Final Technical Report

Award DE-SC0016751

Support for the Core Research Activities and Studies of the Computer Science and Telecommunications Board

Principal Investigator: Dr. Jon K. Eisenberg, Director CSTB, 500 5th St, NW, Washington DC 20001
Recipient Organization: National Academy of Sciences, 500 5th St, NW, Washington, DC 20001
Period of Performance 7/15/2016-7/14/2019
Submitted by: Jon K. Eisenberg

Abstract

This award provided partial support for the operation of the Computer Science and Telecommunications Board. This included planning, organization, and agenda preparation for twice-annual board meetings; selection and organization of topical sessions at board meetings; identification and recruiting of outside speakers; and identifying and recruiting new board members from academia and industry.

A number of study reports or related materials were enabled in part by support under this award (and largely funded through separate project-specific awards):

In 2018: Quantum Computing: Progress and Prospects, which assesses the current progress and possible future pathways towards developing a general-purpose quantum computer as well as its potential implications; Recoverability as a First-Class Security Objective, which summarizes presentations and discussions from a Feb. 2018 Forum on Cyber Resilience workshop on how to restore normal operations and security following an attack or failure of software or hardware; Securing the Vote: Protecting American Democracy, which recommends steps that the federal government, state and local governments and election administrators can take to make elections more secure, accessible, reliable, and verifiable; Opportunities from the Integration of Simulation and Data Science: Proceedings of a Workshop, which examines current and emerging science applications that span simulation and data-driven science, their characteristics, and future approaches for cyberinfrastructure to support them; Data Science for Undergraduates: Opportunities and Options, which offers a vision for the emerging discipline of data science at the undergraduate level and outlines considerations and approaches for academic institutions and others to help guide the ongoing transformation of the field; and Decrypting the Encryption Debate: A Framework for Decision-Makers, which proposes a framework for evaluating proposals to provide authorized government access to the plaintext of encrypted communications and stored data.

In 2017: Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions, which explores how a more effective national alert and warning system might be created and sets forth a research agenda to advance the nation's alert and warning capabilities; Software Update as a Mechanism for Resilience and Security: Proceedings of a Workshop, which summarizes discussions at a workshop organized by the Cyber Resilience Forum exploring practices, mechanisms, policies, and technologies; Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions, which focuses on foundational research strategies and on building collaborative links across disciplines and between research and practice; Information Technology and the U.S. Workforce: Where are We and Where do We Go from Here?, which explores current and emerging information technology capabilities and their interplay with various dimensions of work, and highlights areas where new research and data would help to improve understanding and inform future decision-making; and Cryptographic Agility and Interoperability: Proceedings of a Workshop, which summarizes discussions at a Cyber Resilience Forum workshop on drivers for cryptographic agility and its technical and societal implications.

In 2016: A 21st Century Cyber-Physical Systems Education, which describes the knowledge and skills required to engineer increasingly capable, adaptable, and trustworthy systems that integrate the cyber and physical worlds and recommends paths for creating the courses and programs needed to educate the engineering workforce that builds them; Data Breach Aftermath and Recovery for Individuals and Institutions: Proceedings of a Workshop, which summarizes the presentations and discussions from a January 2016 workshop convened by the Cyber Resilience Forum; and Exploring Encryption and Potential Mechanisms for Authorized Government Access to Plaintext: Proceedings of a Workshop, which summarizes presentations and discussions at a June 2016 workshop.

CSTB's reports, enabled in part by support under this award, and its website provide a resource for researchers and policy makers concerned with information technology research, development, deployment, implications, and policy. All past and current work is made available to the public through this Web site. Also, briefings on study results were provided to project sponsors and other interested parties.

Major goals

The Computer Science and Telecommunications Board of the National Academies convenes the nation's foremost computer science, telecommunications, and information technology experts. They provide authoritative advice to the nation on technical and public policy aspects of IT and its social and economic implications, on sustaining leadership in IT innovation, and on using IT in desirable and beneficial ways. CSTB's products include workshops, other public meetings, and influential and widely read reports.

