Government-University-Industry Research Roundtable
Policy and Global Affairs

February 23-24, 2016

CRITICAL INFRASTRUCTURE SECURITY

The Role of Public-Private Partnerships

To ensure the security of the nation's critical infrastructure, it is necessary to better understand the cross-sector dependencies of infrastructure sectors and the potential cascading effects of a breach. On February 23 and 24 the Government-University-Industry Research Roundtable held a meeting to explore the state of critical infrastructure security in the United States, share and discuss current protection and prevention efforts, identify research priorities, and examine how public-private partnerships can enhance critical infrastructure security.

The keynote address on February 23 was given by **Joe Weiss**, managing partner of Applied Control Solutions, LLC. "When people hear 'cybersecurity,' they think data breach," Weiss began. "However the threats from control system cybersecurity that can be literally existential to a country are what merit concern—control system cyber can easily be a poor man's atom bomb."

Weiss's focus is on the importance of "keeping the lights on, the water flowing, the manufacturing lines running, and trains from crashing." Such processes depend on control systems, which monitor and control a process adaptively, autonomously, in real time. Control systems are used to manage pressure, temperature, or radiation; in a manufacturing facility they may regulate the size, shape, or color of a component or product. Chemical plants, water facilities, and nuclear facilities also use control systems. Modern control systems are now tightly integrated with cyber infrastructures and smart sensor technologies, a complex cyber-physical system posing more R&D challenges in providing critical infrastructure security.

"Security is a three-legged stool, consisting of physical security, IT security, and control systems security," said Weiss. Not much progress has been made in terms of security on the control systems front. While working at the Electric Power Research Institute, Weiss traveled to cybersecurity conferences all over the world and found that most of the conversation was focused on password protection policies and intrusion detection logs—the business side of the utility—rather than the "lights on, water flowing" operational security he prioritized. During his long career, Weiss said he has seen minimal improvements made to the cybersecurity of control system field devices.

"Anyone who thinks the U.S. power grid is secure is being badly misled," Weiss said. "There have already been more than 250 control system cyber incidents and 5 major cyber-related outages in the United States—each affecting at least 90,000 customers—but none was identified as a cyber event." Weiss has compiled a database that now contains over 800 control system cyber incidents. According to his analyses, there have been more than 60 control system cyber incidents to date that have injured or killed people—over 1,000 deaths so far—but none of these incidents has been identified as a cyber incident, Weiss said.

Weiss noted limitations in the regulatory scheme for cybersecurity at power plants. "The electrical distribution system is not covered by the Federal Energy Regulatory Commission's cybersecurity standards, and the North American Electric Reliability Corporation's standards only apply to plants that generate at least 1,500 megawatts at an individual site—leaving at least 80 percent of the non-nuclear power plants in North America outside the scope of the standards."

Weiss explained that the Department of Defense (DOD) is working with utilities, providing them with Aurora hardware mitigation devices.[1] The utility collects and sends data to DOD, which analyzes it and sends the information back to the companies. But few utilities are working with DOD to implement the Aurora hardware solutions. "We need to figure out how best to partner to make this work," he continued. "A cross-disciplinary organization is needed—one involving operations, maintenance, engineering, IT, telecom, forensics, risk, as well as public relations people to inform the public when something happens. Control system security needs to be funded and overseen with the same rigor as for IT. Cybersecurity policies and metrics are also needed," said Weiss.

Weiss closed by encouraging GUIRR members to help by treating control system cybersecurity with as much importance as IT security, participating in industry-government efforts to shape cybersecurity for industrial control systems, and sharing information with others. Weiss concluded, "Europe has an information-sharing program within end user communities, and there is no reason why the United States cannot develop the same type of program. ...This is not an individual industry problem, or a North American problem. Control systems are used to manage, command, direct, or regulate other devices or systems worldwide."

NATIONAL PLAN FOR CRITICAL INFRASTRUCTURE SECURITY

The first presentation on February 24 was offered by **Bob Kolasky** of the Department of Homeland Security's Office of Infrastructure Protection. Kolasky, who played a large role in rewriting the current National Infrastructure Protection Plan, noted that the challenge is to build a required apparatus for sharing information between government and non-government entities, while not being overtaken by that same apparatus. He suggested that the structure of the National Infrastructure Protection Plan was aimed to enable this.

