NATIONAL ACADEMY OF SCIENCES
NATIONAL ACADEMY OF ENGINEERING
INSTITUTE OF MEDICINE
NATIONAL RESEARCH COUNCIL

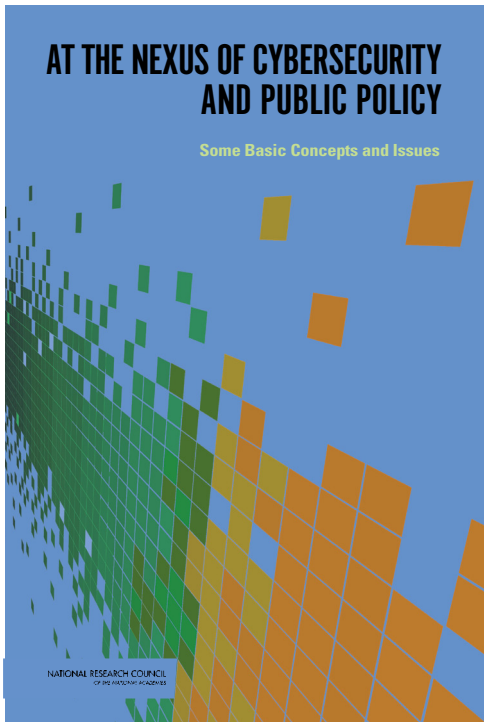
REPORT IN BRIEF

At the Nexus of Cybersecurity and Public Policy

Some Basic Concepts and Issues

Computer Science and Telecommunications Board · Division on Engineering & Physical Sciences · May 2014

Our nation is increasingly dependent on computers and information technology. Systems as diverse as our power grid, health care system, armed forces, and financial services, rely on computers and networks at every stage. Malevolent actors can exploit vulnerabilities in these systems to steal money, intellectual property, or classified information; snoop on private conversations; impersonate others; harass or bully innocent people anonymously; damage important data; disrupt the operation of physical machinery controlled by computers; or deny the availability of normally accessible services. In light of growing concerns for our nation's cybersecurity and numerous policy proposals, this report was assembled to help decision makers and the interested public make informed choices.



A Primer on Cybersecurity

Drawing on over two decades of previous work by the National Research Council's Computer Science and Telecommunications Board, the report provides necessary background for understanding issues at the nexus of cybersecurity and public policy. In addition, it offers six major findings that provide a point of departure for informed discussions at this nexus.

The report defines cyberspace broadly as the artifacts based on or dependent on computer and communications technology; the information that these artifacts store or process; and how these various elements are connected. Cybersecurity is about technologies, processes, and policies that help to prevent or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology (IT) by a malevolent actor.

Cybersecurity issues arise because of three factors taken together—the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the inevitable presence of vulnerabilities in IT systems that malevolent actors can take advantage of. Despite these factors, however, we still expect information technologies to do what they are supposed to do and only when they are supposed to do it, and to never do things they are not supposed to do. Fulfilling this expectation is the purpose of cybersecurity.

No cybersecurity solution is permanent

Against this backdrop, it appears that cybersecurity is a never-ending battle, and a permanently decisive solution to the problem will not be found in the foreseeable future. Cybersecurity problems result from the complexity of modern IT systems and human fallibility in making judgments about what actions or information is safe or unsafe from a cybersecurity perspective. Furthermore, threats to cybersecurity evolve, and adversaries constantly adopt new tools and techniques to compromise security when defenses are erected to frustrate them. As information technology becomes more ubiquitously integrated into society, the incentives to compromise the security of deployed IT systems grow. Thus, enhancing the cybersecurity posture of a system must be understood as an ongoing process. Ultimately, the relevant policy question is not how the cybersecurity problem can be solved, but rather how it can be made manageable.

Better defenses slow and deter malevolent actors

At the same time, improvements to the cybersecurity posture of individuals, firms, government agencies, and the nation have considerable value in reducing the loss and damage that may be associated with cybersecurity breaches. A well-defended target is less attractive to many malevolent actors than are poorly defended targets. In addition, defensive measures force a malevolent actor to expend time and resources to adapt, thus making intrusion attempts slower and more costly and possibly helping to deter future intrusions.

Apply existing practices and develop new practices to improve cybersecurity

Improvements to cybersecurity call for two distinct kinds of activity: efforts to more effectively and more widely use what is already known about improving cybersecurity, and efforts to develop new knowledge about how to improve cybersecurity even further. The gap in security afforded by the U.S. national cybersecurity posture and the threat has two parts. The first part of the gap is the difference between what our cybersecurity posture is and what it could be if known best cybersecurity practices and technologies were widely deployed and used. The second part is the gap between the strongest posture possible with known practices and technologies and the threat as it exists (and will exist). The first gap is primarily nontechnical in nature—closing this gap does not require new knowledge of cybersecurity per se, but rather the application of existing knowledge. Research will be needed to understand how better to promote deployment and use of such knowledge. Closing the second gap is where new technologies and approaches are needed, and is the fundamental rationale for technically focused research in cybersecurity.

