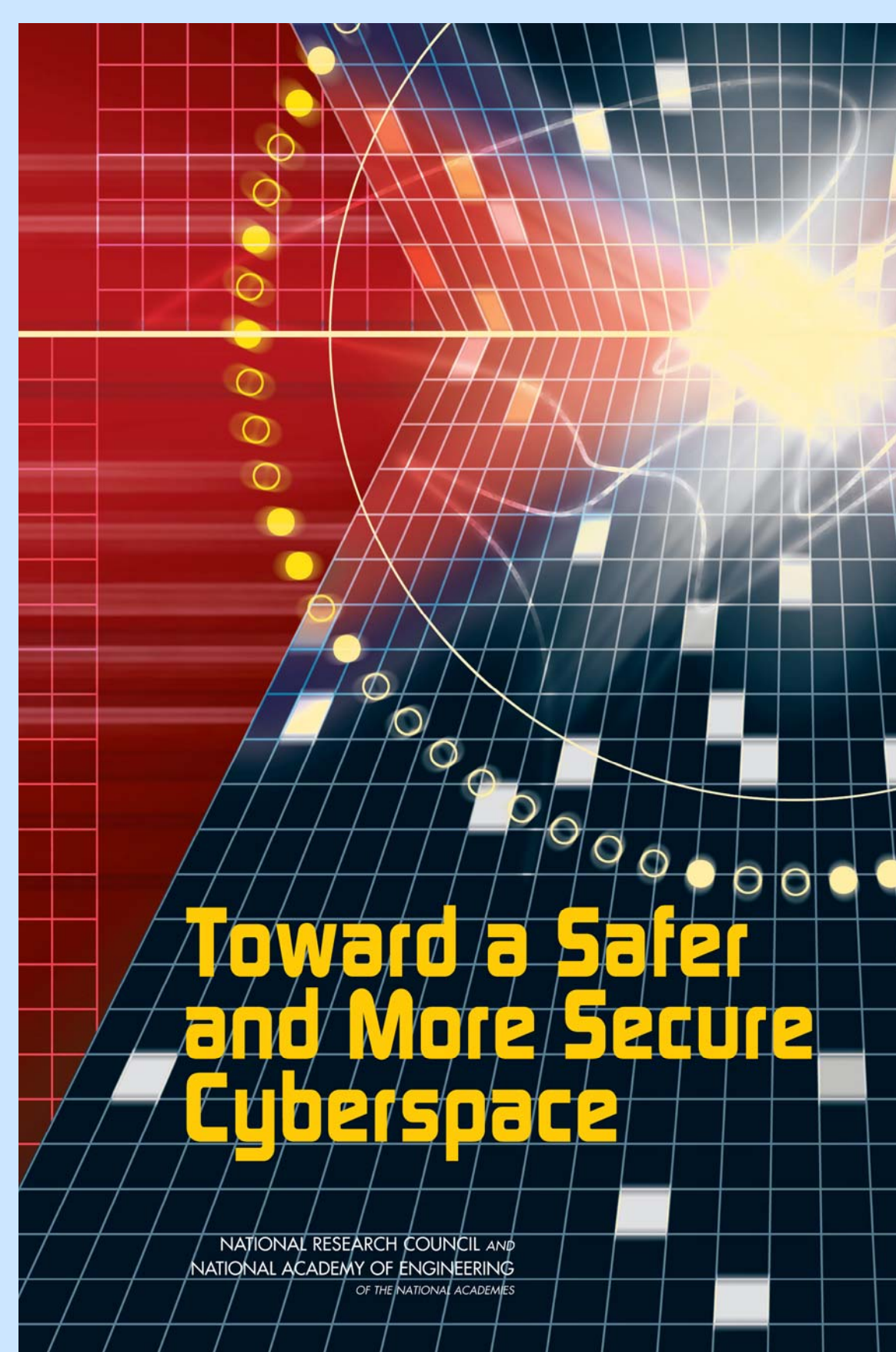


Toward a Safer and More Secure Cyberspace

Committee on Improving Cybersecurity Research in the United States
Computer Science and Telecommunications Board, National Research Council

Seymour E. Goodman and Herbert S. Lin, Editors



- Explains the nature of cybersecurity threats
- Explores why previous cybersecurity research efforts have had less impact on the nation's cybersecurity posture than desired
- Enumerates societal objectives for trustworthy systems
- Presents a broad strategy for cybersecurity research and proposes some research thrusts that are presently not major foci of the research community
- Proposes resources for advancing cybersecurity research agenda that are commensurate with the threat

A Vision for A More Secure Cyberspace: A Cybersecurity Bill of Rights

Holistic System Properties

1. Availability of system and network resources to legitimate users.
2. Easy and convenient recovery from successful attacks.
3. Control over and knowledge of one's own computing environment.

Security Properties

4. Confidentiality of stored information and information exchange
5. Authentication and provenance .
6. The technological capability to exercise fine-grained control over the flow of information in and through systems.

Cross-cutting Properties of Systems and Applications

7. Security in using computing directly or indirectly in important applications, including financial, health care, and electoral transactions and real-time remote control of devices that interact with physical processes.
8. The ability to access any source of information (e.g., email, web page, file) safely.
9. Awareness of what security is actually being delivered by a system or component.

Jurisprudence Property

10. Justice for security problems caused by another party.

Principles for the Ongoing Research Agenda

- Conduct cybersecurity research as though its application will be important.
- Hedge against uncertainty in the nature and severity of the future cybersecurity threat.
- Ensure programmatic continuity.
- Respect the need for breadth in the research agenda.
- Disseminate new knowledge and artifacts to the research community.

Categories of Research Focus

- Blocking and limiting the impact of compromise
- Enabling accountability
- Promoting deployment and use
- Deterring would-be attackers
- Cross-cutting problem-focused research (e.g., security for legacy systems, the role of secrecy in cyber defense, coping with the insider threat, and security for new computing environments)
- Speculative ("out-of-box") research

Can be read at www.cstb.org,
purchased from www.nap.edu,
or downloaded in PDF format from www.cyber.st.dhs.gov/