Current national policy on critical infrastructure security and resilience is rooted in a presidential directive signed in 2013 by President Obama, who on the same day signed an Executive Order on cybersecurity for critical infrastructure, explained Kolasky. "Those two documents asked us to evaluate the public-private partnership for critical infrastructure to see what was working," said Kolasky, who led DHS's efforts to implement the documents. In collaboration with industry and other levels of government, his office conducted the evaluation and published it in the summer of 2013. Based on that publication, the National Infrastructure Protection Plan was updated later that same year.

"As this process was happening, the Office of Infrastructure Protection was also working with the National Institute for Science and Technology to develop a cybersecurity framework intended to update information-sharing processes and to guide organizations and industry in making risk management decisions," said Kolasky. "There was a high level of interest from industry in helping to define the approach to cybersecurity, and industry had a strong incentive to demonstrate that a voluntary partnership could work. After considering regulatory options, the administration made a commitment to do as much as possible through voluntary mechanisms."

Those involved in developing the national plan were primarily the government agencies and industry linked to 16 critical infrastructure sectors identified (see Figure 1) in the 2013 presidential directive, including commercial

Figure 1. Critical infrastructure sectors. Source: Bob Kolasky's presentation at the February 23-24, 2016 GUIRR meeting.

1 In a presentation made at IEEE PES 2011 General Meeting Super Sessions in July, 2011, Aurora was defined as "a gap in protection which has the following characteristics: 1) Out-of-synch, open/close sequence of 1 or more breakers; 2) Induced torques can cause permanent damage to the generator; 3) Open/close as fast as 10 to 15 cycle, i.e., traditional protection will not trip (gap); 4) Physical/Cyber attack." Source: "Aurora Vulnerability: Issues & Solutions Hardware Mitigation Devices," June 2011, Quanta Technology. https://www.smartgrid.gov/document/aurora_vulnerability_issues_solutions_hardware_mitigation_devices_hmds.

facilities, communications, dams, chemicals, and nuclear reactors. The effort also included state and local officials, regional consortiums, academia, and nongovernmental organizations. Fifteen of the 16 sectors have created self-governing organizing counsels where industry can collaborate to reduce vulnerabilities and share information, said Kolasky.

"The National Infrastructure Protection Plan is not a detailed strategic plan with milestones and a program management plan," stated Kolasky. "The complex environment doesn't allow for a plan in which someone is in charge and everyone is assigned particular things to do. Most of the time, DHS's role is to provide support to owners and operators who are making decisions about what is best for their infrastructure. The agency tries to enable information sharing and to create incentives to reduce barriers, and hopes that industry is making decisions to elevate their security and resilience. There are times when we are not confident that adequate steps are being taken, and then we explore policy options for other ways to exert influence. And in certain circumstances, the federal government will play a leadership role—where there is an imminent threat, for example, or in the middle of an incident."

Kolasky offered a brief overview of the National Infrastructure Protection Plan's vision and goals, which include assessing and analyzing threats (see Figure 2), vulnerabilities, and consequences; encouraging securitythat will deal with a number of risks; and enhancing critical infrastructure resilience. The plan also includes a call to action that encourages building on existing partnerships, innovating in managing risks, and focusing on outcomes.

Figure 2. Evolving threats to critical infrastructure. Source: Bob Kolasky's presentation at the February 23-24, 2016 GUIRR meeting.

"At the end of the day, we are trying to have pre-existing information-sharing interactions in place, so that when problems do happen, we can work together," he concluded.

The next presentation was given by **Margaret Grayson** of DHS's National Infrastructure Advisory Council (NIAC), which was founded in 2002. She began by noting that her comments were her own as a private citizen, and also pointed to the availability of NIAC's report on its recommendations for a National Research and Development Plan on DHS's NIAC website.

