THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 10 NUMBER 10
AND HOMELAND SECURITY

APRIL 2012
CYBERSECURITY

Contact: dhardy1@gmu.edu
703.993.8591

Click **here** to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

This month's issue of *The CIP Report* focuses on Cybersecurity; an increasing threat to our critical infrastructure.

We begin with a look at the difference between critical information infrastructure protection and cybersecurity. The Founder, President, and CEO of a homeland security consulting firm discusses the integral part that cybersecurity now plays in our everyday lives. Then we take a look at cyber-physical critical infrastructures and how to secure them. Next, two professors discuss critical infrastructure information dependency and finally an attorney with The McCormack Firm, a Boston law firm with practice areas that include security and privacy, delves into the current and future challenges of cybersecurity.

This month's *Legal Insights* reviews cybersecurity legislation. We also highlight two upcoming conferences we are co-hosting.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Is Critical Information Infrastructure Protection and Cybersecurity One and the Same?

by Myriam Dunn Cavelty and Jennifer Giroux,
Center for Security Studies, ETH Zurich, Switzerland

It has been well over 10 years since the critical infrastructure protection (CIP) debate emerged, yet there is still little clarity with regard to a clear and stringent distinction between the two key terms "CIP" and "CIIP" (critical information infrastructure protection). In general, while the former comprises all the critical sectors of a nation's infrastructure, the latter pertains only to critical *information* infrastructure and thus oftentimes subsumed under the heading of CIP in official publications. However, in today's networked world, CII seems to be finding a much stronger distinction via the term, and indeed a growing field of, cybersecurity. This is an interesting trend that merits closer attention.[1] What does it signify? Alost, what implications does it have for protection concepts? To answer these questions, we first look more closely at the early distinctions between CIP and CIIP and then at the more recent shift of the term CIIP to cybersecurity. Drawing from government cybersecurity strategies, we show the emerging conceptualization of CIP and cybersecurity as two respective yet inter-related domains of national security.

Distinguishing the Critical 'I' from the Information 'I'

A clear distinction between CIP and CIIP is lacking in most official documents. Most of the time, CIP is used to refer to national infrastructures and sometimes exclusively to information infrastructures, or CIIP. In this respect, can one talk about CIIP without talking about CIP (or vice versa)? The answer is no, for the following reasons.

First, the interrelation of the two concepts is apparent from the current debate on protection necessities: the debate jumps from talk of defending critical physical infrastructure — telecommunications trunk lines, power grids, and gas pipelines — to protecting data and software residing on computer systems that operate these physical infrastructures. This indicates that the two cannot and should not be discussed as completely separate concepts. Rather, CIIP seems an essential *part* of CIP.

Second, and relatedly, (critical) information infrastructures are regarded as the backbone of critical infrastructures given that the uninterrupted exchange of data is essential to the operation of (physical) infrastructures and the services that they provide. Not only do they interlink various other infrastructures, but they also create new vulnerabilities, particularly in how they can be targeted. Illustrating this point, the U.S. Cyberspace Policy Review notes that "…the growing connectivity between information systems, the internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures."[2] Thus, it comes as no surprise that many so-called CIP policies have a strong focus on the protection of specific information infrastructures rather than focusing on all critical infrastructure sectors and aspects.

From CIIP to Cybersecurity

In addition to the aforementioned interrelationships, the growth and reach of information and communication infrastructure or technologies (ICT) has also led to a

(Continued on Page 3)

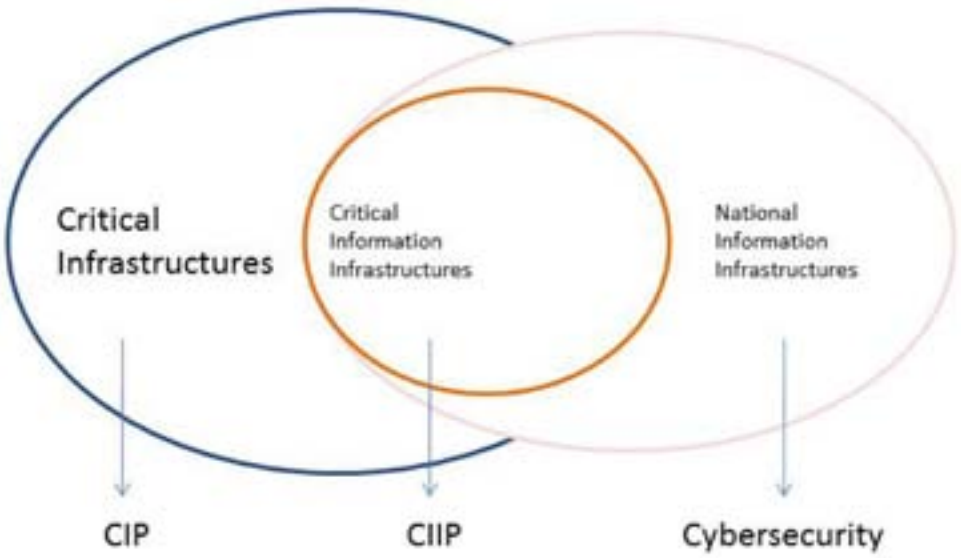
1. This observation is based on previous work conducted by the "Risk & Resilience Research Group" at the Center for Security Studies on cybersecurity, see: http://www.css.ethz.ch/policy_consultancy/topics_INT/Cyber-Security_EN. In particular, see: http://www.css.ethz.ch/policy_consultancy/topics_INT/DetailansichtPubDB_EN?rec_id=1392.
2. U.S. Government, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure," U.S. Government Printing Office, Washington DC., (2009).

CIIP *(Cont. from 2)*

considerable broadening of the discussion on CII; one where the protection of ICT and of the information which is processed by these systems is not only crucial for critical infrastructures but also absolutely essential for societal and business relations across the board. Framed this way, critical information infrastructures are not only part of the global or national information infrastructure that is essential for the continuity of critical infrastructure services, but also have other crucial components. On the one hand, there is a *physical* component, consisting of high-speed, interactive narrow-band and broadband networks; satellite, terrestrial, and wireless communications systems; and the computers, televisions, telephones, radios, and other products that people employ to access the infrastructure. On the other hand, there is an *immaterial*, sometimes very elusive component, namely the information and content that flows through the infrastructure, the knowledge that is created from this, and the services that are provided through them.

This broadening of CII has led to the development of policies tailored to the security of information infrastructures more generally — meaning not only for *critical* information infrastructures from a government perspective — that aim to secure all interactions that are enabled by and depend on them. These economic, social, and cultural interactions take place in what is labeled "cyberspace." Accordingly,

Figure 1: Concepts and their Interrelationships



the policies that aim to secure these interactions are usually called cyberspace security policies or, in short, cybersecurity policies. Figure 1 best illustrates the full articulation of this trend, whereby the cybersecurity field, which is overlapped with the CIP field, includes CII.

Since one of the first national cybersecurity strategies, "Defending America's Cyberspace," released in January 2000, cybersecurity policies have become more ubiquitous and intertwined in national security debates. In the last several years alone, countries such as Belgium, Estonia, France, Germany, India, Japan, the Netherlands, Great Britain, the United States, Sweden, and Switzerland have released new cybersecurity strategies.