Cybersecurity issues lack public urgency

Publicly available information and policy actions to date have been insufficient to motivate an adequate sense of urgency and ownership of cybersecurity problems afflicting the United States as a nation. For a number of years, the cybersecurity issue has received increasing public attention and a greater amount of authoritative information regarding cybersecurity threats is available publicly. But all too many decision makers still focus on the short-term costs of improving their own organizational cybersecurity postures and little has been done to harness market forces to address matters related to the cybersecurity posture of the nation as a whole. If the nation's cybersecurity posture is to be improved to a level that is higher than the level to which today's market will drive it, the market calculus that motivates organizations to pay attention to cybersecurity must be altered in some fashion.

Cybersecurity policies will require tradeoffs

Cybersecurity is important to the nation, but the United States has other interests as well, some of which conflict with the imperatives of cybersecurity. Tradeoffs are inevitable and will have to be accepted through the nation's political and policy-making processes. Senior policy makers have many issues on their agenda and they must set priorities for the issues that warrant their attention. In an environment of many competing priorities, reactive policy making is often the outcome. Support for efforts to prevent a disaster that has not yet occurred is typically less than support for efforts to respond to a disaster that has already occurred. In cybersecurity, this tendency is reflected in the notion that "no or few attempts have yet been made to compromise the cybersecurity of application X, and why would anyone want to do so anyway?", thus justifying why immediate attention and action to improve the cybersecurity posture of application X can be deferred or studied further.

Progress in cybersecurity policy has also stalled at least in part because of conflicting equities. As a nation, we want better cybersecurity, yes, but we also want a private sector that innovates rapidly, the convenience of not having to worry about cybersecurity, and the right to no diminution in our civil liberties. Although research and deeper thought may reveal that, in some cases, tradeoffs between security and these other equities are not as stark as they might

appear at first glance, policy makers will have to confront rather than avoid tensions when they are irreconcilable. Honest acknowledgment and discussion of the tradeoffs (e.g., a better cybersecurity posture may reduce the nation's innovative capability, may increase the inconvenience of using information technology, may reduce the ability to collect intelligence) will go a long way toward building public support for a given policy position.

U.S. offensive cyber capabilities lack public discussion

The use of offensive operations in cyberspace as an instrument to advance U.S. interests raises many important technical, legal, and policy questions that have yet to be aired publicly by the U.S. government. Some of these questions involve topics such as U.S. offensive capabilities in cyberspace, rules of engagement, doctrine for the use of offensive capabilities, organizational responsibilities within the Department of Defense and the intelligence community, and a host of other topics related to offensive operations. It is likely that behind the veil of classification, these topics have been discussed at length. The resulting opacity has many undesirable consequences, but one of the most important consequences is that the role offensive capabilities could play in defending important information technology assets of the United States cannot be discussed fully.

What is sensitive about offensive U.S. capabilities in cyberspace is generally the fact of U.S. interest in a specific technology for cyberattack (rather than the nature of that technology itself); fragile and sensitive operational details that are not specific to the technologies themselves (e.g., the existence of a covert operative in a specific foreign country, a particular vulnerability, a particular operational program); or U.S. knowledge of the capabilities and intentions of specific adversaries. Such information is legitimately classified but is not particularly relevant for a discussion about what U.S. policy should be. That is, unclassified information provides a generally reasonable basis for understanding what can be done and for policy discussions that focus primarily on what should be done.

Conclusion

In summary, cybersecurity is a complex subject, whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law. Although technical measures are an important element, cybersecurity is not primarily a technical matter. Furthermore, what is known about cybersecurity is often "siloed" along disciplinary lines, reducing the insights available from cross-fertilization.

The report emphasizes two central ideas. The cybersecurity problem will never be solved once and for all. Solutions to the problem, limited in scope and longevity though they may be, are at least as much nontechnical as technical in nature.

Click here to view a short video summary of this report at youtu.be/C_asue70Xl8.

Committee on Developing a Cybersecurity Primer: David Clark, Massachusetts Institute of Technology, Chair; **Thomas Berson**, Anagram Laboratories; **Marjory Blumenthal**, Georgetown University

Staff: Herbert S. Lin, Study Director and Chief Scientist, Computer Science and Telecommunications Board; **Eric Whitaker**, Senior Program Assistant

Support for this project was provided by the National Science Foundation. Additional support was provided by Microsoft, Google, and the President's Committee of the National Academies. Any opinions, findings, or conclusions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project, or the National Research Council.

Copies of this report are available free of charge from http://www.nap.edu.

Report issued May 2014.