"The question of what R&D we, as a country, should invest in is critically important," said Grayson. "Many of the recommendations that came out of the 1998 presidential directive on critical infrastructure protection have still not been implemented. Information on vulnerabilities has been gathered and shared, but little action has been taken. We now need to move to action, and that will require the involvement of all stakeholders, public and private."

"More than 80 percent of the nation's critical infrastructure is owned and operated by private industry, and so government has mostly been in a supporting role, providing and facilitating a forum for people to work within," she continued. One of the first initiatives NIAC worked on was fostering the ability to talk to one another. DHS's Critical Infrastructure Partnership Advisory Council (CIPAC) opened a forum where infrastructure experts could discuss vulnerabilities and risks they discovered without worrying that these vulnerabilities would be exposed or wind up on the front page of *The New York Times*.

NIAC's recent report presented six fundamental strategic drivers for research and development requirements—including dependency and interconnectedness of cyber systems, aging infrastructure, evolving terrorist and physical threats, and evolution in workforce requirements—and outlined recommendations, many of which address barriers that are standing in the way of action. "We need to look at legislation and policy and set aside what no longer works," said Grayson. "For example, if antitrust laws are preventing companies from working together, how do we change the legislation so that that doesn't happen? Universities, industry, and government can work together to see what aspects of the regulatory framework used to make sense but are no longer working.

Given what we now know about sea-level rise, for example, does it still make sense to have a policy requirement that a building's critical operating systems need to be located in the basement?" She also noted that much of the country's critical infrastructure is aging. "How can

we take structures that are 50 or 100 years old and bring them into new technology areas? Our workforce is aging as well; the people who understand these infrastructure systems—how to run them and how to keep them safe—are reaching retirement age. This is another area for study and investment."

Grayson stressed that the growing complexity of the cross-sector interdependence could not be overstated. "Those sectors depend on each other, and our economy depends on them being safe, secure, and resilient. The responsibility of government to its citizens is to make sure that happens, but the infrastructure is owned by the private sector—which means that public-private partnerships are extremely important."

MODELING POTENTIAL THREAT AND IMPACT SCENARIOS

The next panel examined the modeling of potential threat and impact scenarios. The panel included four speakers, whose presentations are summarized below.

Brandon Wales of DHS's Office of Cyber and Infrastructure Analysis (OCIA) offered the first presentation, focusing his remarks on infrastructure modeling and its associated challenges. OCIA uses tools such as modeling to understand infrastructure and what happens when there are disruptions and failures, and then provides that information to decision makers (see Figure 3).

Some of the office's work involves collaborating with other federal, state, and local agencies and the private sector to model scenarios that can inform planning for infrastructure disruptions. For example, OCIA worked with Federal Emergency Management Agency regions along the west coast to model the effects of an earthquake and tsunami on coastal infrastructure and to understand how long it would take to restore services. This knowledge can help the agencies know where to position equipment. "We also generally try to model two hurricane scenarios every year and keep those accumulated scenarios on the shelf, and we can pull those if a situation similar to a modeled scenario emerges," said Wales.

OCIA also studies infrastructure dependencies—"some of which is easy, and some of which is hard," Wales explained. "The office has worked to model dependencies between water and electric power, for example, in order to see how an extended drought affects power generation and supply.

With Hurricane Sandy our modeling failed us because we did not know about the existence of a particular transmission line between a power generation plant and a substation. To fully understand a scenario, you need very granular, specific information, and it is challenging to extract those minute details that may matter very much in a critical situation."