Compared to CIIP policies, which are typically embedded in CIP strategies, cybersecurity policies pursue a broad view on the security of ICTs and the protection of the information that is processed by them. For example, Germany's "ICT Strategy of the German Federal Government: Digital Germany 2012," released in 2010, is a rather comprehensive document that outlines the country's ICT strategy — taking into account not only protection measures, but also highlighting the importance of ICT in contemporary social and economic activities.[3] In another case, and one more closely aligned to the CIP debate, the Estonian Cyber Security Strategy describes the formulation of a cybersecurity strategy as the first step "to protect the country's critical infrastructure and to ensure the country's information security."[4] Thus, in order to examine the key concepts and policies with regard to CIIP, it is important not only to look at national security strategies or CIP policies, but also to analyze those

(Continued on Page 17)

3. Federal Ministry of Economics and Technology, "ICT Strategy of the German Federal Government: Digital Germany 2015," (2010).
4. Ministry of Defence of Estonia, "Cyber Security Strategy," Cyber Security Strategy Committee, Tallinn, (2008), p.8.

The Cybersecurity Cornerstone

by Scott Algeier*

As the IT infrastructure has become a core component of our society, it has been integrated into daily business and leisure activities. IT products and services enable utility companies to power buildings, grocery stores to manage their inventories, and banks to process payments. It enables people to connect with friends and family from mobile devices that fit in a hand and enhances the productivity of employees who can work regardless of where they are physically located. Because of this, everyone has an interest in cybersecurity, including policymakers in the Nation's capital.

There are two basic sets of consequences that are often associated with cyber-attacks. The first is the loss of sensitive business or national security information. This includes key intellectual property, personal information of customers, and national security secrets. For example, well-funded, highly sophisticated nation states looking for corporate or national secrets target specific people within organizations in attempts to gain access to their networks so that they can then steal these secrets. Unhappy customers, contractors, and "hackitvists" target companies and organizations to implement their own brand of justice or revenge. These attacks are the most likely and occur relatively frequently. It seems each week there are new reports of this type of attack.

The other concern, which is less likely but potentially more damaging, is that a successful cyber-attack could "take down" key elements of the economy or cause significant physical damage. Such concerns include a total loss of the Internet, the electricity grid being taken offline for an extended period, or the inability of the financial system to operate. If any of these scenarios were to occur, the economic damage could be significant.

Based on these potentially severe consequences, a debate has emerged as to what is the best way to address cybersecurity. Although industry-government partnership has been the cornerstone of national policy for over a decade, some now argue that the Federal government should have a stronger role in securing critical infrastructure networks, either through imposing standards and developing regulations, or giving government agencies the responsibility to secure key critical infrastructure networks. The claim is that this is necessary since the private sector does not take the threat seriously and is incapable of securing its networks. Therefore, this argument goes, the interest of national security, requires strong government measures.

However, moving away from industry-government partnerships will actually impede national efforts to enhance cybersecurity, rather than advance them. A top down regulatory and standards based approach is not agile enough to keep pace with the cyber threat. Technology changes more quickly than regulations can be developed and standards force creative, forward thinking security professionals to develop security policies focused on checking compliance boxes rather than developing effective solutions.

In fact, industry-government collaboration is the only real way to address the cybersecurity challenge. Industry and government can collectively accomplish more working together by leveraging their strengths than they could by working individually. The idea that industry is not contributing enough to national efforts ignores the facts. Industry collectively has contributed many millions of dollars to this national effort, through memberships in Information Sharing and Analysis Centers (ISACs), supporting Sector Coordinating Councils (SCC), the Partnership for Critical Infrastructure Security, countless regional coalitions, and participating in the planning and development of national cyber exercises, among other activities.

(Continued on Page 5)

Cornerstone *(Cont. from 4)*

This is in addition to the support industry provides through embedding industry analysts at the National Cybersecurity and Communications Integration Center (NCCIC), the National Coordinating Center, as well as the steps companies take to secure their own networks and products.

In many cases, the problem is not lack of industry commitment, but the failure of policymakers to fully consider the contributions of industry. For example, in 2009, the Baseline IT Sector Risk Assessment was released by the U.S. Department of Homeland Security (DHS) and the IT SCC. It brought subject-matter experts from industry and government to examine the threat to six "Critical Functions" that the IT Sector provides. The end result was a prioritized set of "Risks of Concern" for five of the critical functions. Similar risk assessments have been done in other critical infrastructure sectors.

It is important to note that "the Internet going down" was not identified as a "Risks of Concern" in the IT assessment, yet many prominent thought leaders and policymakers continue to consider this one of our greatest risks. This, in turn, creates calls for the government to compel industry to "do more" when, as demonstrated by the Risk Assessment, the risks are already being appropriately managed. Industry answered the Federal governments' call to jointly develop sector-based risk assessments, but it is not at all clear how these assessments are being used to inform policymaking.

One of the key challenges industry and government face in working together is that they perceive the risk in different ways. The government views cybersecurity as a national security issue and devotes huge sums of money to try to eliminate national security risks. The mission of the Federal government is to protect the country.

While recognizing the national security concerns, industry views cybersecurity as a risk that needs to be managed at the individual corporate level. Operating in a competitive global market with the goal of providing the greatest value to customers and return on investment to shareholders, businesses balance the need to invest in cybersecurity against their needs to invest in research and development, sales and marketing, and other business interests. In short, industry manages cyber risk as a business risk as it pursues its business interests.

These two views of cybersecurity are not incompatible, but are complimentary. They provide the opportunity for industry and government to leverage the knowledge and resources of the other for the improvement of corporate and national security. They provide for more informed decision-making within industry and in government. Working together enables government policymakers to better understand business concerns and potential consequences of proposed policies. Likewise, industry can be better informed of government priorities and gain access to more detailed threat information. Together, industry and government can identify common interests and set priorities.

For example, industry best knows how IT assets are leveraged, deployed, and secured in their corporate environments. The private sector makes most of the IT products and provides most of the IT services that are deployed on industry and government networks. The experts for each critical infrastructure sector reside in the private sector (the National Monuments and Icons and Government Facilities sectors are excluded, of course). Without a partnership, government would lose this essential insight.

Similarly, the government has information about threat actors and techniques not widely available in the private sector. Industry is not interested in the classified sources and methods of this information. Instead, it is looking for indicators and other information that can enable it to take action to protect corporate networks. Sharing this information widely with industry through trusted channels will enhance corporate and national security.

Moving forward, rather than building new structures or creating a regulatory environment, it is imperative that the focus is instead on improving the existing partnership model so that it better meets the needs of both partners.

(Continued on Page 6)

Cornerstone *(Cont. from 5)*

As a Nation, we devote huge resources into building plans and writing documents, but devote comparatively few resources to implement and operationalize plans. This equation must change. We must spend less time writing plans and developing new policies and devote more resources to implementing and operationalizing current strategies. The time spent developing new strategies, organizations, and plans is time taken away from maturing and maximizing current capabilities. We already have the strategy and structure in place to effectively address cybersecurity. We just need to better use what has been built.

