, without appreciating the difficulty of doing so. The Internet's designers understood that many security problems would best be addressed through encryption, but encryption was not a commercially practical technology at the time for reasons of performance and lack of open standards. At the time, encryption was also regulated as a munition for export purposes. These considerations, together with the imperative to get the Internet to work at all, led to several classes of security problems. In particular:

[17] Edward Amoroso, "An Open Letter to the President-Elect on Cyber Security," LinkedIn, November 25, 2016, at https://www.linkedin.com/pulse/open-letter-president-elect-cyber-security-edward-amoroso, accessed December 10, 2016.

1. Several of the core control protocols and supporting services of the Internet were designed without an approach to security, and adding security after the fact has proved more difficult than anticipated. These protocols include the global, inter-domain routing protocol (Border Gateway Protocol or BGP), the Domain Name System (DNS),[18] and the Certificate Authority system. In all these cases, secure alternatives have been proposed but have not been taken up in the marketplace. What the original designers thought would be a technical challenge has turned out in all cases to be a challenge created by misaligned economic incentives, poor coordination and leadership, a lack of global trust among stakeholders, and disagreements about what the security problems are.

2. Strictly speaking, the Internet is simply the network that connects end-points using a technical protocol called "TCP/IP."[19] It was never meant to police itself for criminal or offensive behavior. To a significant degree, therefore, the Internet is doing what it was designed to do: that is, to connect end-points. Many (perhaps most) of the vulnerabilities in our systems occur at other levels – in hardware designed with little or no consideration for basic security, for example;[20] in carelessly written software;[21] and in applications created for quick market penetration that are unable to meet reasonable security requirements.[22] In the early days of the Internet's development, the designers paid relatively little attention to the challenge of developing secure applications, since in their view they had no control over what application designers could do. Most application designers today are motivated by features, time to market, and return on investment. These priorities align poorly with security. This set of actors is highly diverse, unregulated, transnational, and sometimes hard to find, and it is not clear what approach could be used to nudge them to attend more to security.

[18] "Domain Name System," Wikipedia, at https://en.wikipedia.org/wiki/Domain_Name_System, accessed December 12, 2016.

[19] For definitions of the Internet and TCP/IP protocols, see respectively Wikipedia at "Internet," https://en.wikipedia.org/wiki/Internet, and "Internet Protocol Suite," https://en.wikipedia.org/wiki/Internet_protocol_suite, both accessed January 7, 2017.

[20] For the IoT attack on an important Internet company, see Schneier on Security blog, "Lessons from the Dynamics's DDoS Attack," https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html; James Scott and Drew Spaniel, *Rise of the Machines: The Dynamics's Attack Was Just a Practice Run,* December 2016, Institute for Critical Infrastructure Technology report, at http://icitech.org/wp-content/uploads/2016/12/ICIT-Brief-Rise-of-the-Machines.pdf, accessed January 8, 2017.

[21] See, e.g., Wikipedia, "Buffer Overflows," at https://en.wikipedia.org/wiki/Buffer_overflow, accessed January 3, 2017. Buffer overflows have been known to be a security vulnerability for years.

[22] See, e.g., Lucian Constantin, "App Developers Not Ready for Stricter IoS Security Requirements," Computerworld, December 6, 2016, at www.computerworld.com/article/3147373/security/app-developers-not-ready-for-stricter-ios-security-requirements.html, accessed December 7, 2016.

3. There is no agreement today on who, if anyone, should be responsible for making the Internet ecosystem more secure. For example, it can be extremely difficult, even impossible, to be certain who you are communicating with on the Internet. Identities can be easily spoofed and websites counterfeited, enabling fraud. But which actors in the Internet ecosystem should undertake to fix this? Should the packet-forwarding layer of the Internet attempt to impose a single, global identity scheme that applies to all applications? Doing so would raise yet again the question of global trust and coordination. It would make anonymous action very difficult. That would reduce crime, but it would also enhance surveillance powers and thereby threaten privacy. Should the large and uncoordinated community of application designers be told that identity assurance is their problem? In fact, the solution probably requires support at all layers. But there is no institutional forum in which an allocation of responsibility can be resolved.

4. Data files, which are passive, and executable files, which perform operations on data, cannot be distinguished as they are transmitted across the Internet. But this approach left the discrimination between data and executable files to the application designers in the end-nodes, who were often indifferent to the issue. As a result, malicious executables are easily disguised among large quantities of data. They are easy to insert and extremely difficult to find in a large database or system. This problem became much more difficult once data files (e.g., a Word file) were designed to embed executable code (e.g., macros).

After Congress made the Internet generally available for commercial use in 1992, the network became the backbone of our entire system of economic and social communication, and increasingly of our physical operations, so these inherent weaknesses assumed enormous significance. As Richard Danzig has noted, "Cyber systems create serious security problems because they concentrate information and control and because the complexity, communicative power and interactive capabilities that enable them unavoidably create vulnerabilities."[23] Putting massive amounts of information in one place, which is highly efficient, also facilitates massively efficient theft. And connecting almost everything to almost everything else, which is also efficient, means that a vulnerability in any part of the interconnected system is a vulnerability in every part of it. These factors, together with the difficulty of tracing and attributing attacks, make the Internet a prime environment for criminals.

[23] Richard Danzig, "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies," Center for a New American Security (July 2014), p. 9, at https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies, accessed December 24, 2016.

It is a serious error to assume that cybersecurity is entirely a matter of technical specifications and system design. Poor business management, lack of clear responsibility within organizations, and bad user behavior would continue to create significant vulnerabilities even if the technical issues could suddenly be fixed. Last year, when for the first time the Bank of England included cybersecurity as a major risk factor for the financial stability of the United Kingdom, its number one finding was, "Overemphasis on technological (as opposed to management, behavioural and cultural) aspects weakens cyber defensive capabilities."[24] We concur.

A common human error enabling fraud is susceptibility to an online scam known as phishing. Phishing involves sending a mass email that appears to come from a trusted source such as a bank or a well-known company, but does not. A recipient (the "phish") who opens the email and clicks on the attachment unwittingly downloads malware. The purpose of the malware varies. It may steal information such as passwords or credentials, or it may enlist the recipient's machine in a campaign to advertise pornography, drugs, etc. Phishing campaigns are nearly cost-free to conduct and are highly successful. According to Verizon, thirty percent of recipients open phishing emails, and about a third of them click on the attachment. "The median time for the first user of a phishing campaign to open the malicious email [was] 1 minute, 40 seconds. The median time to the first click on the attachment was 3 minutes, 45 seconds …."[25]

Spear phishing is a socially engineered fraud aimed at a specific person, often a corporate or government official. This is a favorite tactic of sophisticated criminal gangs and intelligence services, which can craft an email that appears to come from a trusted person on a topic that the recipient is known to be interested in. Sometimes the malware is automatically downloaded merely by opening the email. In a recent survey by Trend Micro, "spear-phishing tactics were cited by all responding members as the single biggest attack method they had to defend against, with the exploitation of unpatched vendor software vulnerabilities being a distant second." Whether an effective technological defense to this vulnerability can be deployed remains to be seen.

