FORUM ON CYBER RESILIENCE

2018 ANNUAL REPORT OF ACTIVITIES

FORUM ON CYBER RESILIENCE
2018 ANNUAL REPORT

MISSION

The Forum on Cyber Resilience, established by the National Academies of Sciences, Engineering, and Medicine in 2015, facilitates and encourages the exchange of ideas among scientists, practitioners, and decision-makers concerned with the resilience of computing and communications systems, including the Internet, critical infrastructure, and cyber-physical systems, that support societally important functions. The Forum is a multi-disciplinary group comprised of approximately 20 senior scholars, industry leaders, and government experts who represent a range of technical, legal, policy, and other disciplines.

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.

The Forum holds meetings and convenes workshops and discussions with the following goals:

- Improve cyber resilience and the strength and vitality of information and communications infrastructure;
- Facilitate and enhance the exchange of ideas among scientists, practitioners, and policy makers concerned with urgent and important issues related to cyber resilience and sustaining a vibrant and effective information and communications infrastructure;
- Identify and engage the key challenges and opportunities for achieving greater cyber resilience and a more robust information and communications infrastructure that maintains room for continued innovation and reflects the values and needs of its many, diverse stakeholders;
- Explore and engage with the research community on the technical challenges that underlie operational and policy issues and identify important research problems.

The Forum engages 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 attracts 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. 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 members are appointed by or on behalf of the chair of the National Research Council, generally for staggered one or two three-year terms. The Forum membership currently consists of 21 experts in computer science, software engineering, and related technical and social science research disciplines, legal and technical experts in cybersecurity and privacy, experts in design, human-computer interaction, and organizational and social implications of infrastructure, individuals with insight into private sector information infrastructure security and reliability requirements, and individuals with insight into similar government needs (to include both defense/military needs and civilian agency requirements). Membership is balanced among academic, private sector, and public sector perspectives. New members are added annually, and suggestions and nominations are solicited regularly from current members, sponsors, workshop speakers, CSTB, the NAE and the NAS, and others in the community. Members are appointed under National Academies' roundtable processes and the membership is regularly overseen and approved by the National Academy of Sciences President.

The Forum and its activities are supported by professional and administrative staff in the National Academies' Division on Engineering and Physical Sciences. They plan Forum meetings; interact regularly with Forum members, sponsors, and other experts and stakeholders; draft, edit, and publish workshop summaries and other Forum products; and manage travel and logistics.

FORUM MEETINGS & ACTIVITIES

The Forum on Cyber Resilience met in person three times in 2018 for Forum meetings (February 8-9, June 5-6, and October 3-4) to engage with experts, host workshops, and plan activities

Forum activities connect experts and stakeholders across disciplines and sectors, provide a sounding board for leaders of other cybersecurity studies and programs, explore topics in depth and put information and insights into the public record, and affect the practice and research activities of those who participate in its activities. They provide opportunities for informal discussion with and among private sector participants and government officials in a neutral setting. They engage the public through workshops and other public sessions. Forum members also meet with and brief stakeholders on ongoing activities and discussions.

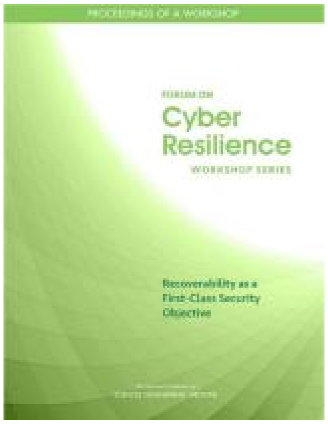
The Forum also advises and supports other cyber resilience-related Academies activities through a variety of interactions with other Academies groups and activities. Illustrating the increasing urgency of these topics and their multidisciplinary nature, the Forum has already had substantive interactions with each of the National Academies' major program divisions—covering earth and life sciences, behavioral and social sciences and education, engineering and physical sciences, health and medicine, transportation, and policy and global affairs. Forum discussions provide input to and spin-off separately organized workshops and studies. Forum members suggest topics and experts to participate in these activities, and routinely serve as committee members and peer reviewers.

The Forum convenes 1 or 2 public workshops and symposia each year on topics identified by its members (including sponsors). The goal is to push the conversation 'beyond the headlines' and to surface critical and sometimes unanticipated policy implications as well as technical research questions.

Expert Inputs, Workshops, Activities, & Dialogues

The Forum engaged with a number of experts about a wide range of topics during its third year and hosted two public workshops. Each meeting provided opportunities to further advance strategies and plan for future Forum activities, and to engage around previously identified themes of interest.

February 8-9



PROCEEDINGS OF A WORKSHOP

FORUM ON Cyber Resilience WORKSHOP SERIES

Recoverability as a First-Class Security Objective

The February meeting featured a public workshop on Recoverability as a First-Class Security Objective. The workshop featured presentations from experts in industry, research, and government roles who spoke about the complex facets of recoverability—that is, the ability to restore normal operations and security in a system affected by software or hardware failure or a deliberate attack. Speakers included: **Heather Adkins** (Google), **Matthew Barrett** (NIST), **Steve Cauffman** (NIST), **Richard Danzig** (Johns Hopkins University Applied Physics Laboratory), **Dave Edelman** (Citigroup), **Butler Lampson** (Microsoft), **Tim Roxey** (North American Electric Reliability Corporation), **Steve Schmidt** (Amazon), and **Fred Schneider** (Cornell University).

The workshop resulted in the publication of *Recoverability as a First-Class Objective: Proceedings of a Workshop.*[1]

In addition to hosting the public workshop, the Forum invited **Robert Axelrod**, University of Michigan, to speak on cyber norms from a political science perspective. **Travis Breaux**, Carnegie Mellon University, joined the Forum to discuss topics and activities related to technologically mediated misinformation and disinformation at scale. **Vinh Nguyen**, Office of the Director of National Intelligence, also spoke on cyber challenges from a national intelligence and national security perspective. **Fred Chang**, Southern Methodist University and co-chair of the Intelligence Community Studies Board met with the Forum to explore overlapping topics of interest related to artificial intelligence and cybersecurity.

June 5-6

During the June meeting, the Forum heard from **Richard J. Harknett**, University of Cincinnati regarding his piece in *Lawfare* titled "United States Cyber Command's New Vision: What It Entails and Why It Matters." **Jeanette Manfra**, Department of Homeland Security, spoke regarding programs and initiatives under the Office of Cybersecurity and Communications.

October 3-4

The October meeting featured a public symposium, *Beyond Spectre: Confronting New Technical and Policy Challenges*. The symposium brought together researchers, public and private sector stakeholders, along with other experts to explore the technical and policy implications of newly-discovered computer hardware flaws, including Spectre and Meltdown. Speakers included: **Brandon Baker** (Google), **Ernie Brickell** (independent security researcher), **Galen Hunt** (Microsoft), **Paul Kocher** (independent researcher), **Katie Moussouris** (Luta Security), **Andrew Myers** (Cornell University), **Audrey L. Plonk**

[1] National Academies of Sciences, Engineering, and Medicine. 2018. Recoverability as a First-Class Security Objective: Proceedings of a Workshop. Washington, DC: The National Academies Press. https://doi.org/10.17226/25240.

(Intel), **Mark Ryland** (Amazon), **Fred Schneider** (Cornell University), **Ari Schwartz** (Venable, LLP), and **Paul Waller** (National Cyber Security Centre, United Kingdom). A summary proceedings of the symposium will be published in early 2019.

In addition to hosting the symposium, the Forum invited **Katherine Charlet**, Carnegie Endowment for International Peace, to discuss cyber norms in a global context and coping with strategic information campaigns. **Rosalyn W. Berne**, who directs the Center for Ethics and Society at the Nation Academy of Engineering, spoke about the importance of keeping ethics and human values at the forefront of technology design.

***

Forum members and staff contributed to or participated in several other National Academies' activities in 2018. Forum chair **Fred Schneider** is a member of both the Computer Science and Telecommunications Board and the Naval Studies Board, and he regularly engages with the Intelligence Community Studies Board. Schneider also participated in a security dialogue with Russia on issues related to cyber and space security with the Academies' Committee on International Security and Arms Control. Forum director **Lynette Millett** is assisting the Board on Life Studies with a study on safeguarding the bioeconomy.[2] Forum Member **Bob Blakley** was a member of the study committee that produced the report *Quantum Computing: Progress and Prospects*[3]. Forum Member **David Vladeck** served as review monitor for the report *Securing the Vote: Protecting American Democracy*.[4] Forum member **Fred Cate** chaired and Forum members **Steven Lipner**, **Susan Landau**, and **David Hoffman** served on the study committee that produced *Decrypting the Encryption Debate: A Framework for Decision Makers*. **Emily Grumbling** is planning to develop and help lead a new steering committee to examine Implications of Artificial Intelligence for Cybersecurity.[5]

The Forum anticipates and welcomes additional interactions with stakeholders on a range of topics over time. Its working list of potential future topics and activities includes:

- Multi-party vulnerability disclosure challenges
- Cyber resilience of the electric grid
- Artificial intelligence in adversarial contexts
- Cybersecurity challenges and the bioeconomy
- Cyber policy graduate education
- Consumer information and protection for Internet of Things devices
- Resilience to and coping with disinformation
- Attribution and public trust
- Vulnerability disclosure and vulnerability equities
- Cyber norms in a global context
- Cybersecurity in regulated industries
- Financial services sector infrastructure
- Implications of AI to cybersecurity

[2] See the website for the project, "Safeguarding the Bioeconomy: Finding Strategies for Understanding, Evaluating, and Protecting the Bioeconomy while Sustaining Innovation and Growth " at http://nas-sites.org/dels/studies/bioeconomy/

[3] National Academies of Sciences, Engineering, and Medicine. 2018. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196.

[4] National Academies of Sciences, Engineering, and Medicine. 2018. Securing the Vote: Protecting American Democracy. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.

[5] For more information, see: http://sites.nationalacademies.org/CSTB/CurrentProjects/CSTB_188827

CONNECTING WITH THE FORUM

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.

During 2018, the Forum also engaged with several other groups within the National Academies and with several government groups to explore topics of mutual interest. National Academies groups including the Board on Mathematical Sciences and Analytics, the Board on Energy and Environmental Systems, the Board on Life Sciences, the Naval Studies Board, the Intelligence Community Studies Board, and the National Academy of Engineering's Center for Ethics and Society. Agencies and government groups the Forum interacted with included the National Institute of Standards and Technology, the National Science Foundation, the National Security Agency, United States Government Accountability Office, the United States Department of the Treasury, Office of the Director of National Intelligence, and the United States Department of Homeland Security.

***

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

***

Ways to connect with the Forum on Cyber Resilience include:

- **Subscribe to the Forum's Mailing List**
  Visit our website at nas.edu/cyber to sign up for news and updates regarding Forum activities.

- **Attend a Forum Event**
  The Forum hosts 1-2 workshops each year on topics a range of topics related to cyber resilience.

- **Share Your Expertise**
  Help advance our work by speaking at a Forum event or reviewing a workshop report.

- **Collaborate with the Forum**
  Cyber resilience is a multidisciplinary, multi-sector challenge and we welcome collaboration. Mechanisms include coordinating stakeholder meetings, convening working groups, and co-organizing workshops.

- **Become a Sponsor**
  We appreciate the support of our founding sponsors and invite additional support for our ongoing portfolio of activities. Sponsors can contribute towards a specific activity or the Forum as a whole.

***

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, the National Security Agency with assistance from the Office of the Director of National Intelligence, and the National Institute of Standards and Technology.

MEMBERSHIP OF THE FORUM ON CYBER RESILIENCE
as of December 31, 2018

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

Dr. Anita Allen, NAM
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
Independent Consultant

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

Paul Kocher, NAE
Independent Researcher

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

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

Susan Landau
Bridge Professor
Fletcher School of Law & Diplomacy and School of Engineering,
Department of Computer Science
Tufts University

Steven B. Lipner, NAE
Executive Director
SAFECode

John Manferdelli
Professor of the Practice
Executive Director - Cybersecurity and Privacy Institute
Northeastern University

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

David Vladeck
Professor of Law
Georgetown University Law Center

Mary Ellen Zurko
MIT Lincoln Laboratory

Ex Officio Members:

Donna Dodson
Chief Cybersecurity Advisor
National Institute for Standards and Technology

Jeremy Epstein
Assistant Director, Computer and Information Sciences and Engineering
National Science Foundation

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

Staff:
Lynette I. Millett, Director
Emily Grumbling, Program Officer
Katiria Ortiz, Associate Program Officer
Shenae Bradley, Sr. Program Assistant