FORUM ON CYBER RESILIENCE

2015 ANNUAL REPORT OF ACTIVITIES

FORUM ON CYBER RESILIENCE
2015 ANNUAL REPORT

MISSION

The Forum on Cyber Resilience is a roundtable of the National Academies of Sciences, Engineering, and Medicine. It was created to facilitate and enhance the exchange of ideas among scientists, practitioners, and policy makers who are concerned with urgent and important issues related to the resilience of the nation's computing and communications systems. The Forum serves as a source of knowledge, insight, and expertise and as a catalyst for stakeholder collaborations. It offers a venue in which to examine and discuss emerging challenges and issues as they become evident. At the same time, as a standing body, the Forum provides a base of engaged, long-term sustained thinking about emerging and future trends as cyber infrastructure challenges, threats, and issues evolve.

CONTEXT AND OPERATIONS

The Forum fosters sustained and candid dialogue among its government, academic, and industry members, and it serves as an independent focal point for honing and refining questions and issues that may not otherwise arise elsewhere or through the traditional Academies study-development process. The Forum is designed to foster activities developed by its members and to advocate for consensus studies or other activities, as needed, to inform its future meetings, and to raise awareness of issues and consequences in the wider public.

The Forum convenes senior representatives from government, universities, and industry to define and explore critical issues that are of shared interest, frame critical questions and needs, and incubate activities of ongoing value to participants. Broad themes it addresses include:

- traditional notions of cybersecurity and trustworthiness, such as maintaining security in the face of attacks, resistance to degradation, and the ability to recover from adverse events,
- ways to foster resilience in the face of natural and man-made disasters, disruptive technological change, and diverse and dynamic user populations,
- how to sustain capacity for innovation and adaptation, and
- ways to reflect the values—such as privacy, openness, trust, expression, usability, dignity, access—and needs of many stakeholders.

The Forum will engage the policy community and multi-disciplinary research communities, along with industry practitioners, those who support and maintain critical infrastructure, and the broader public. One of the Forum's strengths lies in its convening power—the reputation of its members and of the Academies will attract key stakeholders to its activities. As an Academies convening body, the Forum offers opportunities to bring experts and practitioners together who may not otherwise get a chance to interact, to share insights across sectors and across communities, and to invite public participation in activities. The Forum serves as a vehicle for framing new research questions, connecting stakeholders with needed expertise, and enhancing communication and understanding between sectors and disciplines. It is often in the intersections between areas and between disciplines where some of the most innovative thinking occurs. So a key goal of the Forum is to surface and explore insights related to the broad challenge of cyber resilience in ways that help change the conversation around these

topics in productive ways. The Forum also works as an objective, technically-grounded, and technically-rigorous body, to help clarify the option space for policymakers.

MEMBERSHIP

The scope of the Forum is broad, encompassing technology and engineering as well as associated social and policy challenges. Accordingly, the membership consists of senior experts from a variety of disciplines, with a broad range of expertise, who represent a number of institutional perspectives and who can help lay a strong foundation for the roundtable to persist as a standing body. Forum activities span 3 axes of interest: ranging from immediate challenges to strategic long-term challenges related to infrastructure and resilience; from practical or operational needs to basic research; and from technical issues to social and policy issues:

IMMEDIATE CHALLENGES	<---------->	STRATEGIC THINKING
PRACTICAL/OPERATIONAL	<---------->	RESEARCH
TECHNICAL	<---------->	SOCIAL/POLICY/ORGANIZATIONAL

The Forum membership was appointed with these axes in mind, and it includes experts and practitioners from academia and the private sector, along with ex-officio members from federal agencies (the National Science Foundation, the National Security Agency, and the National Institute for Standards and Technology). Forum members have backgrounds in law, policy, ethics, computer science and engineering, and cybersecurity.

Fred B. Schneider, a member of the National Academy of Engineering and Samuel B. Eckert Professor of Computer Science at Cornell University, was appointed as the inaugural chair of the Forum.

Membership will be periodically updated or expanded and membership will rotate over time.