Weaknesses in the email system also contribute to identity spoofing. The basic design of email is older than the Internet; it existed in the late 1960s in an earlier internal Defense Department network called ARPAnet. There seemed to be little need in those days to build an authenticated identity system to validate the sender of an email on a closed system involving trusted parties. Since that time, there have been proposals put forward to secure email by having the sender sign the mail in a trustworthy manner, but those proposals achieved little market traction owing to lack of market demand,

[24] Bank of England, "Financial Stability Report," July 2015, Table A.10, p. 32, at http://www.bankofengland.co.uk/publications/Documents/fsr/2015/fsrfull1507.pdf, accessed January 6, 2017.

[25] Verizon, "2016 Data Breach Investigations Report," p. 18, available at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/, accessed December 24, 2016.

engineering complexity, development costs, disagreements about the correct approach, the lack of an institution that could exercise acceptable global leadership, and so on. There would also be little if any market advantage to incurring these costs if others failed to follow. These issues are not technical.

The vulnerabilities at all levels of the cyber environment have been well known for years, yet many firms fail to take basic security precautions. And it is still the case that a large majority of intrusions are discovered by law enforcement and other third parties and not by the enterprise that owns the network.[26] Even among owners and operators of critical infrastructure, decisions to expose their operations to these vulnerabilities have repeatedly been made with little or no regard for the risks thus imposed on the enterprise, let alone the risks imposed across the entire economy. Enterprises that expose their operations to the Internet must accept Internet services as they find them, replete with vulnerabilities, and protect themselves accordingly. Insofar as those enterprises are regulated, the cost of doing so should be reflected in the rates they are permitted to charge.

In short, profound network *in*security has persisted for twenty-five years for many reasons. A problem this enduring in so fundamental an area demands concerted attention. It also calls for concentrating resources devoted to research and development efforts (R&D) into technologies *and policies* to make attacks more difficult and expensive to launch and less difficult and expensive to combat.

Coordinating Research Policy

There has been no shortage in recent years of federal pleas for research into critical infrastructure cybersecurity, but they have tended to remain general and hortatory. In 2009, for example, the Department of Homeland Security (DHS) published "A Roadmap for Cybersecurity Research" that identified an important problem set but did not develop a research agenda to deal with it. In 2011, the National Science and Technology Council (NSTC) articulated the need for federal spending in basic cybersecurity research but was content to describe challenge areas (e.g., mobile security, creation of trusted spaces, etc.) rather than specific areas for research.

In 2013 a presidential policy directive emphasized that research was a critical aspect of achieving critical infrastructure security and resilience[27] but was not specific. In

[26] Verizon, 2016 DBIR, p. 11, fig. 9.

[27] Resilience is the ability to operate at an acceptable, if suboptimal, level of performance in the face of attack or failure. For a thoughtful exploration of this concept, see Harriet Goldman, "Building Secure, Resilient Architectures for Cyber Mission Assurance," Case 10-3301, MITRE Corp., 2010, at https://pdfs.semanticscholar.org/911a/9c301359a0bcbdc3e49b2f7a04cf7eef14b2.pdf, accessed January 5, 2017.

June 2014, a subcommittee of the NSTC issued a cogent statement of federal cybersecurity research objectives, but did not identify a path to get there. Last year DHS brought additional attention to the challenge with its R&D plan for research in this area, but the plan did not go beyond a general statement of objectives. Reports and directives from high levels of government are inevitably general, but lack of follow-through and inattention to detail are not inevitable. At the agency level, specific but uncoordinated research projects are underway to tackle technical cybersecurity problems. For example, at the Defense Advanced Research Project Agency (DARPA) a project on Organically Assured and Survivable Information Systems (OASIS) focuses on increasing fault tolerance in systems and networks. But these programs are not coordinated, and many of the general problems described in high-level government documents remain insufficiently addressed, if addressed at all.

Against this background, the nation must devote substantial *coordinated* resources (1) to identify the most salient risks to critical infrastructure networks, and (2) to describe specific cybersecurity objectives that could reduce those risks and that could be broken into manageable research projects. This is what IPRI and CIS have sought to do.

The Workshop Plan

IPRI and CIS convened four sector-specific workshops to study the challenge of a coordinated research and policy plan, and later a fifth workshop to distill what we learned from the first four. It was clear from the start that "critical infrastructure" had become too broad a rubric to guide our work. In the United States, the term means "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[28]

Sixteen sectors have now been designated "critical." We therefore selected four sectors we deemed most critical,[29] and scheduled the following day-long workshops, all held in Cambridge, Massachusetts at MIT:

• Electricity	October 8, 2015
• Finance	November 5, 2015
• Communications	December 3, 2015
• Oil and Natural Gas (ONG)	February 8, 2016
• Final Workshop	May 2, 2016

[28] 42 U.S.C. § 5195c (e).

[29] Time constraints precluded an additional workshop on the transportation sector.

Participants came from key industry firms in the United States, Canada, Japan, and Europe; from pertinent government offices, from MIT, and from Carnegie-Mellon University. Most of the MIT participants and several of the industry and government participants attended all the workshops. We limited attendance to twenty people at each workshop and did not ask for prepared presentations. Instead we asked participants to do three things:

1. Describe their most severe challenges in terms of systemic issues;
2. Describe the characteristics of a more secure environment for IT and the OT linked to it; and
3. Identify the technical, political, and economic impediments to achieving those characteristics.

Each workshop took on a dynamic of its own. We asked questions but did not limit the topics of discussion. Not surprisingly, some industry participants had difficulty framing questions in strategic terms, while some academic participants had difficulty framing theoretical questions that were relevant to the concerns of the industry participants. Yet each workshop produced spontaneous, lively discussions that served to frame and sharpen issues. Although we asked participants to address the three questions just stated, the output of each workshop fell into a simpler dyad: a consensus list of the greatest risks to the sector, and a consensus list of most important challenges for the sector. Except for certain regulatory issues, every major challenge was discussed in every workshop. If a challenge appears in the account of one workshop but not another, that is because it received the most emphasis in that workshop.

To create a research agenda, we convened a fifth workshop of twenty participants selected from the previous workshops and presented them with a distillation of ideas from the previous sessions. We asked them to identify the most critical challenges across all sectors and to turn those challenges into questions amenable to research. The outcome of that workshop formed the basis of the IRPI-CIS statement of the seven high-level challenges and the related recommendations and research questions in this report.