Fortunately, the foundation for a more effective partnership exists. It can be improved through the following:

• Building an Integrated Industry — Government Response Capability: DHS has established the NCCIC to serve as the primary domestic cyber operations center. It has begun to leverage the private sector, including industry specific ISACS into its operations. As this coordination continues, it is essential that the NCCIC develop policies and procedures that streamline information sharing with the private sector representatives in the NCCIC.

• Promoting and Enhancing Sensitive Information Sharing: Industry and government need to better utilize sector designated operational organizations such as ISACs to share trusted information. The National Council of ISACs is a key forum for facilitating cross-sector information sharing, but the capabilities of many ISACs remain underutilized. The Federal government can further assist the growth and capabilities of ISACs by actively encouraging private sector participation in them and by providing baseline funding to those ISACs that request it so that they can provide broad based information sharing and analysis capabilities throughout their sector. The private sector can also support these forums through their active participation in them.

• Increasing Awareness about Cybersecurity Issues: DHS has partnered with industry and others to promote National Cyber Security Awareness Month each October. This is a useful vehicle for promoting sound online behavior and basic cybersecurity awareness, but a more sustained effort is needed to promote cybersecurity to meaningfully impact end user behavior.

• Better Coordinating Cybesecurity Research and Development: The Federal government needs to better coordinate R&D efforts and funding across agencies and with the private sector to ensure that we collectively maximize the value of each dollar spent by ensuring efforts are not duplicated and are focused on identified priorities. For example, the 2009 Baseline IT Sector Risk Assessment, which was a joint effort by industry and government under the National Infrastructure Protection Plan, or NIPP, model, identified key research and development needs focused on core IT Sector Critical Functions. The Federal government has not yet taken any action on these recommendations.

• Collaborating Internationally: Since the information infrastructure is global, cybersecurity is a global issue. Just as implementing partnerships within national borders is essential to enhancing national cybersecurity, partnering across borders is essential to enhancing the security of the global infrastructure. This includes CERT to CERT (Community Emergency Response Teams) operational collaboration as well as effectively engaging in international policy forums to enhance cybersecurity.

In summary, the cyber threat is real. Each day, cybersecurity professionals in industry and government repel countless attacks against their networks. The cyber adversaries are diverse, talented, creative, and organized. Successfully managing cyber risks requires a common understanding of the threat so that actions can be identified and prioritized.

A unified effort between industry and government enables us collectively to identify and prioritize risks and develop defensive measures to address them. It leverages the resources and intelligence capabilities of government, with the subject-matter expertise of industry. The result is better informed and coordinated risk management strategies. The national cybersecurity challenge

(Continued on Page 17)

Establishing Short- and Long-term Plans for Securing Cyber-Physical Critical Infrastructures

by Alvaro A. C´ardenas
Fujitsu Laboratories of America

For the Federal government, the protection of our cyber-physical critical infrastructures against computer attacks is a matter of national security, public safety, and economic stability; however, most of our critical assets are owned and operated by private companies with pressing operational requirements, tight security budgets, and aversion to regulatory oversight. For most of these companies, creating a business case for improving computer security and for supporting long-term security research is a difficult task, partly because cyber-security risk is almost impossible to measure, and partly because most companies managing critical infrastructures have not (yet) been subject to damaging computer attacks. As the U.S. Department of Energy (DOE) stated in their Power Grid Roadmap,[1] "[m]aking a strong business case for cybersecurity investments is complicated by the difficulty of quantifying risk in an environment of rapidly changing, unpredictable threats with consequences that are hard to demonstrate." This has left our cyber-physical critical infrastructures fairly vulnerable to computer attacks.

This short article describes some of the most pressing security issues that need to be addressed in a short time. It outlines future long-term research in cyber-physical systems, and concludes with a brief discussion of current government efforts to improve the security posture of cyber-physical infrastructures.

Short-Term Security Issues

The increasing interconnection of control systems is exposing traditionally isolated systems to more scrutiny, and research has demonstrated the fragility of these systems. Some Internet-connected control systems are fully accessible online,[2] and some of them have even been attacked: in a recent example, the energy-management system of a building was compromised via the Internet by an attacker who changed the temperature set points, resulting in unusually high temperatures inside the facility.[3]

One of the main reasons for the brittleness of these systems stems from the equipment used in the field. In general, vendors of equipment for managing control systems have few incentives for establishing well-funded secure development programs to provide hardened systems because their customers are not requesting them.

Sean McBride of Critical Intelligence made an analysis of publicly disclosed control system vulnerabilities since 2001,[4] and reported that vendors and many others have only patched half of the vulnerabilities. In addition, ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) stated that 60 percent of the patches did not fix the problem. The frustration of more than ten years of continuous demonstrations of the insecurity of many products led Digital Bond — a leading control systems security company — to release Metasploit modules that can be used to compromise seven devices from five different control vendors[5] with the hope of "demonstrating the ease of compromise and potential catastrophic impact possible for any owner/operator, vendor, consultant or anyone else involved in ICS. C-level executives running the critical infrastructure SCADA (supervisory control and data acquisition) and DCS (distributed control systems) will know beyond any doubt the

(Continued on Page 8)

[1] http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.
[2] http://www.digitalbond.com/2012/02/27/get-your-ics-off-the-internet/.
[3] http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Feb2012.pdf.
[4] http://www.digitalbond.com/2012/01/30/documenting-the-lost-decade-ics-vuln-analysis/.
[5] http://www.digitalbond.com/2012/01/19/project-basecamp-at-s4/.

Cyber Plans *(Cont. from 7)*

fragility and insecurity of these devices. Hopefully they will find this unacceptable, demand their vendors offer a secure replacement, and spend the money to replace the PLCs."[6]

It is clear that the current situation is unacceptable and there is a need to create incentives so that asset owners request from vendors secure coding practices, hardened systems, and quick response when new vulnerabilities or attack vectors are identified.

Software development is an interesting case in the analysis of critical infrastructure security. While most companies are held accountable for the safety of their products, the current practice in the software industry is to disclaim responsibility for the quality of their software through user license agreements.

To address this lack of accountability, the American Law Institute (ALI) proposed the *Principles of the Law of Software Contracts* in May of 2009. Their goal was to clarify and unify the law of software transactions, because the current law is "a mish-mash of common law, Article 2 of the Uniform Commercial Code, and federal intellectual property law, among other things, is in dire need of improvement. This should not be a surprise. Most of the bodies of law that courts draw upon to decide software contract cases predate software and are not responsive to its needs. But software transactions are too important to be relegated to a second-hand legal subject-matter status."[7]

One of the controversial rules makes software vendors liable for knowingly shipping buggy software by establishing an implied warranty of no material hidden defects that is non-disclaimable. In an unlikely alliance, Microsoft and the Linux Foundation have joined forces against this proposal, arguing that the laws would stifle innovation, raise the cost of software, and hurt small developers.[8] One of the arguments in the letter by Microsoft and the Linux Foundations is that today, "there is no great failure in terms of substandard quality or unmet expectations that would justify imposition of new mandatory rules."[9] Given the examples presented earlier in this article, it is not clear if their argument holds given the current state of software products for control systems. Perhaps software used for monitoring and control of critical infrastructures can be used as a testing ground of these new principles.