FORUM MEETINGS & ACTIVITIES

In its inaugural year, the Forum on Cyber Resilience met twice (April 6-7 and August 11-12) to develop objectives and to plan activities. Early discussions and interviews with members led to the development of a working list of potential future topics and activities. Here is that preliminary list of themes to explore over time:

- Defining cyber resilience and learning through analogies to other domains
- Implications of cyber dependence and choices to manage risk and degrees of dependence
- Tactical approaches that could help today
- Challenges and opportunities for public-private information sharing
- International norms and boundaries
- Internet governance and implications for network resilience
- Hardware and the supply chain
- Social values and institutional practice
- Affording confidence and engendering trust in systems
- A variety of potential case studies to examine in more depth
- Emerging and potential research topics

The Forum's initial activity included several conversations with individual experts and policymakers, along with beginning to develop relationships with other organizations.

Expert Inputs & Dialogues

The Forum engaged with a number of experts about a wide range of topics during its first year.

April 2015 (Inaugural Meeting)

To kick off discussions, **NAE President C. Dan Mote** spoke at the Forum's inaugural meeting in April, urging this new roundtable to lead, seed, and disseminate transformative thinking about cyber resilience. In addition, at that meeting, members participated in panel presentations on the following topics:

- today's dynamic cyber landscape;
- social values—embedded in systems and reflected in policy; and
- affording confidence and trust in systems.

Forum member **Richard Danzig** presented key insights from his 2014 paper, *Surviving on a Diet of Poisoned Fruit: Reducing the Risks of America's Cyber Dependencies* in a public session.

August 2015

Surveillance, transparency, and trust were among the themes that the Forum identified as potential areas to explore. To seed its discussions and thinking about these and related topics, the Forum convened a session at its August meeting to hear from internal and external experts about recent, related activities.

- **Robert Sproull** (NAE, outgoing CSTB Chair, and Chair of the CSTB Study Responding to Section 5(d) of Presidential Policy Directive 28: The Feasibility of Software to Provide Alternatives to Bulk Signals Intelligence Collection) shared an overview of a recent CSTB study along with his perspective on related topics;
- Forum member **Peter Swire** shared insights from his experience as a member of the Presidential Review Group on Intelligence and Communications Technologies; and
- Forum member **Fred Cate** provided an overview of an Academies workshop he chaired that addressed privacy for the intelligence community-emerging technologies, academic and industry research, and best practices.

Forum members will continue to identify topics to be discussed, and with whom; what the Forum might do to catalyze these discussions; and how the Forum can best facilitate productive engagement between stakeholders.

The Forum invited **William Newhouse**, cybersecurity advisor at NIST, to the August meeting to provide an update on federal cybersecurity research and development efforts and an overview of the interagency process for developing and updating the federal cybersecurity research strategy. Also at the August meeting, to learn more about the federal research agenda in cybersecurity, privacy, and cyber resilience, the Forum visited **researchers at the National Security Agency**. Topics discussed there included mobile security and the security and resilience properties of the emerging Internet of Things.

To begin to explore cyber-resilience issues in the regulatory and civilian agency context, the Forum welcomed **Federal Trade Commission Commissioner Julie Brill** to its August meeting. Commissioner Brill spoke about FTC activities and perspectives on security, privacy, and the Internet of Things. That led to a lively discussion that was part of the impetus for the development of a workshop on a data breach aftermath and recovery that the Forum is planning for 2016.

The Forum anticipates and welcomes additional interactions with policymakers on a range of topics over time.

Multidisciplinary Interactions

The Forum is the first roundtable to be developed by the Academies' **Computer Science and Telecommunications Board** (CSTB). A pioneer in exploring Internet and information technology policy, CSTB convenes the nation's foremost computer science, telecommunications and information technology experts. The Forum on Cyber Resilience draws on CSTB's nearly three decades of foundational work in cybersecurity, privacy, and IT systems and is designed to leverage that and other Academies' work. Forum and CSTB members and staff collaborate closely to ensure alignment of the work of both.

***

The Forum has also started interacting with other groups. At its first meeting, the Forum was briefed by **Cameron Oskvig**, director of the **Federal Facilities Council** (FFC) and by FFC member **Darryl Haegley**. FFC is grappling with the challenge of cybersecurity and cyber-resilience for federal facilities. FFC's mission is to identify and advance technologies, processes, and management practices that improve the performance of federal facilities over their entire life-cycle, from planning to disposal. FFC identified cybersecurity of federal facilities as a priority area for them to address in 2015. Forum members provided input and suggestions on how to effectively address the resilience challenge in that domain.