The Sector-Specific Workshops

1. Electricity Sector Workshop

Electricity sits at the base of any modern society's operational structure. Nearly all economic and social activity depends on it. Not surprisingly, the risk most feared in this workshop, even more than loss of information, was disruption of service.

The electricity sector operates in a unique and complex regulatory environment and displays striking internal differences, especially between the larger firms and the smaller enterprises and cooperatives. Electricity transmission in the United States[30] is governed by federal law, but delivery is regulated by the fifty states and the territories in inconsistent ways. As a general matter, regulated entities are entitled to a specified rate of return on expenditures allowed into their rate base, as determined by their regulator. They therefore have an incentive to make expenditures allowable into that base. According to our industry participants, state regulation has historically been consistent in its emphasis on rate regulation, which is a politically sensitive topic, and on safety. Expenditures calculated to lower rates (such as software designed to create efficiencies) or to improve safety are favored, they said. In contrast, network security has not been a regulatory focus, and some participants asserted that capital expenditures necessary to defend digital systems are more difficult candidates for regulatory approval. Because of the asserted difficulty of assigning a return on investments in network security, such expenditures were also more difficult candidates for corporate approval, according to these participants. These statements should be verified because, if true, these factors, together with the long lifespan of much of the sector's OT, would impede the adoption of needed security measures.

The Most Severe Risks

Risk 1: Risk from aging operating systems retrofitted with digital controls.

Most participants believed the most important risk factor for their sector was the networking of aging valves, pumps, and other hardware that were designed to be physically isolated and locked up, but which are now accessible remotely. Many of these operating components were twenty or more years old. They now form parts of systems that were retrofitted ("cobbled together") to be electronically accessible through acquisition programs that failed to take the resulting vulnerabilities into account. A participant compared the state of the industry to the Office of Personnel Management, which had digitized old systems without understanding the vulnerabilities thus created.

[30] The U.S. electric grid is better described as being part of the North American electric grid. There are many dependencies at the grid level between the U.S. and Canada.

Participants also stated that no one fully understood the extent to which the electricity industry is tightly coupled with other sectors, and therefore did not sufficiently understand the risk of catastrophic, macroeconomic failure. There was support for the view that the Department of Energy should be more concerned about disruptions lasting longer than two to three weeks.

Risk 2: Risk from third-party access.

One participant identified his company's chief risk as unauthorized external access to networks and systems owing to the extension of access privileges to third parties, mostly vendors and other contractors. All agreed this was a significant risk factor. Some doubted whether meaningful network perimeters still exist. In some cases, companies required dual-factor identification and the use of a VPN to engage in remote maintenance, but if the threat arose in a trusted vendor's system, as some thought likely, those steps did not help.

Data centers and the increasingly ubiquitous Internet of Things ("IoT") also created third-party risk. The IoT created an attack surface that was huge and expanding dramatically, and many of the connected devices related to energy consumption and had little or no security designed into them. If attacked, these devices could cause localized failure and be used to steal customer information. They could also be organized into botnets to attack any sector of the economy. That observation has since been borne out.[31]

Risk 3: Risk Created by Regulatory Emphasis on Compliance versus Security.

Participants stated there was a confusion among many executives and regulators about the difference between compliance with published standards and adequate security. That confusion is not restricted to this sector. In contrast, no such confusion exists among security professionals, who understand that compliance certifications are a necessary condition of doing business but insufficient because they do not adequately address constantly changing risks. Some participants also stated that the basic compliance standard issued by the North American Electric Reliability Corporation, known as the "NERC CIP," compared unfavorably to standards issued by the Payment Card Industry. Compliance is check-list oriented and gives a false impression of security. Participants also emphasized cultural factors, noting that the oil-and-gas sector's concerted emphasis on physical safety may be a model for an emphasis on security.

[31] David E. Sanger and Nicole Perlroth, "A New Era of Internet Attacks Powered by Everyday Devices ," *New York Times*, October 22, 2016, at http://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html?_r=0, accessed October 25, 2016.

The Challenges

The electricity workshop identified high-level security objectives supported, in most cases, by more detailed objectives necessary to achieve them. Most of the identified challenges were economic, commercial, and legal rather than technical. In nearly all cases, however, meeting the objectives would require a substantial effort simply to gather the data necessary for high-quality analytics. Obtaining the necessary data in ways that did not create additional risk for the data provider would itself be a significant challenge.

Challenge 1: Quantifying risk at the enterprise, sectoral, and macroeconomic levels.

There was general agreement that quantifying risk was both difficult and necessary. As one participant stated, a dollar spent on "vegetation management" (trimming trees) was more valuable to his company's board than a dollar spent on cybersecurity, because its effect could be measured, whereas network risk could not. Participants also stated that baselining risk – that is, describing the current state of a network – was difficult but necessary to quantify risk. One participant stated that many utilities do not even own their own data, which would be required for risk analysis, intelligence gathering,32 and prediction.

Challenge 2: Measuring and reducing intra-sector and cross-sector fragilities through simulation-based, cross-sector exercises.

These fragilities were insufficiently understood. There are about 3000 utilities in the United States, but seven utility holding companies serve about 70% of U.S. customers.33 The level of operating and security sophistication in the market was not uniform. More attention should be paid to IT/OT inter-connection risk across this disparate market and to coordinating defenses. There was general agreement that the electricity sector lagged the financial sector in this regard, and that sectors were tightly coupled. Participants did not believe the country could detect a series of rolling, low-level events that could precipitate a crisis. Participants broke this challenge into three parts:

a. **Compile the data required for quality simulations**. Exercises between the electric and the financial sectors could yield major security gains, participants believed. Various exercises coordinated by the Treasury Department and the Financial

[32] The U.S. Department of Energy (DoE) has spearheaded an effort called the Cybersecurity Risk Information Sharing Program, or CRISP, to share classified as well as unclassified information in this sector. See letter of Patricia Hoffman, Assistant Secretary, DoE Office of Electricity Delivery and Energy Reliability to Tom Fanning and Fred Gorbet, August 5, 2014, at http://www.nerc.com/pa/CI/Resources/Documents/Department%20of%20Energy%20Letter%20-%20Cybersecurity%20Risk%20Information%20Sharing%20Program%20(CRISP).pdf, accessed January 6, 2017.

[33] Information courtesy of the Edison Electric Institute.

Services Sector Coordinating Council were a good model.[34] But simulations require large quantities of good data, which firms have been reluctant to share. Utilities measure success based on reliability, safety, low costs, and consumer satisfaction. What data would induce companies to add network security to this list?[35]

b. **Secure the participation of state, local, and federal governments in cross-sector simulation exercises.** A series of disaster exercises called Gridex now exists, but it is limited to public-sector stakeholders. In the next scheduled exercises, planned for the autumn of 2017, "participation is open only to registered utilities and others specifically invited by the utility (e.g., vendors, local law enforcement)."[36] Additional exercises should broaden participation in the public and private sectors.

c. **In a collaboration between MIT and industry, develop realistic scenarios for simulation exercises.**

Challenge 3: Creating a model for a rational regulatory scheme that would align investment and security requirements with risk.