The goals of the CSTB, as partially supported by this award, are to:

- Provide objective, nonpartisan, scholarly analysis, blending expertise in computer science (CS), electrical engineering, telecommunications, and various applications and impacts of information technology (IT).
- Engage experts from the entire IT community in mixed collaborative groups, developing ideas, explanations, assessments, and recommendations reflecting diverse points of view and rigorous peer review.
- Provide a focal point for engaging the research community in the development of new research agendas and in raising the level of policy debate.
- Plan for, oversee, and follow up on projects and to be forward-thinking and proactive in formulating new activities.
- Deliver its reports and provides briefings to key decision-makers and practitioners in the research, education, and policy- making communities.

What was accomplished under these goals?

This award provided partial support for the operation of the Computer Science and Telecommunications Board. Staff organized and ran the meetings of the CSTB, including meeting planning and agenda preparation; selected and organized topical sessions at board meetings; identified and recruited outside speakers; and helped identify and recruit new board members from academia and industry.

- The Sept. 2016 meeting included updates from NSF/CISE, an update from the deputy U.S. chief technology officer on OSTP activities, and a ½-day colloquium on future scientific infrastructure for scientific discovery.
- The March 2017 meeting included a discussion of a potential periodic survey of computing research for NSF, a briefing of the just-released Information Technology and the U.S. Workforce report, a discussion of potential priorities in AI, and a roundtable with Bay Area Research Directors.
- Topics at the September, 2017, CSTB meeting included a discussion of AI and cybersecurity with Vinh Nguyen, National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence, an exploration of the role of AI in health care, an update on Academies efforts to measure computing capabilities to gauge workforce impacts, and a panel exploring federal computing research priorities with Jim Kurose (NSF), Charles Romine (NIST), and Bryan Biegel (NITRD NCO). In addition, CSTB members discussed the kick-off of a new study to update the “tiretracks.”
- The March 2018 CSTB meeting included updates on recent, current, and prospective CSTB projects. presentations from the NSF assistant director for CISE (Jim Kurose), the Hewlett Foundation Cyber Initiative program director (Eli Sugarman), a discussion with the Alliance Silicon Valley Lab chief technology director (Maartin Sierhuis), and a discussion with members of the Bay Area Research Directors. CSTB members reviewed results of and lessons learned from two recently completed studies: Assessing and Responding to the Growth of Computer Science Undergraduate Enrollments and Envisioning the Data Science

Discipline: The Undergraduate Perspective. Finally, they explored possible future CSTB activities related to computing education, digital skills, and the future of work.

- The Nov. 2018 meeting included updates on computing research issues from Peter Highnam (DARPA), Lynne E. Parker (OSTP), Jim Kurose (NSF), and Charles Romine (NIST) and presentations from Andrew Appel (Princeton) on computer security and elections and Mark Horowitz (Stanford) on quantum computing progress and prospects.

Individual Project Results

A number of individual study reports or related materials were enabled in part by support under this award, and largely funded through separate project-specific awards.

2018

- Quantum Computing: Progress and Prospects. Assesses the current progress and possible future pathways towards developing a general-purpose quantum computer as well as its potential implications.
- Recoverability as a First-Class Security Objective. Summarizes presentations and discussions from a Feb. 2018 Forum on Cyber Resilience workshop on how to restore normal operations and security following an attack or failure of software or hardware.
- Securing the Vote: Protecting American Democracy. Recommends steps that the federal government, state and local governments and election administrators can take to make elections more secure, accessible, reliable, and verifiable.
- Opportunities from the Integration of Simulation and Data Science: Proceedings of a Workshop. Examines current and emerging science applications that span simulation and data-driven science, their characteristics, and future approaches for cyberinfrastructure to support them.
- Data Science for Undergraduates: Opportunities and Options offers a vision for the emerging discipline of data science at the undergraduate level and outlines considerations and approaches for academic institutions and others to help guide the ongoing transformation of the field.
- Decrypting the Encryption Debate: A Framework for Decision-Makers. Proposes a framework for evaluating proposals to provide authorized government access to the plaintext of encrypted communications and stored data.

2017

- Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions. Explores how a more effective national alert and warning system might be created and sets forth a research agenda to advance the nation’s alert and warning capabilities.
- Software Update as a Mechanism for Resilience and Security: Proceedings of a Workshop. Sum- marizes discussions at a workshop organized by the Cyber Resilience Forum exploring prac- tices, mechanisms, policies, and technologies.

- Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions. Focuses on foundational research strategies and on building collaborative links across disciplines and between research and practice.
- Information Technology and the U.S. Workforce: Where are We and Where do We Go from Here?. Explores current and emerging information technology capabilities and their interplay with various dimensions of work, and highlights areas where new research and data would help to improve understanding and inform future decision-making.
- Cryptographic Agility and Interoperability: Proceedings of a Workshop. Summarizes discussions at a Cyber Resilience Forum workshop on drivers for cryptographic agility and its technical and societal implications.

2016

- A 21st Century Cyber-Physical Systems Education. Describes the knowledge and skills required to engineer increasingly capable, adaptable, and trustworthy systems that integrate the cyber and physical worlds and recommends paths for creating the courses and programs needed to educate the engineering workforce that builds them.
- Data Breach Aftermath and Recovery for Individuals and Institutions: Proceedings of a Workshop. Summarizes the presentations and discussions from a January 2016 workshop convened by the Cyber Resilience Forum.
- Exploring Encryption and Potential Mechanisms for Authorized Government Access to Plaintext: Proceedings of a Workshop. Summarizes presentations and discussions at a June 2016 workshop.

What opportunities for training and professional development has the project provided?

CSTB activities train large numbers of computer scientists and engineers (and also experts from other disciplines) that participate in its activities, notably those who serve as members of its study committees convened for specific projects, but also including those who participated in workshops and other meetings. CSTB's blend of computer science and engineering with other disciplines that relate to public policy gives committee members and other participants in its activities a unique opportunity to relate computer science and engineering to public policy and vice versa.

How have the results been disseminated to communities of interest?

All past and current work is made available to the public through CSTB's web site, www.cstb.org. Also, briefings on study results were provided to project sponsors and other interested parties.

Products and Publications

Website: Computer Science and Telecommunications Board
URL: http://www.cstb.org

Description: Provides information on current CSTB activities and access to all past CSTB reports, organized chronologically and thematically.

National Academies reports partially enabled by this award and largely funded by separate individual awards (all peer-reviewed following National Academies procedures and published by National Academies Press, Washington, DC.)

2018

Quantum Computing: Progress and Prospects
Recoverability as a First-Class Security Objective
Securing the Vote: Protecting American Democracy
Opportunities from the Integration of Simulation and Data Science: Proceedings of a Workshop.
Data Science for Undergraduates: Opportunities and Options
Decrypting the Encryption Debate: A Framework for Decision-Makers

2017

Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions. Software Update as a Mechanism for Resilience and Security: Proceedings of a Workshop. Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions. Information Technology and the U.S. Workforce: Where are We and Where do We Go from Here?
Cryptographic Agility and Interoperability: Proceedings of a Workshop.

2016

A 21st Century Cyber-Physical Systems Education
Data Breach Aftermath and Recovery for Individuals and Institutions: Proceedings of a Workshop
Exploring Encryption and Potential Mechanisms for Authorized Government Access to Plaintext: Proceedings of a Workshop

Participants

Dr. Jon K. Eisenberg, principal investigator/project director (together with other CSTB professional staff and board chair Farnam Jahanian) organized and ran the meetings of the Computer Science and Telecommunications Board, including meeting planning and agenda preparation; selected and organized topical sessions at board meetings; identified and recruited outside speakers; and helped identify and recruit new board members from academia and industry. Eisenberg also administered CSTB's program of studies and professional staff, managed CSTB's Web site, cstb.org, which is a primary vehicle for disseminating the results of CSTB studies, and CSTB's database of experts and technical, business, and policy leaders to whom report results and other project information are disseminated; conducted outreach to technical and policy leaders in federal agencies, companies, and private foundations to explore areas of interest or concern in the computer science and engineering community, to identify potential experts to involve in CSTB studies and other activities, to obtain inputs relevant to

particular CSTB ongoing or prospective studies, and to explore potential new studies and other activities; prepared briefings and other materials, made presentations, and otherwise disseminated the results of recent CSTB activities to federal agency officials, congressional staff, computer science researchers, and others interested in IT R&D and policy.