In addition, during the summer of 2015, **a small working group of the Forum** conducted a series of telephone interviews to further examine the challenge of cybersecurity for facilities. This group worked with staff to find private sector experts in domains, such as healthcare (hospitals), hospitality & entertainment (hotels, theme parks, large event venues, museums), finance (banks), and cloud service providers (datacenters), and then to frame questions to be explored. Through a series of informal conversations with these experts, the sub-group and staff collected insights and impressions about the state of facilities security, and available tools, practices, and models. The subgroup presented a summary of what they learned from these interviews at the Forum's August meeting.

***

The Forum is working with the Academies' Health and Medicine Division and its **Board on Health Care Services** to explore the topic of health IT and cybersecurity. A small steering group has been convened that includes cybersecurity experts and healthcare experts. That group will plan and host a planning meeting in 2016 to bring together up to 20 experts who will discuss current challenges and policy issues in the cybersecurity of health information technology and who will consider whether the Academies could be of assistance in improving the security of health IT through a consensus study or other activities.

***

The Forum can serve as a guide and resource for other groups within the Academies grappling with tough cyber-resilience issues within particular domains. Such interactions will also provide fodder for the Forum's own strategic thinking.

OUTREACH

The Forum's website is **www.cyber-forum.org**. Members of the public who would like to be notified of upcoming Forum activities and meetings are invited to contact staff or to subscribe directly to an email list there.

In addition to core activities, the Forum is open to requests for potential collaboration. For example, the Forum could assist in making stakeholder connections, identifying experts, providing input to other activities, or disseminating information. Possible collaboration mechanisms include coordinating small stakeholder meetings, convening working groups, or co-organizing workshops.

The Forum is interested in hearing from the broader community about key cyber resilience topics and questions to address in its core work. Queries, requests, and ideas may be sent to the Forum at cyberforum@nas.edu.

For more information about the Forum and upcoming activities, see www.cyber-forum.org. The Forum on Cyber Resilience is sponsored by the National Science Foundation and the National Security Agency on behalf of the Special Cyber Operations Research and Engineering Interagency Working Group.

Dr. Fred Schneider, *Chair, NAE*
Samuel B. Eckert Professor of Computer Science
Department of Computer Science
Cornell University

Dr. Anita Allen
Vice Provost for Faculty
Henry R. Silverman Professor of Law and Professor of Philosophy
University of Pennsylvania

Dr. Bob Blakley
Global Head of Information Security Innovation
Citigroup

Fred Cate
Distinguished Professor and C. Ben Dutton Professor of Law
Maurer School of Law
Indiana University

Dr. David Clark, *NAE*
Senior Research Scientist
Computer Science and Artificial Intelligence Lab
Massachusetts Institute of Technology

Hon. Richard Danzig
Senior Advisor
Center for a New American Security

Dr. Eric Grosse
VP Security and Privacy Engineering
Google, Inc.

David A. Hoffman
Director of Security Policy & Global Privacy Officer
Intel Corporation

Paul Kocher, *NAE*
President and Chief Scientist
Cryptography Research, Inc.

Dr. Tadayoshi Kohno
Short-Dooley Professor, Department of Computer Science and Engineering
University of Washington

Dr. Butler Lampson, *NAS, NAE*
Technical Fellow
Microsoft Corporation

Steven B. Lipner
Independent Consultant

Deirdre K. Mulligan
Associate Professor, School of Information
University of California, Berkeley

Tony Sager
Senior VP
Center for Internet Security

Dr. William H. Sanders
Department Head and Donald Biggar Willett Professor of Engineering
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Peter Swire
Nancy J. and Lawrence P. Huang Professor of Law and Ethics, Scheller College of Business
Georgia Institute of Technology

Mary Ellen Zurko
Principal Engineer, Security Business Group
Cisco Systems

Ex Officio Members:

Donna Dodson
Chief Cybersecurity Advisor
National Institute for Standards and Technology

William "Brad" Martin
Research Advisor to the National Security Agency
Director's Special Assistant for Cyber
National Security Agency

Keith Marzullo
Director, National Coordination Office for Networking and Information Technology Research and Development

Forum Staff:
Lynette I. Millett, Director, Forum on Cyber Resilience, & Associate Director, CSTB
Emily Grumbling, Program Officer, CSTB
Shenae Bradley, Administrative Assistant, CSTB