Many participants stated that prevailing regulatory regimes create intense pressure to adopt software technology without any pressure to secure it. The following specific steps toward creating a better model were proposed:

a. Perform a comparative analysis of state regulation of electric utilities in Massachusetts, Rhode Island, and New York. An industry participant with experience in these jurisdictions stated that studying their differences would be enlightening.

b. Compare data integrity measures in the electric and financial sectors. The financial sector was said to be intensely concerned with data integrity and was more advanced than this sector in securing it.

[34] See, e.g., Sean Waterman, "Bank regulators briefed on Treasury-led cyber drill," *FedScoop*, July 20, 2016, at http://fedscoop.com/us-treasury-cybersecurity-drill-july-2016, accessed November 8, 2016; U.S. Department of Treasury, "Joint Statement from the U.S. Department of The Treasury and Her Majesty's Treasury," November 12, 2015, at https://www.treasury.gov/press-center/press-releases/Pages/jl0262.aspx, accessed November 8, 2016.

[35] A participant noted that the automobile industry had created massive cyber vulnerabilities in vehicles, but that the industry is fixing them now because the potential liabilities could be very large. Regulated utilities were said not to face a comparable risk.

[36] NERC, "GRIDEX IV Frequently Asked Questions," p. 1, December 2, 2016, available at http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx, accessed January 5, 2017.

c. **Study nuclear regulation as a potential model for the regulation of non-nuclear electricity.** A participant stated that the nuclear industry went from a prescriptive to a performance-based regulatory regime, recognizing that technologies were advancing more quickly than regulation could keep up.

d. **Optimize legal, regulatory, and tax, policy for security investment to maximize investment incentives and place costs where they can be reflected in the price of the goods and services produced.** Existing regulatory schemes and tax policy did not do this, according to participants. There was broad but not unanimous support for the view that liability should play a greater role in driving better network security, and that now it plays almost none.

Challenge 4: Supporting a market for simpler, less vulnerable technology.

The widespread use of field-programmable gate arrays[37] and multi-purpose controls were cases in point. Both were cheaper to produce than special-purpose devices and were highly capable – but were therefore more vulnerable. Creating a market for limited-purpose devices was seen as more of a political and economic challenge than a technical one. In this regard, some participants wanted to explore the use of analog devices within, or alongside digital systems, especially at end points.

Challenge 5: Improving human expertise in network management.

a. **Identify the skill sets uniquely required in this sector and expand the talent pool.** There are not enough qualified operating engineers and computer scientists who understand the challenges unique to the electricity sector.

b. **Investigate the "Rickover Model" for the training and selection of navy personnel for the nuclear submarine service.** When the U.S. Navy created a nuclear submarine service, Admiral Hyman Rickover required applicants to complete a rigorous training regimen for admission to the service. Could that model be adapted for security professionals in this or other sectors?

[37] "A field-programmable gate array (FPGA) is an integrated circuit designed to be configured by a customer or a designer after manufacturing …. FPGAs contain an array of programmable logic blocks, and a hierarchy of reconfigurable interconnects that allow the blocks to be "wired together", like many logic gates that can be inter-wired in different configurations." "Field-programmable Gate Arrays," Wikipedia, at https://en.wikipedia.org/wiki/Field-programmable_gate_array, accessed December 12, 2016.

Challenge 6: Integrating the Management of IT and OT.

Each utility is different in the way it integrates, or fails to integrate, the management of operating technology (OT) and information technology (IT). Some do not converge until the corporate level; others converge much lower down. No one believed a single governance model would be useful, but the group did believe that IT and OT have substantially converged – at any rate, they have converged sufficiently so that operating systems can now be attacked through IT systems. Management structures should reflect that fact.

a. **Unify security functions.** In the view of many participants, someone in the enterprise should have a view of the full scope of security threat, from wherever they came. The group did not agree on that person's proper title and reporting responsibilities, but did agree that he or she should report to an officer of the company and possibly to the board.

b. **Optimize OT/IT replacement cycles, which are out of synch.** OT in this sector has historically been on replacement cycles of 15-25 years. In contrast, IT measures technology generations in 3-5 years. These cycles should be studied and optimized.

2. Financial Sector Workshop

The finance workshop identified three risks that were unique or especially severe in the sector:

1. Data integrity risk;
2. Systemic risk to the financial system that may not be apparent when considering enterprises or the sector in isolation; and
3. Third-party risk arising from the inability to alter long-term contractual arrangements with other market participants.

The financial sector also shares risks common to critical infrastructure, though it has the most advanced network defenses of any sector.

The Most Severe Risks

Risk 1: Data Integrity.

Risk to the integrity of financial data topped the list of our participants' concerns. Our economy is based on a system of accounts recording who owes what to whom at any moment. Those accounts are digitized, and so are back-up systems. An attack that destroyed or corrupted the accounts of a major financial institution could wreak devastating economic havoc unless those accounts could be quickly and reliably reconstituted. The risk extends beyond banks to securities exchanges, brokerage firms, investment companies, clearing organizations, and other financial enterprises.

A sophisticated network attack could lock-up this sector. A logic bomb, for example, could randomly delete system files. According to one participant, that has already occurred, and it took time to understand what had happened and to fix it. But disruption is only one risk that could arise form from data loss or corruption. A subtle, more limited operation that corrupted the pricing of selected securities, for example, could be used to manipulate markets, create illegal profits and losses, and drive parties out of business.

Participants agreed that a slowly rolling attack on an institution might create more havoc than an attack that brought the institution to an immediate halt, for which the larger institutions prepare. A "low and slow" corruption of accounts would be difficult to spot, and unless it were stopped quickly, it would infect back-up systems, too. The longer it lasted, the more backup accounts would also be infected. Research that addressed this risk would be of great value.

Risk 2: Systemic Risk from Tight Coupling Within and Across Sectors.

Participants were concerned about the cross-sector risk created by the tight coupling of finance, energy, and telecommunications, but they were also concerned about risk from tight coupling within their sector. Several participants agreed that financial enterprises assume that in this space all parties are managing their own risks and that systemic risk is therefore also being managed through the sector, but they doubted this is true. Notwithstanding the perception that the level of cooperation in this sector is high, these participants believed it was insufficient and that more collective action on information sharing would be required to better protect the sector from attack. The nuclear power industry was cited as an example. In that sector there was widespread understanding that an adverse incident that affected any of them would adversely affect them all. The financial sector was said not to be at that point.