Even without the imposition of new mandatory rules, asset owners have the means to influence vendors to provide more secure products by requesting better software development practices. To help with that effort, DHS released a procurement language guide.[10] This guide can serve as a starting point for developing more and better tools for education and awareness of asset owners and operators.

Long-Term Research

While the previous section dealt with the low-hanging fruit for improving the security of cyber-physical infrastructures, securing a system against advanced persistent threats is usually outside the scope and budget of most private critical system operators.[11] Stuxnet made clear that there are well-funded groups with motivations and skills to mount sophisticated computer-based attacks to critical infrastructures.

Stuxnet is a computer worm that uses several zero-day exploits, a Windows rootkit, the first known Programmable Logic Controller rootkit, antivirus evasion techniques, peer-to-peer updates, and stolen certificates from trusted Certificate Authorities. The sophistication of this attack and reverse-engineering of the executed code has led many to believe that

(Continued on Page 18)

6. http://www.digitalbond.com/2012/01/23/project-basecamp-vigilante-hopes/.
7. Highlights of the Principles can be viewed here.
8. http://www.linuxfoundation.org/sites/main/files/publications/msft_lf_ali_letter.pdf.
9. Ibid.
10. Section 5, Coding Practices in DHS Procurement Language Guide, available at http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf.
11. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
12. The sophistication of this attack has led many to believe that Stuxnet is the creation of a state-level sponsored attack.

From Critical Infrastructure Protection (CIP) to Critical Infrastructure Information Dependency (CI-ID)

by David Bakken,[1] Associate Professor of Computer Science, Washington State University, USA; and
Neeraj Suri, TUD Chair Professor, Dept. of CS, TU Darmstadt, Germany

Protecting critical infrastructures (CIs) has always been a concern of governments everywhere and has, of course, accelerated greatly since 9/11. Traditionally, CIs were closed systems and domain specific protections worked adequately. Over time, CIs have incorporated varied information and communications technologies (ICT) techniques primarily intended to provide supplemental CI functionalities. However, these ICT elements often become interspersed (by design or by oversight) with the core CI functions to now expose these CIs to ICT-based attacks. Unfortunately, in terms of "protecting" our CIs, most of the focus on CIP (and also the ICT parts) has been on cybersecurity, with some risk management, inter-CI dependencies, and a handful of other topics thrown in arguably in somewhat ad hoc ways.

However, the technologies that can help protect societies' critical infrastructures involve much broader end-to-end systems issues than just cybersecurity. Indeed, as a cybersecurity pioneer said long ago (just for cybersecurity alone): "If you think encryption is the solution to your problem, then you don't understand encryption, and you don't understand your problem,"[2] The core of classical security is often defined as CIA (confidentiality, integrity, and availability), but the CIP community has largely focused on the CI part to the neglect of A. Unfortunately, there is a range of interrelated concerns far beyond cybersecurity (including just adding more 'A') that need to be addressed in a systematic fashion to adequately protect CIs from disturbances in the ICT it heavily depends upon.

Dependable Computing Groundwork

The dependable computing community has done promising initial work in this area over the last three decades.[3] Its definition of dependability is "the measure in which reliance can justifiably be placed on the service delivered by a system" (emphasis is ours); this includes fault-tolerance, cybersecurity, safety, maintainability, and other issues in a carefully integrated manner.[4] However, the dependable computing community has long known that modern societies depend on information and communication technologies far beyond what can be reasonably justified. In no realm is the lack of justification more severe than that with modern critical infrastructures, in terms of consequences to our modern way of life.

Gaps in CIP Efforts

The huge dependence of CIs on ICT is a well-known problem. However, this knowledge falls far short of what is needed to characterize the dependencies of a given CI on ICT so that it is adequately actionable in terms of being able to reason about, model, validate, manage, explore alternatives, etc. If the state of the art and practice are both extended in such ways, it would be quite useful in helping explore fundamental mechanisms and strategies that are useful across different CIs as well as beginning to systematically reason about how interrelated the ICT dependencies are across CIs.

(Continued on Page 10)

1. Contact author.
2. This is widely attributed to Roger Needham, the co-inventor of the Needham-Schroeder authentication algorithm. We note that Needham and some others attribute this gem to pioneer computer systems researcher Butler Lampson, who in turn attributes it to Needhmam.
3. These include the IEEE/IFIP DSN conference (and its predecessors FTCS, DCCA), the IFIP WG 10.4 on Dependable Computing and Fault Tolerance, and others.
4. A. Aviziensis, J. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, 1(1), (January 2004), 11-33.

CIID *(Cont. from 9)*

Right now, it seems fairly safe to assume that a broad attack on ICT, if successful, greatly harms most or all CIs. However, with the aforementioned ICT dependency characterizations, it may be possible to better understand these dependencies and eventually devise ways to defend them all in a holistic way that is much more effective than today's relatively domain-specific CIP. That is, different CIs could have fundamentally different structures in their dependency on ICT that provides similar or identical benefits, yet this design diversity removes (or at least reduces) common mode ICT vulnerabilities across CIs.

Electric Grid Example

Prior research programs, reports, and other efforts in CIP have fallen short in a number of ways compared to the comprehensive coverage outlined above. To illustrate this, we consider the Electricity Sector.

Electric grids across the world had almost zero reliance on digital ICT for many decades. However, after a large blackout in the northeastern United States in 1965, there began a major push to get utilities to have some modest amount of sensors beyond what was directly measurable at their control centers. This is today's SCADA (supervisory control and data acquisition) infrastructure. It has since been augmented in a fairly piecemeal fashion by more modern ICT technologies.

Further, the Electricity Sector moves very slowly on the ICT front, and thus well behind (and often unaware of advances in) other industries in its sophistication in use of ICT developments over the last few decades.[5] In devising protection and control schemes, ancillary services, and the like, power researchers and engineers generally assume that communications will be where they are needed and will be good enough. This is, of course the opposite of what CI-ID management requires. It also is the case, despite the well-known fact, that the new kinds of wide-area protection and control strategies that are necessary to deal with an increasingly stressed grid rely heavily on data communications, for which they have significantly more challenging delivery requirements than other industries (and even the military) typically have.[6] These delivery requirements are also quite diverse, so it is not all "one size fits all" delivery.

There are glimmers of hope, however, in the Electricity Sector that offer a hint of what systematic CI-ID management may evolve to. There are at least a few papers in the last decade that do consider the effect on communications latencies and availability on power strategies.[7,8,9] There are also multiple projects in the European Community addressing some more broader basics of CI dependency on ICT.