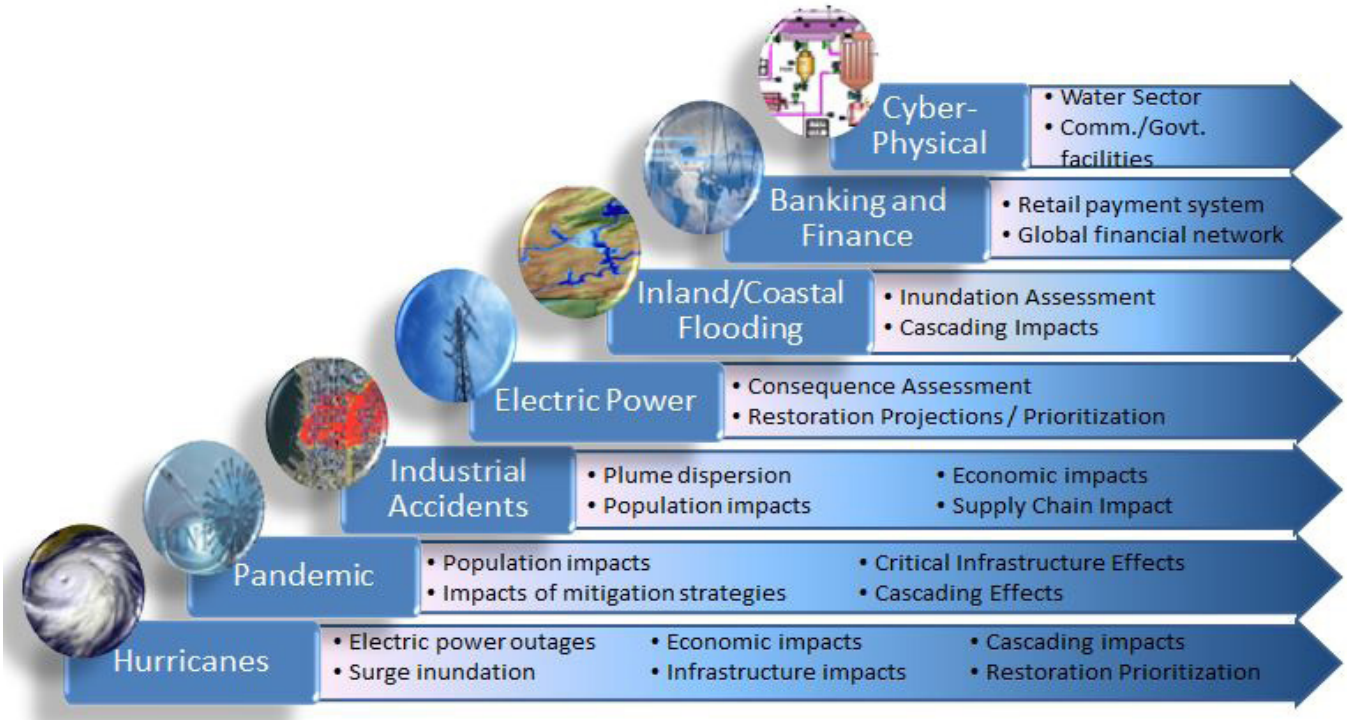

Figure 3. OCIA analytic evolution. Source: Brandon Wales' presentation at the February 23-24, 2016 GUIRR meeting.

According to Wales, modeling supply chains is probably the most complex thing OCIA does. If there is a disruption at a refinery or a pipeline or terminal, the plan that follows must consider how the disruption will affect the supply of transportation fuels, where the likely shortages will occur, and how long they will last.

OCIA has been working with national lab partners on the democratization of modeling so that non-experts can use these models to advance understanding of critical infrastructure. The office also wants to enhance its ability to build uncertainty into its models so it can provide information about uncertainty to decision-makers as necessary.

"Modeling is not easy," said Wales. He tells his analysts, "We want to be bold, but we need to be humble." This is a challenging effort, and while the office is not expected to predict perfectly, "We need to provide our decision-makers with improved information every day," Wales concluded.

Lori Parrott of Sandia National Laboratories spoke next, focusing her remarks on the role played by a federally funded R&D center in government-university-industry partnerships. "Federally funded research and development centers (FFRDCs) such as Sandia have unique resources to bring to these partnerships," said Parrott. "As an FFRDC, we should only be doing cyber-related work that industry and academia cannot, will not, or should not do—because of the nature of the information, because there is no profit motive, or because there is a critical need that requires our capabilities."

Sandia has a long history in cyber and information assurance, beginning with nuclear weapons, where the lab developed command and control systems to ensure the proper use and prevent unauthorized use of these weapons and technology. That assurance grew into deep capability in understanding how to conduct vulnerability assessments on information and electronic systems.