In particular, several participants complained of poor network security among competing institutions ("shirking"). They gave two examples: (1) competitors that sought market advantage by saving money on network security, and (2) community banks that lacked the financial and other resources to make themselves reasonably secure. As to the latter, participants noted that the share of assets controlled by community banks continues to fall, so some questioned the significance of this risk. Others noted that imposing further regulation on these banks would accelerate consolidation in the banking sector. However, that risk was not equally troubling to everyone present. A participant noted that shirking was merely one aspect of the more general problem of consistent standards. As institutions other than banks and SEC-regulated businesses became larger players, the problem of inconsistent regulation would present a growing problem. Several participants stressed that one should pay close attention to the application of regulatory standards as well as to their content when assessing consistency.

Risk 3: Contractual Risk from Long-Term Third-Party Contracts.

Long-term contracts with other institutions (which some participants called "locked handshakes") were a special example of risky intra-sector coupling. The example given involved payment processors, which allegedly employ hard, pre-set passwords that are not regularly rotated, if rotated at all. That kind of arrangement was said to lock in network access rights of third-parties with allegedly poor security. These contracts were said to allocate risk in ways that participants believed were unfair and that were not foreseen when the contracts were made. These contracts can have terms of twenty years, and many were made before the sector fully came to grips with network risk. These assertions should be tested empirically. However, industry participants believed this risk was real, that the sector needed a means to force the renegotiation of these contracts, and that quantifying the problem would be helpful. We detected a willingness among several industry participants to favor a regulatory solution to this issue, and one of them specifically suggested that the issue could be of interest to the Federal Trade Commission (which has recently used Section 5 of the FTC Act[38] to address unfair as well as misleading practices affecting network security). Another suggested that clearing agencies might be able to provide leverage for achieving higher security levels. In evaluating these contentions, attention must be paid to the competitive interests involved as well as to the alleged security risks.

Risk 4: Difficulty of Identifying Malicious Actors.

The difficulty of attributing behavior to malicious actors is an aspect of the identity management problem common to every sector, but our participants stressed the challenge of ascertaining internal as opposed to external identities. And they were concerned with controlling administrative privileges because most hacks they dealt with involved abuse of administrator access. Some participants said that machines also have identities and privileges, and that managing identities was easier for people than for machines. Several participants stated, without dissent, that "operator risk" – that is, insider threat from malicious or simply negligent behavior – was a medium, not a low, probability. Some participants agreed that the government's unsuccessful efforts regarding trusted identities illustrated the difficulty of accomplishing anything comprehensive in this space.

The Challenges

Challenge 1: Enhancing the integrity of backup systems.

A slowly evolving attack could be a bigger threat to financial institutions than an attack aimed at a sudden network collapse because it would not be discovered as quickly – and possibly not until backup systems had been infected. Participants were particularly interested in the possible applicability of blockchain technology to their systems and the status of blockchain research to the latency problem (that is, the time required to complete a communication or transaction). Some participant firms are investing in blockchain research.

[38] 15 U.S.C. §§ 41-58, as amended. The Commission is a consumer protection agency, not a financial regulator. It considers three factors in determining whether a practice violates the prohibition on unfair consumer practices: (1) whether the practice injures consumers; (2) whether it violates established public policy; (3) whether it is unethical or unscrupulous." FTC, "FTC Policy Statement on Unfairness," December 17, 1980, accessed November 16, 2016.

Challenge 2: Identifying and reducing cross-sector risk through joint cross-sector exercises.

Robust joint exercises using sophisticated data would help illuminate the risk from the tight coupling of power, finance, and telecommunications. These exercises would elucidate intra-sector and cross-sector vulnerabilities and would benefit all participating sectors. They would also highlight sectoral differences about the priorities given to availability, integrity, confidentiality – another area for potential research.

Challenge 3: Improving identity management consistent with privacy concerns.

a. Among Communicants

The tension between privacy and identity management among communicants concerned many participants, but there was widespread agreement that it is important to focus on the specific information fields that would be most useful, and then to determine whether and how that data can be shared consistent with EU and US law. Several participants asserted that EU law made it more difficult to identify both malware and malicious actors in their systems.

A non-industry participant stated that banks and credit card companies are not using in their own networks the kinds of data-driven identity management/risk flagging techniques they employ to monitor credit risk. It would be useful to know whether, why, and to what extent this may be true.

b. Among Providers

It is technically simple to divert large amounts of traffic when it is "handed off" from one service provider to another. This has occurred several times. These hand-offs occur at border gateways, following border gateway protocols (BGP). These protocols are weak, which is to say that identity assurance[39] is weak at the BGP level as well as at the level of individual communications. Traffic diversion could cripple communications, and although it would be quickly discovered and repaired, the delay in a crisis could be critical. A more secure version of BGP exists, called BGPSEC, but few U.S. carriers have adopted it, presumably because they do not expect a benefit from adoption that would offset its cost. What economic or other factors impede the adoption of border gateway protocols that would make it impossible, or substantially more difficult, to divert network traffic? How can those factors be reduced or eliminated? Fixing this systemic weakness would not appear to raise privacy concerns.

[39] Machines, systems, and regions of the Internet, as well as persons, have identities.

Challenge 4: Containing the "Blast Radius" of Destructive Attacks.

It is now widely understood that malware cannot reliably be kept out of even very sophisticated and well-run systems. The challenge was therefore to contain its effects – or as one participant put it, to contain its "blast radius." Participants returned several times to this topic and were deeply interested in technical means of accomplishing this objective (e.g., flexible segmentation and rapid reconstruction of networks).

Challenge 5: Modernizing the Regulatory Environment

Regulatory challenges fell into two groups: (i) creating flexible standards that would improve security as well as guide compliance (a goal that may be as elusive in theory as it has been in practice), and (ii) harmonizing regulations nationally and internationally.

a. Flexible Standards

Industry participants stated that regulatory norms are not adapting to rapidly changing technology and are rigid and costly without being effective. They noted several instances where firms were compliant with applicable standards but were penetrated anyway. They were interested in seeing flexible standards that would evolve with technology and reduce risk when implemented – like a standard of care. Participants referred to standards issued by the National Institute of Standards and Technology (NIST) and the International Standards Organisation.[40] These could evolve into enforceable standards of care, but legally binding standards of care usually evolve through litigation; regulations are promulgated.

A non-industry participant stated that compliance and risk-based standards are not necessarily in conflict, and that expecting government or a standards organization to compel virtue was not realistic. He added that mandating red-teaming forces threat-modeling. More broadly, he asked what success would look like under a risk-based approach and suggested this could be a fruitful research question. In this regard, participants would be interested to know whether sectoral stress tests could be developed.