Ms. Lynette Millett, Co-Project Director, helped organize and run meetings of the Computer Science and Telecommunications Board, including meeting planning and agenda preparation; selected and organized topical sessions at board meetings; identified and recruited outside speakers; and helped identify and recruit new board members from academia and industry. Helped administer CSTB's program of studies and professional staff, managed CSTB's Web site, cstb.org, which is a primary vehicle for disseminating the results of CSTB studies, and CSTB's database of experts and technical, business, and policy leaders to whom report results and other project information are disseminated; conducted outreach to technical and policy leaders in federal agencies, companies, and private foundations to explore areas of interest or concern in the computer science and engineering community, to identify potential experts to involve in CSTB studies and other activities, to obtain inputs relevant to particular CSTB ongoing or prospective studies, and to explore potential new studies and other activities; prepared briefings and other materials, made presentations, and otherwise disseminated the results of recent CSTB activities to federal agency officials, congressional staff, computer science researchers, and others interested in IT R&D and policy.

Impact

1. What is the impact on the development of the principal discipline(s) of the project?

CSTB convenes computer scientists and engineers (and others) as members of the Board to consider issues that bear on the health of the discipline and the contributions of the discipline to the nation; it convenes computer scientists and engineers (and others) as members of its project committees, which develop reports that are circulated widely to researchers and others as appropriate to the topic. This grant helped to make the overall program possible and supported specific activities as needed and as opportunities arose.

Several of the reports partially enabled by this award specifically address future research opportunities and directions.

- Quantum Computing: Progress and Prospects
- Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions
- Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions.
- Information Technology and the U.S. Workforce: Where are We and Where do We Go from Here?

Three other reports look at education related to computing and data:

- Data Science for Undergraduates: Opportunities and Options
- Assessing and Responding to the Growth of Computer Science Undergraduate Enrollments
- A 21st Century Cyber-Physical Systems Education

2. What is the impact on other disciplines?

CSTB has a strong interdisciplinary orientation. Its contributions to other disciplines occur through its convening of senior people in the Board and the Board's committees as well as in the content of its reports.

Activities explicitly concerned with interdisciplinary concerns included:

- Securing the Vote: Protecting American Democracy
- Decrypting the Encryption Debate: A Framework for Decision-Makers
- Data Science for Undergraduates: Opportunities and Options
- Future Research Goals and Directions for Foundational Science in Cybersecurity
- Information Technology, Automation, and the U.S. Workforce

3. What is the impact on the development of human resources?

CSTB activities educate senior people in the field through their participation in its studies and other projects. Its books and outreach activities extend that educational process. Some of its activities are explicitly concerned with human resource issues. For example:

- Toward 21st-Century Cyber-Physical Systems Education
- Data Science for Undergraduates: Opportunities and Options
- Assessing and Responding to the Growth of Computer Science Undergraduate Enrollments

4. What is the impact on physical, institutional, and information resources that form infrastructure?

Infrastructure for science was the focus of the following report: Opportunities from the Integration of Simulation and Data Science: Proceedings of a Workshop.

Support for CSTB's core operations, by DOE and an array of other federal agencies and companies is instrumental to enabling CSTB to assess emerging technologies, applications, and policy issues; to involve the broader information technology community in the development of ideas in advance of seeking large scale support for major projects; to undertake activities more quickly and flexibly; and to more quickly develop report updates, special publications, and

briefings for policy makers as the needs arise, based on the knowledge CSTB has developed from thousands of expert study hours.

CSTB's reports, enabled in part by support under this award, and its website provide a resource for researchers and policy makers concerned with information technology research, development, deployment, implications, and policy.

5. What is the impact on technology transfer?

Nothing to report.

6. What is the impact on society beyond science and technology?

Several of CSTB's activities are concerned with the ultimate implications and impact of computing on society. For example:

- Forum on Cyber Resilience is an ongoing Academies roundtable to facilitate and enhance the exchange of ideas among scientists, engineers, practitioners, and policy makers concerned with urgent and important issues related to the
- resilience of the Internet and the nation's information and communications infrastructure and systems more broadly.
- The report Information Technology, Automation, and the U.S. Workforce, explores current and emerging information technology capabilities and their interplay with various dimensions of work, and highlights areas where new research and data would help to improve understanding and inform future decision-making.
- The report Decrypting the Encryption Debate examines the societal tradeoffs associated with technical mechanisms to provide authorized government agencies with access to the plaintext version of encrypted information.