Sandia's current role is to create national cyber capabilities to support DHS in its mission. The lab does vulnerability assessments of systems for the government, private industry, and other stakeholders. "Our long-term applied research goal is to understand infrastructure risks and engineer solutions to them," said Parrott. "Sandia's own systems are attacked daily by every kind of attacker, so the lab has an exquisite data set on the 'state of the art' of cyberattack, which helps in determining how best to defend systems."

According to Parrott, Sandia has also helped DHS deploy the Cybersecurity Protection System, which includes detection, analytics, information sharing, and protection and response. In addition, the lab develops risk assessment tools for supply chain management, and partners with other DOE labs and federal agencies to help secure critical infrastructure control systems.

Parrott discussed the National Infrastructure Simulation and Analysis Center (NISAC), originally founded by Sandia and Los Alamos national labs and now involving other partners. "NISAC is the only place that has the goal of working across the 16 critical infrastructure sectors. It is very complex and difficult, and a perfect place for work by national labs," she said. "The purpose is to support the government in making decisions and prioritizing investments."

Sandia has branched out and moved toward mathematical and quantitative approaches to try to describe resilience. "We have a methodology trying to understand a systems impact: What is the impact of a disruption on a system's ability to deliver its intended good or service? How can it absorb, adapt, and restore? The lab has quantified those mathematically," stated Parrott.

The next presentation was given by **Matt Bohne**, product cybersecurity leader and chief engineer at GE, who spoke on key attributes of successful public-private partnerships. Bohne described one key attribute: "Is the issue you're focused on enduring and compelling? Will it capture the minds and hearts of the people involved, and will they stay engaged? We have found that if the topic is more generic, the partnership is less likely to work."

Bohne described another important attribute as trust. "Is there the right kind of trust among the people involved, and are the right kinds of people involved? Trust among commercial institutions is particularly challenging; our native tendency in cybersecurity is not to discuss issues with others. To build trust, people need to contribute: a lot of people come to meetings to listen, but not to talk or contribute. It helps to run the partnership like a business, with set expectations for the participants—the value they are expected to bring, and what they are expected to do. In any effort you will have activists, foot soldiers, and voyeurs. You will always have some of the latter, but you don't want too many of them. There should also be mentoring for new members of the partnership."

As an example of a strong public-private partnership, Bohne described a group he has been involved with, the Nuclear Information Technology Strategic Leadership, which has been operating for 20 years. "It endures because it was organized around a strong anchor topic—safety and security—and because there is a high level of trust. Everyone shares their information, because improving safety and

security is in the interest of all. Moreover, it is operated like a functional business; there are regular meetings, and people are expected to show up and to contribute. The partnership also produces useful products—for example, it fields surveys about technologies being used at different plants, and everyone shares in the results."

In closing, Bohne reiterated details to consider when setting up a new public-private partnership, including the importance of starting with a focused topic, setting clear and well-defined goals, focusing and validating trust among the partners, and defining expectations from the start.

The last presentation of the panel was offered by **Iris Tien** of the Georgia Institute of Technology, who studies risk and reliability of infrastructure systems. Much of Tien's work focuses on modeling interdependencies between systems in order to find ways to minimize cascading effects from a failure in one system.

Tien and her research group are using a complex systems modeling approach, and one of the challenges that arises is uncertainty. Tien explained that there are many uncertainties with infrastructure systems, the individual components involved, and the systems that evolve dynamically over time. Tien uses Bayesian networks, which use probabilistic graphs with nodes to represent different variables and with links to reveal dependencies between different nodes. If information is entered into any node, it propagates throughout the entire network. This framework can be used to inform decisions by those responsible for designing, managing, and rehabilitating systems.

In particular, Bayesian networks can be used to model interdependent critical infrastructure systems. Tien and her group are building a multi-scale framework with three layers—individual components, individual infrastructure systems, and a top layer to represent interdependencies (the system of systems). This approach allows them to model interdependencies across the network and identify critical nodes/components in the network. They can model the effects of hazards: If something happens to one component, what are the cascading effects across the systems? The goal is to eventually have interdependent system models that include scales from local to regional to national.

"Opportunities for cross-sector collaboration include collecting more data on real systems, which would allow for more meaningful modeling of threat and impact scenarios," said Tien. "Currently, the lack of data on more real systems means that the same systems get studied over and over again. We should also focus more on the actual threats industry and governments are concerned about and tailor more analysis to examine those threats. In addition, there is an opportunity to improve workforce education, training the people who will work with infrastructure systems to think more broadly." Tien also described future research directions, with focus on subjects including advanced sensing and monitoring, using smart infrastructure that integrates cyber and physical systems, determining automation vs. human involvement in monitoring and managing infrastructure systems, and improving hazard and threat models using historical data.

CONGRESSIONAL UPDATE

The final panel of the meeting offered updates on congressional developments in critical infrastructure security. The first presentation was given by **Kirsten Duncan** of the House Committee on Homeland Security (CHS), which is responsible for authorizing, streamlining, updating, and overseeing DHS programs. Duncan gave an overview of the committee's work in recent years.

Duncan reiterated that DHS's Office of Infrastructure Protection (IP) serves as the sector-specific agency for six critical infrastructure sectors, facilitating public-private partnerships across these sectors, and developing strategic goals to mitigate risk and improve resilience. IP also coordinates across all 16 sectors and provides expertise in critical infrastructure resiliency. IP also operate the National Infrastructure Coordinating Center (NICC)—the 24/7 information-sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government.

When an incident involving critical infrastructure occurs, the NICC serves as an information-sharing hub between DHS and local utilities. In 2014, CHS worked on a number of bills, and by the end of the year had passed five bills which eventually became law:

- The National Cybersecurity Protection Act codified the National Cybersecurity and Communications Integration Center (NCCIC), which provides a platform for the government and private sector to share information about cybersecurit threats, incident response, and technical assistance.
- The Federal Information Security Modernization Act (FISMA) of 2014 updated the FISMA of 2002 to centralize the federal government's cybersecurity management within the Department of Homeland Security. It maintained OMB's role over federal civilian agency information security policies, while delegating authorityto DHS to implement these policies.
- The Cybersecurity Enhancement Act of 2014, on which the committee worked closely with the Science Committee. The bill codified NIST's work

on the cybersecurity framework and ensured that there will be robust industry partnerships as that framework continues to be updated.
- A section of the Border Patrol Pay and Reform Act, which gave DHS expanded authorities to hire cybersecurity professionals.
- A workforce assessment piece that required DHS to conduct an assessment of their cybersecurity workforce every three years and put a strategy in place for recruitment and retention.

In 2015 the committee worked on a few additional bills:
- A bill to codify the National Computer Forensics Institute that provides cyber investigative tools and training to localities and states.
- A piece of legislation that would take the tools that NCCIC already has and make them available to states and localities upon request.
- The Cybersecurity Act, which established DHS's NCCIC as the civilian information-sharing portal for cyber threats and defensive measures.

Nick Leiserson of the office of Rep. James R. Langevin (speaking only for himself, not on behalf of the congressman), then discussed the other congressional areas of interest related to cybersecurity.

"One area of congressional interest concerns encryption. This has been a long-running policy debate, and Congress is considering three major tracks in this area—one potential piece of legislation that would try to clarify the responsibilities technology companies have with respect to providing information to law enforcement; another potential bill that would ban states from banning encryption; and a middle path that would charter a congressional committee to examine this issue with people from law enforcement, academia, and technology companies." Leiserson expressed doubt that any congressional action would be taken on this issue, unless Congress pursued the middle path.

Leiserson also explained that Congress is looking at the breach of personally identifiable information. "Currently, 47 state and territorial laws govern data breach, which makes it difficult in a connected world where a company can have customers in different states. Consensus has not been reached on the details, but the House and Senate each have about five competing proposals. If something major is to come out of Congress on cybersecurity in 2016, it will likely be in this area," said Leiserson.

Congress is also examining how to help facilitate the development of cybersecurity risk modeling and robust cyber insurance, as well as how best to address the shortage of trained cybersecurity professionals. Leiserson suggested that the dialogue on information sharing has distracted Congress's attention from other critical infrastructure cybersecurity issues, recalling that there hasn't been legislation on the topic since several bills were proposed and debated but not passed in 2011. With the passage of the Cybersecurity Act of 2015, Congress is again beginning to consider critical infrastructure protection; however, most of the attention remains on the cyber aspects thereof. "If you think critical infrastructure security outside of cyber security issues should be a legislative focus, you should let your legislators know," said Leiserson.

The final presentation was offered by **Daniel Castro** of the Information Technology and Innovation Foundation, who spoke about where policy around cyber security of critical infrastructure has come from and where it is headed. "It has taken a long time for Congress to pass legislation on information sharing and to propose standardizing the response to data breach across states, and it is good that they have done so, but these actions are low-hanging fruit," said Castro. "The best that Congress has done will not come close to solving the problems we have today."

Castro offered thoughts on why the necessary solutions still feel far off, and how to change the system to enable these changes. "Government is not acting rationally," said Castro. "It is not fixing the problems and vulnerabilities that it knows need to be fixed. Part of this is caused by the culture in government, where it is acceptable to be in an agency where the systems for which you are responsible have vulnerabilities or are failing. We need to change that mentality, through congressional oversight and through hiring practices. And on the private sector side, we need to make it so that it is easy, cheap, and desirable to do cybersecurity well. How do we fix what is currently a fundamental market failure? There is a reason the private sector underinvests in cybersecurity, in part because it doesn't yield enough rewards."

"U.S. policy puts a premium on offensive cybersecurity capabilities—the ability to intercept data and to hack into or shut down systems, domestic or foreign—and pays little attention to defensive capabilities. Although it perhaps sees some interest in protecting some of its own systems, it does not see a lot of value in fixing everyone's cybersecurity. And we see little international cooperation because most countries do not consider it in their interests to improve cybersecurity for everyone."

Castro suggested that to reorient the government strategy around cybersecurity we need to become "cyber-pacifists," switching the focus from offensive capabilities to defense and resiliency, so that the government becomes an active

partner to the private sector in strengthening cybersecurity. "Part of reorienting government strategy must be changing the conversation; if you look at the decisions that have been made about mass surveillance, there was an overreliance on the intelligence community, and the economic considerations and private-sector impact were left off the table."

"We have lost strategic thinking on cybersecurity," said Castro in closing. He argued that the U.S. government had its priorities wrong. "Today the Federal Trade Commission announced a settlement with a company where they agreed to follow a cybersecurity framework and to be subject to greater oversight for 20 years. We are pursuing these measures for a company that makes home wi-fi routers and motherboards, but not for our critical infrastructure, which is much more important to our economy and national security," he said. ■

PLANNING COMMITTEE: **Andrew Reynolds** (Chair), Independent Consultant; **Michele Masucci**, Temple University; **Yannis Yortsos**, University of Southern California. **STAFF**: **Susan Sauer Sloan**, Director, GUIRR; **Megan Nicholson**, Associate Program Officer; **Laurena Mostella**, Administrative Assistant; **Claudette Baylor-Fleming**, Administrative Coordinator; **Cynthia Getner**, Financial Associate.

The summary was reviewed in draft form by **Maria Penedo**, Northrop Grumman and **Wei Wang,** San Diego State University, to ensure that it meets institutional standards for quality and objectivity. The review comments and draft manuscript remain confidential to protect the integrity of the process.

About the Government-University-Industry Research Roundtable (GUIRR)

GUIRR's mission is to convene senior-most representatives from government, universities, and industry to define and explore critical issues related to the national and global science and technology agenda that are of shared interest; to frame the next critical question stemming from current debate and analysis; and to incubate activities of on-going value to the stakeholders. The forum is designed to facilitate candid dialogue among participants, to catalyze and foster follow-on activities, and, where appropriate, to carry awareness of consequences to the wider public.

Government | University | Industry
RESEARCH ROUNDTABLE

For more information about GUIRR visit our web site at http://www.nas.edu/guirr
500 Fifth Street, N.W., Washington, D.C. 20001
guirr@nas.edu