[40] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," v. 1.0, February 12, 2014, at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, accessed January 7, 2017; ISO/IEC 27032: 2012 Information Technology – Security Techniques – Guidelines for Cybersecurity, July 2012, at http://www.iso27001security.com/html/27032.html, accessed January 7, 2017.

b. Harmonization

The Securities and Exchange Commission, the Commodities Futures Trading Corporation, the Federal Financial Institutions Examination Council (among others) regulate the financial sector in the U.S. Standards issued by the National Institute of Standards and Technology (NIST) and the International Standards Organisation also apply. These regulations and standards should be consistent and should evolve rapidly. While there was broad agreement on this point, specific inconsistencies were not discussed except to note that ISO 17799 was in effect for about ten years before it was superseded.

We heard conflicting views from industry on the issue of global harmonization. Some said that standards of the Federal Financial Institutions Examination Council are already fairly global and that global convergence would have to occur; others stated that the convergence of physical and logical security is making global regulatory convergence ever more difficult. Regulatory differences between Europe and the United States over the security of cloud computing remained a problem. This was particularly troubling because as the number of sensors expands dramatically through the IoT, the information they generate can be managed only through cloud services based on big data analytics and machine learning. Could research on the security of encryption in cloud computing be useful in achieving international harmonization? Again, securing the data required to do this research would be a challenge.

Challenge 6: Re-establishing trust in U.S. global leadership.

Since the Snowden disclosures the United States is no longer the most trusted actor in network space, even among its allies. There is no trusted “sentry on the Roman road.” Regaining international trust, especially among the Western democracies and Japan, was a strategic challenge of high importance to the financial sector.

Challenge 7: Assessing Portfolio Risk from Information Insecurity.

This was a topic of widespread interest but not extended discussion. Whether it could be accomplished without aggregating the risks created by weaknesses in the systems of each company in a portfolio would be an interesting research question. Most participants believed cyber risk was not factored into the pricing of securities.

Challenge 8: Identifying unauthorized executable code.

The architecture of the Internet – and the architecture of the hardware and software that run on the Internet – permit executable code to reside among data files. Indeed, embedding executable code within data files is a feature of some widely used systems, making those systems harder to secure. Unauthorized or malicious code does not identify itself as executable; it masquerades as a data file. In a typically large data file, this kind of malicious insertion is therefore extremely difficult to find and eliminate. Can this weakness be eliminated or made less severe?

Challenge 9: Enhancing workforce development.

Technical education and talent management were problems. Filling the pipeline with highly educated, trained network engineers and computer scientists was the challenge. Education and training should begin early in life.

Challenge 10: Creating effective cyber deterrence.

Is deterrence working? Against whom? Participants had differing views. Some thought it was playing no role in bringing stability to networks because highly sophisticated nation-state actors were operating in our networks. Others noted that nation-states could wreak havoc with one another but had not done it, which suggested that nation-states were indeed being deterred from escalating exploitation to destruction attacks. However, there was broad agreement that fringe states such as North Korea, Iran, and Syria might not be similarly deterred and that containing their attacks would be a challenge going forward.

Challenge 11: Designing systems that do not fail silently.

A non-industry participant stated that one of our most important and difficult challenges was to make “silent failure” impossible. He meant that when a system failed, its operators should know immediately that it had failed. They should also be able to determine why it had failed. To do that, we had to learn how to interrogate algorithms. Absent the ability to do so, algorithms would become increasingly autonomous and beyond human control. He suggested that critical sectors would probably differ on how far autonomy should go, and that research on that point would be useful.

3. Communications Sector Workshop

This workshop was unique in focusing on the risks of managing networks that are too complex to be understood and whose states cannot be known from one moment to the next. Here again this risk not unique to this sector, but it was articulated only in this workshop. The risk feared most in this sector, even more than data security, was catastrophic failure. Many conditions created risk, but two conditions created the most concern: (1) systems too complex to understand, and (2) loss of perimeter control.

The Most Severe Risks

Risk 1: Risk from indeterminate network state.

Over the years, communication hardware has grown massive and software even more so. Once systems attained sufficient size – wherever that threshold might be, the industry had crossed it – participants agreed that systems were inherently unstable and it was difficult to know much about them. That was unnerving. Communications systems were so complex that neither the firms that owned them nor their vendors fully understood them. There was agreement, however, that software-defined networks (SDNs) offered advantages in managing complex networks. Yet there were differences expressed as to the nature of SDNs. One participant stated that they enabled decentralized control and were therefore more resilient even if many nodes were taken out. Another stated that SDNs pulled the network control algorithms out of the routers and into a controller that was conceptually *centralized*. But it was agreed that, through application programing interfaces, SDNs offered significant cost savings and could be reconfigured or rebuilt swiftly even while under attack. No one doubted they would become prevalent in this sector, but there was disagreement about whether SDNs were reducing complexity.

Risk 2: Risk from third-party access and porous network perimeters.

In common with other sectors, industry participants saw widespread third-party access with consequent loss of perimeter control as a major risk. The communication sector is experiencing a major perimeter expansion through cloud computing, network function virtualization, vendor access, and the IoT. The very notion of a perimeter was in question. More physical devices on the network made the stakes much higher. Some industry participants said they were engaged in constant electronic warfare in the military sense.

Interoperability with legacy systems, both internal and external, was part of the problem. Internally, there would always be some subsystems that were more secure than others. Externally, some legacy systems were the equivalent of bad neighborhoods that packets had to traverse.

The Challenges

Challenge 1: Communications networks should be harder to disable.

a. **Failure in any part of the network should be evident.** Failures were inevitable and should be planned for. But no failure should be silent to the operator. One participant referred to the "Chaos Monkey" approach to testing (in which various elements of the system are turned off to see what happens), and said that the way to know if something would fail silently is to make it fail. An industry participant stated that in the public health arena, the reporting of certain diseases was mandatory, and that this sector should adopt a similar policy.

b. **Legacy systems should be retired on accelerated schedules.** Tax incentives, regulatory measures, and better internal risk-assessment could all be helpful in achieving this goal.

c. **Software defined networks (SDNs) should be simpler as well as prevalent.** Participants anticipated that network management and control would become highly distributed as a mean of increasing resiliency and that systems would increasingly manage themselves. They also posed three questions relating to network management. First, they asked whether blockchain technology could help manage international networks by keeping a record of all changes to a network, including the changes that the network made to itself? Second, they asked whether SDNs had the potential to improve the confidentiality of communications – or make them worse. Third, they asked how SDNs could aid in segmenting networks in real time to isolate the effects of a malicious intrusion.

d. **Some critical facilities should be isolated from publicly accessible networks.** Isolation was a relative concept. Total isolation was not possible, as the Stuxnet attacks on Iranian centrifuges demonstrated. With that understanding, participants agreed that a small but undefined number of critical facilities should not be "public facing" but should operate on virtual private networks (VPNs), with air gaps and significant access barriers.

e. **The technological monoculture should be more diverse, and its components should be designed with security in mind.** Participants saw technological diversity as a desirable goal but did not envision a path to get there. They also noted that diversity would require a standards-based architecture to support it. Some were interested in the possible use of analog technology at some points to contain system failure. However, all participants believed that the costs and benefits of innovation should be assessed with security in mind, which is not now the case. It was shocking that we still have injection attacks, for example. Many participants believed that a more robust liability or regulatory regime would be required to make vendors design for security, but there was no consensus on whether tort liability would be welcomed, though it was probably more desirable than most regulatory approaches.