Moving Forward Towards CI-ID

These ICT dependency analysis efforts need to be systematically broadened, and involve other CIs, if the vision of CI-ID (and its corresponding benefits) are to be realized. Some of this work would involve deeper analysis of inter-CI dependencies; the key need for detailing information flows from a CI to various subsystems of ICT to develop relations and vulnerabilities, and other issues. So what kinds of technical expertise would this combine? To name a few: dependable computing (many applied and theoretical sub-disciplines); distributed computing (both applied and theoretical); software engineering; architecture languages; "systems of systems" composition and integration;

(Continued on Page 11)

5. D. Bakken, R. Schantz, and R. Tucker, "Smart Grid Communications: QoS Stovepipes or QoS Interoperability?" Grid-Interop 2009 (best "connectivity" paper).
6. D. Bakken, A. Bose, C. Hauser, D. Whitehead, and G. Zweigle, "Smart Generation and Transmission with Coherent, Real-Time Data," Proceedings of the IEEE (Special Issue on Smart Grids), 99(6), (June 2011), 928-951. Preprint (if IEEE paper not accessible).
7. X. Dong, K. Hopkinson, X. Tong; X. Wang; J. Thorp, "IP-based communication systems for wide-area frequency stability predictive control," Critical Infrastructure (CRIS), 2010 5th International Conference on , IEEE, vol., no., pp.1-7, 20-22 Sept. 2010.
8. S. Bhomik, K. Tomsovic, and A. Bose. "Communication Models for Third Party Load Frequency Control", IEEE Transactions on Power Systems, 19(1), February 2004, 543-548.
9. K. Zhu, M. Chenine, J. König, L. Nordström, "Data quality and reliability aspects of ICT infrastructures for Wide Area Monitoring and Control systems," Critical Infrastructure (CRIS), 2010 5th International Conference on , vol., no., 20-22 Sept. 2010.

CIID *(Cont. from 10)*

operations research; modeling (many kinds); risk management; cybersecurity; and many domain experts on the non-ICT aspects of various CIs (hopefully ones with at least modest ICT exposure!). All working in a closely cooperating community, including funding and leadership from both government and industry, coherent interdisciplinary research programs, and conferences, etc.

A concrete ICT example is the use of middleware and overlay networks in many domains. Overlay networks essentially virtualize network services, and allow the contextualization of solutions for a given CI while allowing the solutions (or variants thereof) to be reused by other sectors. This allows a diverse set of technologies in the underlay network to be harnessed to provide a richer and more resilient set of system-wide properties. For example, the power grid's wide-area data delivery networks developed over the next decade will almost certainly contain carefully federated integrations of (1) core backbone elements that can (and must!) be very tightly controlled, and (2) peer-to-peer networks managing large chunks of the networking infrastructure near the edges over whom much less control is possible, yet exerting whatever control and adaptability is possible.[10] These will be combined with older technologies (e.g., microwave links) that can, if carefully managed, provide valuable extra redundancy for the most important data flows.

CI-ID Applied to the Power Grid

In returning to the power grid example, here is how it could apply CI-ID. Consider a power researcher coming up with a new control strategy. The researcher would typically "optimize" it for some steady state of power conditions, and assume the communication is "good enough." However, the researcher could begin to apply CI-ID by considering how sensitive (in the generic case) to message drops and a few specific failure assumptions. The researcher, if given guidelines and the right CI-ID questions to ask themselves, could likely come up with similar algorithms that might not be quite as "optimal" but would work adequately and over a broader range of IT glitches. Note that, so far, this is a very crude and simplistic description of the dependence of the control algorithms on ICT: models that more richly describe the ICT dependencies are quite possible, as the state of the art supports them. But, some slightly less simple models give a hint at what this line of thinking could ultimately do. For example, the power engineer could also give alternate sets of input data sources that they could work with, along with the benefit/utility of having each set (or even over a predicate expression) for a suite of related algorithms that can work on some diversity in sensor sources. The data delivery infrastructure could then trade off the weighted importance for that application (in the current grid situation) and deliver the best set of data, and switch to the best algorithm given the ICT conditions.

So far, our power engineer has only been describing dependencies on ICT directly. The same concepts, and indeed mechanisms, can be applied to power conditions, as measured in live sensor data. For example, if the power engineer can describe in terms of live power variables each of their related algorithms is appropriate for, that can also be utilized to use the most "appropriate" algorithm, given the current situations in both the power and ICT domains, and a coherent fashion.

The infrastructure for this is not something that the engineer had to build themselves, or even the Electricity Sector has to: the data delivery (of both power status data and ICT instrumentation) is very doable over the conceived NASPInet framework (or its GridStat instantiation[11]). The adaptive middleware for defining such predicates and automatically switching between them has been done in the context of the Quality Objects system starting in the

(Continued on Page 19)

10. D. Germanus, I. Dionysiou, H. Gjermundrød, A. Khelil, N. Suri, D. Bakken, and C. Hauser, "Leveraging the Next-Generation Power Grid: Data Sharing and Associated Partnerships", *IEEE PES Conference on Innovative Smart Grid Technologies Europe*, October 10-13, 2010, Gothenburg, Sweden.

11. A. Aviziensis, J. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, 1(1), (January 2004), 11-33.

Cybersecurity

by John Lacey, The McCormack Firm, LLC

The date is June 6, 2014, 70 years to the day since D-Day. It is 6:44 a.m. and the lights in New York City just went out. Boston, Philadelphia, Newark, and Washington D.C. then lose power. Eventually, the whole East Coast goes dark. Here and there, emergency generators power essential services like hospitals, but for how long? Things are deteriorating at such a fast rate that anarchy is close at hand.

At the same time, the water companies in the Mid-West are reporting that their pumps have either shut down or burned out. The effect is profound: millions of people are going to be without water within a few short hours.

Out in the Southwest, residents are hearing the wailing sound of sirens coming from nuclear power plants. No one knows what is happening; they have never heard the nuclear sirens before. The police are trying to calm the public, but even they have limited or no information on the situation.

Up in the great Northwest, it is still the middle of the night, but the residents will awake to find out that the entire cell phone spectrum is down. No one has a signal. At first, it seems like it must be a glitch, but eventually the landline system is overwhelmed with people trying to find out why their phones do not work. Over the last 10 years, the landline system in the United States has been scaled back due to non-use and cannot handle millions upon millions of phone calls all at once.

Word starts to spread that a foreign entity is responsible for our calamity — and they picked our most successful military day to expose our weaknesses. But who was it? China? Iran? North Korea? Romania? Anonymous? Could this be the "Cyber Pearl Harbor" that people are worried about? Maybe. Is it likely? That depends on who you ask. Theoretically, something like this could happen. But in reality, our cybersecurity issues are a lot less dramatic.

According to DHS, our "critical infrastructure" includes: "[t]he assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof." This would obviously include water, power, transportation, communications, and banking. Of these five, all are connected to the Internet one way or another. Trying to find a person who has not used the internet today would be a challenge (well, excepting certain communities, my Aunt Agnes, and maybe some hardy souls living off the land). The Internet is both a gift and a curse in this regard.

The Internet is used by just about everyone, everyday. It is incredibly powerful, and minimally regulated. Maybe we have all seen too many post-apocalyptic Hollywood movies not to imagine the worst. This author grew up in the time of "The Day After" when we all thought that it was only a matter of time before nuclear Armageddon arrived. Well, it never did, at least not yet. That fear had somewhat abated only to be replaced by irrational Y2K fears, and now Cyber Pearl Harbor fears.

Richard Clarke, former counterterrorism chief for three United States Presidents, recently gave an interview to the *Smithsonian Magazine* where he discussed a possible Cyber Pearl Harbor. This author believes he got it right when he said that a more likely outcome is "death by a thousand cuts" as opposed to one big event. Mr. Clarke states that the Chinese Government has already hacked into every major corporation in the United States. What are they looking for? Ways to marginalize the United States' wealth, he says. We spend billions on research and development to create new and amazing things. It would certainly be a lot easier

(Continued on Page 13)

Cybersecurity *(Cont. from 12)*

to just steal the finished product, would it not?[1] On the other hand, at a hearing on a Cybersecurity bill in Washington D.C., Senator Joe Lieberman said, "to me it feels like September 10, 2001" when discussing the state of cybersecurity for our critical infrastructure.

The Internet is used by Grandma Smith to buy toys for her grandkids as well as NASA to control the Space Station. Billions of dollars fly across the Internet daily, as well as millions of sixth-graders updating their "Facebook status." Can you see the dichotomy here? We are an interconnected world at a level previously thought unimaginable. The Internet transcends countries' boundaries, vast oceans, and even the air above us. Today, we can communicate with a farmer in the Congo as easily as we can with our next door neighbors.

This interconnectivity has not been readily accepted by all. Some countries have decided to create walled off sections of the Internet (see generally: China, Iran, and North Korea) where the incoming and outgoing traffic is highly controlled. The United States, however, has not done this and allowed the Internet to be what it was designed to be: an open network. Perhaps therein lies the real problem. We are playing a game by a different set of rules than everyone else. Well, maybe not everyone, but certainly the ones who appear to want to do us harm. The Internet was designed to be accessible by anyone. If you are part of the critical infrastructure of the United States and you connect your internal operations to the Internet, then you must understand what you just plugged into.

Cybersecurity is not one issue. It is certainly not one issue to be solved by one law coming out of Washington. The private sector took over the Internet early on and has made incredible strides bringing it to billions of people around the Globe. The commercial rewards because of the Internet are staggering.

In large part, profits have been and are driving the growth of the Internet as well as the growth of the criminal element who choose to participate in the more dark aspects of our new interconnectivity. Is there any money in security? Well, if you are the one providing it, sure, but if you are the one paying for it, then probably not.

To get a sense of what is really happening in the digital world, one need only refer to a recent speech given by the Federal Bureau of Investigation's (soon retiring) top cyber cop, Shawn Henry. According to Mr. Henry, the United States is "outgunned" in the "hacker war." He says that the current security is no match for the skills available in the hacker's world. In one very telling moment, Agent Henry says that while investigating one crime, his agents are finding data from another, unrelated, crime. When the missing data owner is contacted, they had no idea it had even been stolen![2]

And there it is… the realization that we just do not get it. If you were given a box of 10,000 tax returns, complete with full bank account numbers to receive any refunds, would you take care not to leave it unprotected? Now, what if you were given the exact same information, except in digital format on a thumb drive? Would your awareness be as high as it was when you had the huge box? Or would the thumb drive simply be something of less importance than, say, your car keys?

As a digitally enhanced society, we need to change our way of thinking. Relying solely on technology or laws to protect our key information will not be enough. Technology is only as good as the person using it and once its key components have been compromised, it is as good as a padlock — one lock cutter away from useless. Passing laws that require businesses to protect information seems like a good idea, but without rigorous education and enforcement, the laws are useless.

Congress is currently debating laws in the cybersecurity arena in order to shore up our defenses. One of the key aspects involves a public-

(Continued on Page 20)

1. Ron Rosenbaum, "Richard Clarke on Who Was Behind the Stuxnet Attack?" *Smithsonian Magazine*, (April 2012), http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html?c=y&page=1.
2. Devlin Barrett, "U.S. Outgunned in Hacker War," *The Wall Street Journal,* (March 28, 2012), http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html.

Legal Insights

Tracking Cybersecurity Legislation

Robert Mueller, Director of the Federal Bureau of Investigation, recently emphasized how vulnerable America is to cyber-attacks when he stated that "there are only two types of companies, those that have been hacked and those that will be." The recently introduced Cybersecurity Act of 2012, the synthesis of a number of different legislative initiatives on the issue, aims at shoring up those vulnerabilities in both public and private networks by combining public and private effort.[1]

If adopted, the act would require the government to take a number of steps towards protecting the Nation from cyber-attacks. These steps are grouped to achieve the following goals:

- Determine the Greatest Cyber Vulnerabilities
- Protect Our Most Critical Infrastructure
- Protect and Promote Innovation
- Improve Information Sharing While Protecting Privacy and Civil Liberties
- Improve the Security of the Federal Government's Networks
- Clarify the Roles of Federal Agencies
- Strengthen the Cybersecurity Workforce
- Coordinate Cybersecurity Research and Development

Under this proposed legislation DHS would consult with a group of stakeholders, including owners and operators, the Critical Infrastructure Partnership Advisory Council, and sector-specific agencies to designate systems and assets as critical infrastructure if their "disruption could result in severe degradation of national security, catastrophic economic damage, or the interruption of life-sustaining services sufficient to cause mass casualties or mass evacuations."

Once systems and assets are designated as critical infrastructure, then owners must comply with "cybersecurity performance requirements," which would be based on sector by sector risk assessments.[2] Two factors are put into place to reduce the burden of these potential requirements, (1) if regulations already exist that provide sufficient protection then the cybersecurity performance requirements would not apply; and (2) owners and operators would have a redress mechanism to appeal the critical infrastructure designation.

If the regulations apply, owners and operators would also be required to report significant cyber security incidents, keep informed of cyber risks, and perform self, or third party audits of their protection systems. If owners and operators comply with the regulations, then they would be protected from civil damages from cyber incidents identified in the risk assessments.

The proposed legislation also suggests a robust regime of information sharing on a voluntary basis. This goal is achieved through a variety of measures, including the development of a cybersecurity information exchange and a ruling out causes of action that rely on information voluntarily disclosed.

The Cybersecurity Act of 2012 is not, however, the only Act being introduced. Senator John McCain and a number of his republican colleagues have introduced the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act (SECURE IT) bill as an alternative focused on privacy, information sharing, and liability limitations.[3] The SECURE IT bill

(Continued on Page 21)

1. http://www.hsgac.senate.gov/issues/cybersecurity.
2. http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105_-summary.
3. http://mccain.senate.gov/public/index.cfm?FuseAction=PressOffice.PressReleases&ContentRecord_id=cf574830-f045-891e-2b5b-5fdee2ada559.

RESILIENCY DC

MAY 1, 2012

at

George Mason University's Arlington Campus
Founder's Hall

The Center for Infraastructure Protection and Homeland Security (CIP/HS), the Business Continuity Institute (BCI), and NorthEast Disaster Recovery Information Exchange (NEDRIX) will be hosting.

"Resiliency Integration of complementary disciplines and approaches." Over the past decade both the government and private sector have independently and collectively focused on developing and implementing various programs to ensure their organization is resilient to any threat or hazard. These complimentary programs include Continuity, Critical Infrastructure Protection (CIP), Emergency Management and Cyber Security. This event brings together experts from both the government and private sector to discuss how these programs are working to integrate and streamline while sharing their best practices, insights, and case studies. In addition, there will be a collaborative table-top exercise that will foster communication and information sharing amongst all attendees.

This one day conference brings together leaders and managers from both the government and private sector to discuss resiliency programs, challenges, successes, and case studies. This year's event expects to be better than last year as it will be held at George Mason University's Founders Hall, has some great speakers, and an interactive information sharing session in the afternoon. Below is the link to the website that provides information on the agenda and allows you to register.

For more information and to register, please visit
http://www.resiliencydc.com/

The Center for Infrastructure Protection and Homeland Security (CIP/HS) is pleased to announce it is co-hosting the "X-SCM: The New Science of Extreme Supply Chain Management"

on

Friday, May 18, 2012 at **George Mason University's Arlington Campus, Founder's Hall**

Washington D.C. area supply chain professional organizations and universities have come together to produce an interactive workshop based on the book of the same name. We will focus on the critical impact of supply chain volatility on private and public sector organizations. Dr. Sandor Boyson, X-SCM co-author, will offer our opening keynote presentation and will be joined by the Cross Sector Supply Chain Working Group. Visionary supply chain leaders, by heeding the impact of volatility on private & public sector supply chains, are vitally important to the success of an enterprise. How prepared is your firm to create a resilient supply chain and proactively implement mitigation strategies and contingency plans as you optimize shareholder value? Join us as we boldly explore - and conquer - the risks posed by the nature of today's myriad forms of supply chain disruptions.

For more information on this event and to register, please visit
http://vlk2.dphen.com/~mentorc/.

Cornerstone *(Cont. from 6)*

will not be fixed by mandates and regulation, but by better leveraging, engaging, unifying, and implementing existing efforts. ❖

Scott Algeier is the Founder, President, and CEO of homeland security consulting firm Conrad, Inc. He also serves as Executive Director of the Information Technology-Information Sharing and Analysis Center and as Vice Chair of the National Council of ISACs. The views expressed are his and do not necessarily reflect the views of his clients.

CIIP *(Cont. from 3)*

documents that refer to cybersecurity.

CIP and Cybersecurity

Brought together, the growing field of cybersecurity coupled with the established CIP field reveals an interesting evolution of the CIP debate — one where the term CIIP has almost disappeared in exchange for the broader, more integrative concept of cybersecurity. Consequently, the debate has pivoted away from framing CIP as mainly a task for national security. To note, strategies and policy papers (also) increasingly emphasize the importance of ICTs for the national economy and point to the high costs of cyberattacks for the corporate sector, whereby these costs are deemed to have a negative impact on the growth of national economy. Some of the strategies and policy papers also explicitly highlight the connection to information society and economic strategies. At the same time, there is a clear nexus between economic and national security interests, which is even more accentuated by the fact that many of the cyberstrategies view cybersecurity as being directly related to other governmental strategies, especially the respective countries' national security strategies.[5]

This shift also has some implications for protection efforts. In short, the growing importance of cybersecurity, or the information domain more broadly, provides more common ground between governments and the corporate sector — strengthening public-private partnerships, which can in turn enhance protection efforts and the resilience of the system as a whole. Responsibility for becoming more resilient can be delegated to the private sector to a large degree, and less persuasion is needed on the side of governments. This, in turn, speaks to both the public and private sectors as protection measures benefit economic interests as well as national security. ❖

---

5. The United Kingdom realizes that: "Cyber security cuts across almost all the challenges outlined in the National Security Strategy, and interlinks with a wide range of Government policies, involving many departments and agencies" (UK Cyber Security Strategy 2009, p. 14). The U.S. encourages the development of a new security strategy, noting that: "The national strategy should focus senior leadership attention and time toward resolving issues that hamper US efforts to achieve an assured, reliable, secure, and resilient global information and communications infrastructure and related capabilities" (U.S. Cyberspace Policy Review 2009, p. 8).

Cyber Plans *(Cont. from 8)*

Stuxnet is the creation of a state-level sponsored attack targeting the Iranian nuclear program.[12] Stuxnet was originally spread by USB sticks to reach networks not connected to the Internet. Once in a network, it searched for a specific industrial control configuration. If it did not find it, the worm would stay dormant and eventually die. However, if it found the specific control system plant, it launched an attack by accelerating and decelerating beyond safe operational limits frequency converters used in centrifuges enriching uranium in nuclear plants. The attack aimed at damaging the centrifuges, while feeding false sensor data to computer monitors to pretend that everything was operating under normal conditions.

There is very little that traditional security mechanisms can do against this type of sophisticated attack. To counter advanced threats, we have previously argued for the need to promote research in resilient cyber-physical systems.[13] The Stuxnet attack would be severely limited if the system had redundant and independent safety mechanisms to report sensed data through alternate systems and detect when the system was not performing according to its specification.

By promoting a research plan in cyber-physical systems security and understanding the interactions of the physical world with IT, we should be able to develop a general and systematic framework for securing control systems in three fundamentally new areas: (1) better understand the consequences of an attack for risk assessment; (2) design new attack-detection algorithms by monitoring the behavior of the physical system under control; and (3) design new attack-resilient algorithms and architectures to survive cyber attacks while sustaining critical functions. This will enable DOE's 2020 vision of smart grid security: "[b]y 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions."

The Road Ahead

To improve our security posture, the Federal government needs to devise new incentives and mechanisms to promote and sustain long-term improvements in security. To this end, there are two opposing proposals currently being discussed in congress: The Cybersecurity Act of 2012 and the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act (SECURE IT).[16] Both proposals emphasize the need to facilitate sharing of cyber-threat information, support education and long-term research in security, and better risk-management in Federal agencies. One of the main differences relates to the new regulatory oversight by DHS proposed by the Cybersecurity Act of 2012 to mandate security improvements in critical infrastructure areas, while SECURE IT relies on incentives for information sharing and public-private partnerships. While more regulation tends to create a culture of compliance instead of a culture of security, it is not clear if market incentives alone will create enough momentum to improve the security posture of our critical infrastructures. In the power grid, North American Electric Reliability Corporation (NERC) CIP regulation is arguably one of the reasons operators and vendors invest in computer security for the bulk power system, while the distribution system (not covered by NERC CIP regulations) has to create new business cases to promote investments in security. However, as explained in the introduction of this article, creating a business case for security investments is complicated by the difficulty of quantifying risk in an environment of rapidly changing, unpredictable threats with consequences that are hard to demonstrate.

Despite the differences between the proposed Acts, it is encouraging to see renewed interest from the government in protecting critical infrastructures. We hope the sponsors of the two bills will work together to create a unified framework with the best parts of both proposals to create a solid government support for the security of cyber-physical infrastructures. ❖

13. http://static.usenix.org/event/hotsec08/tech/full_papers/cardenas/cardenas.pdf.
14. http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011.
15. http://www.wired.com/images_blogs/threatlevel/2012/02/CYBER-The-Cybersecurity-Act-of-2012-final.pdf.
16. http://documents.nam.org/tech/secure_it_summary.pdf.

CIID *(Cont. from 11)*

mid-1990s.[12] It has over 50 person-years of DARPA labor put into it, integrated many QoS and management mechanisms and policies, and is available as an open source along with its set of policy languages, runtimes, and tools. The same concepts and automation (and, most likely, supporting tools) described above could be provided by other tools, and readily be extended to CIs other than electricity.

Next Steps

So what research agencies should be deeply involved in CI-ID? In the United States, DHS and the National Science Foundation are obviously leading candidates, but also likely the National Security Agency. Further, given that CI-ID techniques would benefit not only CIs, but more general infrastructure information dependency (I-ID) management, also the U.S. Department of Commerce. Further, the U.S. military (and others) have long developed detailed contingency plans for ICT (and other) assets being destroyed or degraded. This suggests that DARPA should fund the IID community to help the military benefit from more generalized solutions (let us call that military IID, or MI-ID). Beyond the United States, the European Community as well government agencies responsible for critical infrastructure protection in Canada, Japan, and elsewhere are and should be involved in CI-ID.
And what kind of questions would CI-ID, if successful, be able to answer?

- How much does a given CI actually depend on ICT? How can we build models of such dependencies for a given CI such that we can reason about this (beyond a scalar rating or even a simple grade), measure, and validate such models?

- What is the structure of the dependency of a given CI on ICT technologies? More than a generic and vague scalar or qualified (High, Medium, Low) …. i.e., not nearly actionable.

- How will that complex ICT dependency affect the CI's functionality as the ICT fails in various ways? Is this degraded functionality graceful, predictable, and manageable? If not, what would it take to make it so?

- Given a rich understanding of a CI's ICT dependency, can we devise other ways the CI could depend on ICT that have different failure coverage and characteristics?

- How can the above dependency information be used to defend multiple infrastructures?

- What (partially or completely) reusable techniques can be used here? Can we employ alternate "structure" (topologies, degrees, etc) of dependency on ICT such that they offer the same (or close) functionality for the CI while having different failure/degradability properties, or reduce common vulnerabilities across CIs?

- How can we model and validate all the above?

If successful, CI-ID would enable society to move away from custom technology-specific point solutions to much more generalized, abstract, and reusable information flow analysis. This in turn would enable CIs to be more resilient, and to demonstrably justifiable degrees of dependency on ICT, with less cost.

It is time for such a radical and disruptive change to the hardcoded "business as usual" in critical infrastructures' ICT, don't you think? ❖

Acknowledgements:
We thank Ken Birman, Bob Braden, Mani Chandy, Carl Hauser, Rick Schantz, Richard Stephenson, and John Wroclawski for their discussions on these and related topics.

Professor David Bakken can be contacted at bakken@eecs.wsu.edu and Professor Neeraj Suri can be contacted at suri@cs.tu-darmstadt.de.

12. J. Zinky, D. Bakken, and R. Schantz, "Architectural Support for Quality of Service for CORBA Objects," *Theory and Practice of Object Systems*, (April 1997).

Cybersecurity *(Cont. from 13)*

private information sharing initiative. Congress believes that if the public sector, generally law enforcement, would share their knowledge of the current threat spectrum, then the private sector would be able to respond accordingly. Congress also believes that within the private sector, this same information sharing should occur; a sort of collective knowledge base of the threat matrix. The problem is that the entities in the private sector are in no rush to share their experiences with their competitors when a cyber incident affecting a competitor can become a profitable opportunity for them. Sure, there are certainly entities that share current threat intelligence, but to think that these companies are approaching this issue with wide open books is simply naïve.

Effective security comes as a result of understanding the threat and creating effective defenses to deal with that threat. An offensive approach to threat analysis can greatly enhance ones' defenses. Researchers who specialize in uncovering vulnerabilities can be (and are) sought after commodities. If you are an especially effective researcher, you will be handsomely rewarded. Will the company who decides to pay this researcher willingly provide the results to the rest of his industry? According to a recent article by Dennis Fisher of Threatpost, the answer is no. Mr. Fisher writes, "[t]oday's climate is unlike anything that's been seen in the security world in recent memory."[3]

The bills circulating on Capitol Hill in the cybersecurity arena read more like policy papers than laws and fear is an essential element driving the issue. To think that Washington can legislate cooperation in a profit driven, capitalistic economy, where such specialized information has immense value, is really asking a lot.

Reflect back on Agent Henry's story about his agents informing a business owner that they had found that business' data during another criminal investigation. This business owner did not even know it had been stolen. It is very hard to share your experiences with cyber incidents when you did not even realize you experienced one.

Computers used to be the purview of geeks, nerds, scientists, and other less than mainstream people. Today, these machines have been, for lack of a better term, "dumbed down" to allow their use by the general populace. Computers have infected every aspect of our lives. There is more computing power in the average cell phone than was needed to get to the moon. The problem is we, as a society, do not even realize what we have in our pocket. Our collective awareness is not at the appropriate level.

In order for our cybersecurity to improve, the people involved, not just the "tech" people, need to take a new approach. Cybersecurity is not a pure "tech" issue, it is a societal one. Technological solutions, new laws, and better education; these things are important to improving our cybersecurity, but they will not solve the problem.

In general, people are unaware of the value of the information they either possess or can access. Recall the full disclosure by RSA in the wake of their data breach… it started with a phishing e-mail to a staff member with an attached Excel spreadsheet that was cleverly titled with a name that would resonate with that particular employee. The spreadsheet was opened and the bad guys entered. And enter they did, leaving with a significant amount of very, very valuable data.

Today's concern about a "digital pearl harbor" may be well placed if only to increase the awareness of how our world has changed. We cannot "see," "touch," or "feel" data, yet it is everywhere. If we mistreat it, it will come back to haunt us.

Perhaps this is a generational issue. The generation before mine created the computers, and my generation got them to all talk to each other; perhaps it will be up to the next one to make sure that we retain our superior position over the machines. ❖

[3] Dennis Fisher, "Offense is Being Pushed Underground," *Threatpost*, (March 8, 2012), http://threatpost.com/en_us/blogs/offense-being-pushed-underground-030812.

Legal Insights *(Cont. from 14)*

also differs in that it has a strong focus on not increasing regulatory burden and bureaucratic bloat.

Secure IT vests primary authority with the NSA and U.S. Cyber Command instead of DHS, and utilizes existing centers for information sharing instead of creating a new information sharing exchange. The focus on lean measures was highlighted by Senator Saxby Chambliss, a co-sponser of the bill, when he stated that "more government is seldom the solution to any problem." As an example of the low regulatory burden of the bill, instead of imposing affirmative requirements on all private owners and operators of designated critical systems and assets, the SECURE IT bill only requires federal contractors to disclose cyber threats.

SECURE IT uses an incentive based approach to encourage other private actors to behave in a manner that produces greater security. To promote information sharing, SECURE IT creates anti-trust exemptions to allow competitors to share information on cyber threats. Additionally liability protections are included as incentives to encourage companies to protect their cyber systems.

Although some provisions, such as information sharing, enjoy widespread bipartisan and industry support, the balance between security, regulatory burdens, and liability protections will ultimately be a product of political compromise. Moreover, there are additional cyber security bills that are being floated in the House. ❖

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1