Challenge 2: Regulations and standards should be evidence-based and flexible.

Industry participants severely criticized the current regulatory regime in their sector. Compliance with current standards did not lead to better security and was said to be “a joke” and “a race to the bottom.” There were frequent fines for low level violations, and these fines were taken from security budgets. The net effect was a reduction in security spending. Industry participants wished instead that regulators took steps to ensure that security budgets were increased.

Several participants believed that regulators in the banking sector did a better job of devising and enforcing reasonable standards. In any case, all industry participants believed that (1) communications regulations should be dynamic and evidence-based, (2) regulation should incentivize discovery of vulnerabilities and penetrations, rather than the reverse, and (3) disclosure to the regulator should not be penalized (as in the Aviation Safety Reporting System). There was also support for loosened rules in emergencies based on prioritized threats. A participant suggested that universities could play an important role in designing a better regulatory scheme by bringing economic and legal expertise to bear on the challenge.

Like the electricity sector, the communications sector supports all the others. Historically the various sectors have been regulated by different agencies that focused on different issues. But now these agencies have begun to create cybersecurity regimes, which are not consistent. Harmonization would be useful. One participant stated there were simply too many regulatory and compliance standards and that the federal government should recognize only the NIST standards.

Challenge 3: Continuity-of-operation planning should be widespread and robust for critical infrastructure and critical resource sectors.

Participants said that in every national level tabletop exercise, the participants assumed that communications would be available. This assumption was unrealistic and should be abandoned. Participants wanted to see systematic use of sophisticated modeling and simulations to anticipate and train for attacks. This prescription was common to all workshops, and so was an acknowledgement of the impediment: i.e., the lack of sufficient data to perform robust simulations and to create good models. Some participants proposed that MIT play a role in generating models, but the need for data remained.

Apropos of data sharing, Industry participants were clear that privacy concerns must be carefully balanced against security concerns. They also stated that privacy concerns impeded necessary information sharing – though most admitted that competitive concerns were an even bigger impediment to sharing.

Challenge 4: The government should confront the need for communication priorities in case of national emergency.

Industry participants said they were having difficulty engaging government about prioritizing critical systems. If communications were crippled in a disaster, it would be essential to determine what sectors and firms would get priority service, but government was said to be reluctant to make that determination. In a national emergency, prioritization (also known as tiering) was thought to be inevitable. It would make sense, for example, to give priority to a nuclear power plant or hospital over personal calls, but participants from telecommunications firms said they had no guidance on how to prioritize calls and, as common carriers, were required to treat all calls alike.

This challenge is not unique to this sector. For example, in a national emergency, power might have to be rationed, but it is unclear that anyone has the authority to require it (as opposed to the authority to “coordinate” with distributors). But the issue arose only in this workshop. Cross-sector simulation exercises could illuminate the consequences of this lack of authority.

Challenge 5: The nation should develop a national deterrence strategy.

Deterrence involves both making targets harder to cripple and exacting a price from an attacker. Here the emphasis was on the latter. Participants were troubled that attackers faced little likelihood of paying a price for attacking U.S. targets, that the country had no discernible strategy for punishing attackers, and that the lack of consequences was emboldening adversaries. They noted the successful cyber theft of massive amounts of intellectual property but were even more concerned with the prospect of destructive attacks such as those on Saudi Aramco in 2012 and on Sony in 2014. They predicted that such attacks would increase in the next two years. Playing defense, they said, is not a sufficient strategy.

Challenge 6: The domain name system should be strengthened.

The domain name system, commonly referred to as the DNS, correlates plain-language names for computers, websites, etc. with a numerical IP address. Thus, typing "www.mit.csail.edu" in a browser takes you to 128.30.2.155. The DNS is weak and insecure, which makes spoofing identities easy. There is wide agreement that adopting a secure version of the DNS known as DNSSEC would bring a significant improvement in the security of the Internet. Enterprises should be incentivized to move to the more secure system.

Challenge 7: The cadre of highly qualified network engineers and computer scientists with security expertise should be greatly expanded.

The need in this regard was urgent but could not be met in the short term. The need was felt as strongly in the regulatory agencies as in industry.

4. Oil-and-Natural-Gas Sector Workshop

Like all sectors, the oil-and-natural-gas ("ONG") industry faced the full array of cybersecurity challenges, but it was chiefly concerned with risk to availability of service. This risk arose chiefly from three conditions:

1. Unduly complex, general purpose technology;
2. The inability to swiftly detect malware; and
3. The uncertain ability to swiftly isolate the impact of compromise.

The ONG sector resembles the electricity sector because of their common reliance on industrial operating technology, and both share cross-cutting network risks. At the generation/extraction level, however, this sector enjoys a higher level of threat-information sharing among the majors, and it absorbs new technology more quickly.

The Most Severe Risks

Risk 1: Operational risk created by unduly complex, general purpose technology.

Industry participants singled out insecure, general purpose controls as a supply-chain risk to their operations. The components available from vendors had far more functionality than they needed or asked for, and with superfluous functionality came vulnerabilities. These participants wanted lean components with no more functionality than needed for a particular type of task, but such components were not available in the market. Vendors found it far more profitable to sell generic devices to a wide market.

Risk 2: Operational risk from the inability to swiftly detect malware.

Disguised executable code is easy to insert into a network and exceedingly difficult to find. The risk of malicious executable code is enhanced by supply chain risk but is separate from it. Some participants stated that their inability to detect malware faster was also caused by their inability (i) to visualize their entire network at once and (ii) to know what hardware and software were running on their network.

Risk 3: Operational risk from the inability to swiftly contain the impact of compromise.

Participants assumed that all malware could not be kept out of their systems. They focused on the risk from the inability to compartment the malware's impact. As in the financial sector workshop, the image of containing the "blast radius" of the malware was appealing. The question was how to quickly seal off a compromised area of a network.

The Challenges

Virtually every challenge addressed in the previous workshops was addressed in this workshop too, but the following challenges received the most attention:

Challenge 1: Creating a security environment on the model of this sector's successful campaign to improve its safety environment.

ONG firms have been successful in fostering safety consciousness across the industry and thereby driving down the number and severity of physical accidents. Participants did not believe the industry had made the same commitment to network security. They noted that cybersecurity and physical security and safety had largely converged. Operations were controlled by digital networks. Network intrusions could be used, and indeed have been used, to sabotage operations and thus threaten health and safety. In most companies, however, electronic networks and physical operations were not managed holistically, and several participants stated that the engineering culture they confronted did not understand network security. They saw this as both a management problem and a problem of company culture – not a technological problem.

Challenge 2: Creating a government-industry partnership to foster a supply chain that produces simpler, less vulnerable components, especially industrial operating controls.

General purpose components came with superfluous functionality, and every functionality created potential vulnerabilities. But general purpose components were cheap and profitable. One participant stated that vendors charge maintenance fees, so they benefit from the insecurities they create because they get paid to fix them. This is a commercial, not a technological, problem, and participants saw no solution to it unless the government would support demand for special purpose components for critical sectors by becoming a more demanding buyer. Several participants thought that the departments of defense, energy, and homeland security could play that role. Participants also discussed the potential use of analog devices at key points in their networks but generally believed it would be impossible. Doing so, they said, would mean losing real-time remote monitoring capability. The digital "toothpaste was out of the tube," one participant said. The question remained, however, whether analog devices could serve as fail-safe mechanisms working in parallel with digital systems.[41]

[41] For example, at a conference at MIT's Sloan School of Management in the autumn of 2016, an executive of a major U.S. energy company stated that his company used analog pressure gauges in pipelines that would override a malfunctioning digital pressure system and shut down the line.

Challenge 3: Automatically identifying unauthorized executables.

The challenge of swiftly identifying malware resolved itself into the challenge of automatically identifying unauthorized executable code. This was an aspect of participants' demand for adaptive systems and cyber capabilities at scale, which they believed would be possible only through machine learning and artificial intelligence. Capabilities at scale, machine learning, and artificial intelligence would in turn be available only through cloud services, which must be secure.

Challenge 4: Automatically neutralizing or containing the effects of system failure.

Containing cascading failure would require adaptive systems. Immediate visibility of failure was a prerequisite of containing its effects. Participants also believed that following a failure, systems had to be able to explain what went wrong, even if they had not previously confronted the same circumstances. To do these things, systems had to be capable of machine learning. "Patching on the fly," "dynamic segmentation," and "self-repair" were phrases often heard. These aspirational capabilities could be realized only through big data analytics, which would likely be available only through secure cloud services.

Participants also believed that containing cascading failure would require limiting common mode attacks at scale. Systems were too homogeneous within and across sectors. An attack on one system could therefore be repeated successfully against many other systems. They therefore saw heterogeneity as a goal.

Challenge 5: Encouraging an enforceable standard of care.

Many participants, including several industry participants, favored a legal standard of care for software and equipment and possibly for certain operational activities such as patching. They wanted enforceable standards, much as building codes are enforceable. They also referred to the function of the Underwriters Laboratory in raising standards for electrical appliances. Manufacturers followed these codes because they could be legally liable if they did not and because their insurance carriers required them to do so. At the same time, no industry participant favored mandating statutory or regulatory standards. There was some support, however, for peer reviews of the kind used in the nuclear industry.

Several participants stated that standards of any kind required a standard vocabulary. For example, some participants refer to OT as "everything south of the firewall." Others define OT as anything that produces a physical output. "Failure," "compromise," and "security" also required standard definitions.

Challenge 6: Accelerating and automating patch management.

Participants identified three different challenges relating to patching: (i) prioritizing patches, which in turn implied (ii) measuring the relative risk of unpatched vulnerabilities; and (iii) accelerating the patching process without adding new operational risk. Currently, patching sometimes takes up to four months, which is far too long.

Challenge 7: Assuring memory safety.

One participant stated that computer scientists spend too much time addressing individual vulnerabilities and not enough time addressing classes of vulnerabilities. Memory safety (specifically, eliminating buffer overflow) was a case in point. Another participant stated that this is not basically a technological problem; we know how to fix this. Why does this class of vulnerabilities persist?

Challenge 8: Developing a rational, risk-based model for investment and compliance.

Participants believed that quantifying risk would help rationalize compliance regimes as well as investment decisions. The challenge is broader than simply quantifying aggregate system risk, however, because rational investment involves more than a determination of how much money to spend; it also requires a determination of how to spend it. Several participants believed that insurance carriers could provide more useful requirements than government-mandated standards. Others said that economics departments should consider focusing on security economics as a field of study.

Several industry participants called for more robust threat intelligence. One noted that Congress had resisted funding for prediction markets, which could be useful, and that MIT could play a helpful role in creating or encouraging those markets.

Many of the firms represented in the workshop were not cutting cybersecurity spending, even as other IT spending is decreasing with the low price of oil. The vendor participants said they were seeing increased revenue from cyber products.

Challenge 9: Increasing support for simulation-based complexity modeling and capability maturity.

There was mixed support in this workshop for more information sharing. An Oil and Natural Gas Cybersecurity Network already exists, and some participants were reluctant to expand this trusted network. One participant’s company was already a member of twelve information-sharing networks; that was enough. However, there was no dissent from a proposal for more sophisticated crisis simulations, which require massive amounts of high-quality data from the participants. Several participants suggested that MIT could play a useful role in co-sponsoring simulation exercises and might be a trusted repository for the required data.

March 2017

Joel Brenner was the principal author of this report, with the support and assistance of IPRI's Daniel Weitzner, Dr. David C. Clark, Professor Hal Abelson, Dr. Shirley Hung, Dr. Taylor Reynolds, Melanie Robinson and Adam Conner-Simons (CSAIL) and CIS Professor Kenneth Oye, CIS Director Professor Richard J. Samuels, CIS Executive Director Dr. John Tirman, Michelle Nhuch and Dan Pomeroy. The rapporteurs for the workshops were Reid Pauly and Rachel Tecott.

THE INTERNET POLICY RESEARCH INITIATIVE:

In 2014, MIT established the Internet Policy Research Initiative (IPRI). The Initiative brings together resources from many departments and centers within MIT. Its mission is to work with policy makers and technologists to increase the trustworthiness and effectiveness of interconnected digital systems. Its tools are engineering and public policy research, education, and engagement. IPRI is headquartered in MIT's The Computer Science and Artificial Intelligence Laboratory, which is the largest research laboratory at MIT and one of the world's most important centers of information technology research.

MIT Center for International Studies

The Center for International Studies (CIS) supports international research and education at MIT. It is the home of MIT's Security Studies Program; the MIT International Science & Technology Initiative, its pioneering global education program; the Program on Emerging Technologies; and seminars and research on migration, South Asia politics, the Middle East, cybersecurity, nuclear weapons, and East Asia. The Center has traditionally been aligned with the social sciences while also working with MIT's premier science and engineering scholars. CIS produces research that creatively addresses global issues while helping to educate the next generation of global citizens.

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu