

Free Executive Summary

Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities



William A. Owens, Kenneth W. Dam, and Herbert S. Lin, editors, Committee on Offensive Information Warfare, National Research Council

ISBN: 978-0-309-13850-5, 376 pages, 6x9, paperback (2009)

This free executive summary is provided by the National Academies as part of our mission to educate the world on issues of science, engineering, and health. If you are interested in reading the full book, please visit us online at <http://www.nap.edu/catalog/12651.html>. You may browse and search the full, authoritative version for free; you may also purchase a print or electronic version of the book. If you have questions or just want more information about the books published by the National Academies Press, please contact our customer service department toll-free at 888-624-8373.

The US armed forces, among other intelligence agencies, are increasingly dependent on information and information technology for both civilian and military purposes. Although there is ample literature written on the potential impact of an offensive or defensive cyberattack on societal infrastructure, little has been written about the use of cyberattack as a national policy tool. This book focuses on the potential for the use of such attacks by the United States and its policy implications. Since the primary resource required for a cyberattack is technical expertise, these attacks can be implemented by terrorists, criminals, individuals and corporate actors. Cyberattacks can be used by U.S. adversaries against particular sectors of the U.S. economy and critical national infrastructure that depend on computer systems and networks. Conversely, they can be used by the U.S. intelligence community with adequate organizational structure and appropriate oversight. Focusing on the use of cyberattack as an instrument of U.S. national policy, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities explores the important characteristics of cyberattacks and why they are relatively ideal for covert action. Experts argue that the United States should establish a national policy for launching cyberattacks, whether for purposes of exploitation, offense or defense for all sectors of government. This book will be of special interest to the Department of Defense, the Department of Homeland Security, law enforcement, and the greater intelligence community.

This executive summary plus thousands more available at www.nap.edu.

Copyright © National Academy of Sciences. All rights reserved. Unless otherwise indicated, all materials in this PDF file are copyrighted by the National Academy of Sciences. Distribution or copying is strictly prohibited without permission of the National Academies Press <http://www.nap.edu/permissions/> Permission is granted for this material to be posted on a secure password-protected Web site. The content may not be posted on a public Web site.

Synopsis

This synopsis is intended to provide the reader with a sense of what the report contains. However, it is necessarily incomplete, and it omits any mention of many significant topics contained in the main body of the report.

UNDERSTANDING CYBERATTACK

What Is Cyberattack?

Cyberattack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks. The U.S. armed forces are actively preparing to engage in cyberattacks, perhaps in concert with other information warfare means and/or with kinetic attacks, and may have done so in the past. Domestic law enforcement agencies also engage in cyberattack when they jam cell phone networks in order to prevent the detonation of improvised explosive devices.

Such matters pose some very important issues that relate to technology, policy, law, and ethics. This report provides an intellectual framework for thinking about cyberattack and understanding these issues.

A first point is that cyberattack must be clearly distinguished from cyberexploitation, which is an intelligence-gathering activity rather than a destructive activity. Although much of the technology underlying cyberexploitation is similar to that of cyberattack, cyberattack and cyberexploitation are conducted for entirely different purposes. (This contrast is relevant to much of the public debate using the term "cyberattack," which in common usage often lumps both attack and exploitation under the "attack" label.)

Second, weapons for cyberattack have a number of characteristics that differentiate them from traditional kinetic weapons. Compared to kinetic weapons, many weapons for cyberattack:

- Are easy to use with high degrees of anonymity and with plausible deniability, making them well suited for covert operations and for instigating conflict between other parties;
- Are more uncertain in the outcomes they produce, making it difficult to make estimates of deliberate and collateral damage; and
- Involve a much larger range of options and possible outcomes, and may operate on time scales ranging from tenths of a second to years, and at spatial scales anywhere from "concentrated in a facility next door" to globally dispersed.

Third, cyberattack as a mode of conflict raises many operational issues. For example, given that any large nation experiences cyberattacks continuously, how will the United States know it is the subject of a cyberattack deliberately launched by an adversary government? There is also a further tension between a policy need for rapid response and the technical reality that attribution is a time-consuming task. Shortening the time for investigation may well increase the likelihood of errors being made in a response (e.g., responding against the wrong machine or launching a response that has large unintended effects).

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

S-1

Illustrative Applications of Cyberattack

Cyberattack can support military operations. For example, a cyberattack could disrupt adversary command, control, and communications; suppress air defenses; degrade smart munitions and platforms; or attack war-fighting or war-making infrastructure (the defense industrial base). Cyberattack might be used to augment or to enable some other kinetic attack to succeed, or to defend a friendly computer system or network by neutralizing the source of a cyberattack conducted against it.

Cyberattack can also support covert action, which is generally designed to influence governments, events, organizations, or persons in support of foreign policy in a manner that is not necessarily attributable to the U.S. government. The range of possible cyberattack options is very large, and so cyberattack-based covert action might be used, for example, to influence an election, instigate conflict between political factions, harass disfavored leaders or entities, or divert money.

Illustrative Applications of Cyberexploitation

For intelligence gathering, cyberexploitation of an adversary's computer systems might yield valuable information. For example, U.S. intelligence agencies might learn useful information about an adversary's intentions and capabilities from a penetration of its classified government networks. Alternatively, they might obtain useful economic information from penetrating the computer systems of a competing nation's major industrial firms.

The Legal Framework Governing Cyberattack

In the committee's view, the essential framework for the legal analysis of cyberattack is based on the principle that notions related to "use of force" and "armed attack" (terms of special relevance to the Charter of the United Nations) should be judged primarily by the effects of an action rather than its modality. That is, the fact that an attack is carried out through the use of cyberweapons rather than kinetic weapons is far less significant than the effects that result from such use, where "effects" are understood to include both direct and indirect effects.

Furthermore, the committee believes that the principles of the law of armed conflict (LOAC) and the Charter of the United Nations—including both law governing the legality of going to war (*jus ad bellum*) and law governing behavior during war (*jus in bello*)—do apply to cyberattack, although new analytical work may be needed to understand how these principles do or should apply to cyberweapons. That is, some types of cyberattack are difficult to analyze within the traditional LOAC structure. Among the more problematic cases are the following:

- The presumption of nation-to-nation conflict between national military forces,
- The exception for espionage, and
- The emphasis on notions of territorial integrity.

The Dynamics of Cyberconflict

The escalatory dynamics of armed conflict are thought to be understood as the result of many years of thinking about the subject, but the dynamics of cyberconflict are poorly understood. This report speculates on some of the factors that might influence the evolution of a cyberconflict.

For major nation-states with significant capabilities for kinetic attack and cyberattack at their disposal, among the important issues regarding the dynamics of cyberconflict are the following:

- Crisis stability (preventing a serious cyberconflict from breaking out),
- Preventing a cyberconflict from escalating to physical space, and
- Knowing when a cyberconflict has been terminated.

Matters can be further complicated by the presence of non-state actors, such as cyberterrorists, patriotic hackers, and criminal groups. Perhaps the most important complication relates to identification of the appropriate party against which action might be taken and the related availability of cyber targets whose destruction might cause pain or meaningful damage to the terrorist or criminal group.

FINDINGS

Cyberattack is an important capability for the United States to maintain, but at the same time the acquisition and use of such capabilities raise many questions and issues, as described below.

Overarching Findings

1. The policy and organizational issues raised by U.S. acquisition and use of cyberattack are significant across a broad range of conflict scenarios, from small skirmishes with minor actors on the international stage to all-out conflicts with adversaries capable of employing weapons of mass destruction.
2. The availability of cyberattack technologies for national purposes greatly expands the range of options available to U.S. policy makers as well as to policy makers of other nations.
3. Today's policy and legal framework for guiding and regulating the U.S. use of cyberattack is ill-formed, undeveloped, and highly uncertain.
4. Secrecy has impeded widespread understanding and debate about the nature and implications of U.S. cyberattack.
5. The consequences of a cyberattack may be both direct and indirect, and in some cases of interest, the indirect consequences of a cyberattack can far outweigh the direct consequences.

Legal and Ethical Findings

6. The conceptual framework that underpins the UN Charter on the use of force and armed attack and today's law of armed conflict provides a reasonable starting point for an

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

S-3

international legal regime to govern cyberattack. However, those legal constructs fail to account for non-state actors and for the technical characteristics of some cyberattacks.

7. In today's security environment, private parties have few useful alternatives for responding to a severe cyberattack that arrives over a network such as the Internet.

8. Cyberattack poses challenges to existing ethical and human rights regimes.

Policy Findings

9. Enduring unilateral dominance in cyberspace is neither realistic nor achievable by the United States.

10. The United States has much to lose from unrestrained cyberattack capabilities that are proliferated worldwide.

11. Deterrence of cyberattacks by the threat of in-kind response has limited applicability.

12. Options for responding to cyberattacks on the United States span a broad range and include a mix of dynamic changes in defensive postures, law enforcement actions, diplomacy, cyberattacks, and kinetic attacks.

Technical and Operational Findings

13. For many kinds of information technology infrastructure targets, the ease of cyberattack is increasing rather than decreasing.

14. Although the actual cyberattack capabilities of the United States are highly classified, they are at least as powerful as those demonstrated by the most sophisticated cyberattacks perpetrated by cybercriminals and are likely more powerful.

15. As is true for air, sea, land, and space operations, the defensive or offensive intent motivating cyber operations in any given instance may be difficult to infer.

16. Certain cyberattacks undertaken by the United States are likely to have significant operational implications for the U.S. private sector.

17. If and when the United States decides to launch a cyberattack, significant coordination among allied nations and a wide range of public and private entities may be necessary, depending on the scope and nature of the cyberattack in question.

18. The outcomes of many kinds of cyberattack are likely to be more uncertain than outcomes for other kinds of attack.

19. Early use of cyberattack may be easy to contemplate in a pre-conflict situation, and so a greater degree of operational oversight for cyberattack may be needed compared to that for the use of other options.

20. Developing appropriate rules of engagement for the use of cyberweapons is very difficult.

Organizational Findings

21. Both the decision-making apparatus for cyberattack and the oversight mechanisms for that apparatus are inadequate today.

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

22. The U.S. Congress has a substantial role to play in authorizing the use of military force, but the contours of that authority and the circumstances under which authorization is necessary are at least as uncertain for cyberattack as for the use of other weapons.

RECOMMENDATIONS

Fostering a National Debate on Cyberattack

1. The United States should establish a public national policy regarding cyberattack for all sectors of government, including but not necessarily limited to the Departments of Defense, State, Homeland Security, Treasury, and Commerce; the intelligence community; and law enforcement. The senior leadership of these organizations should be involved in formulating this national policy.

2. The U.S. government should conduct a broad, unclassified national debate and discussion about cyberattack policy, ensuring that all parties—particularly Congress, the professional military, and the intelligence agencies—are involved in discussions and are familiar with the issues.

3. The U.S. government should work to find common ground with other nations regarding cyberattack. Such common ground should include better mutual understanding regarding various national views of cyberattack, as well as measures to promote transparency and confidence building.

Organizing the Decision-Making Apparatus of the U.S. Government for Cyberattack

4. The U.S. government should have a clear, transparent, and inclusive decision-making structure in place to decide how, when, and why a cyberattack will be conducted.

5. The U.S. government should provide a periodic accounting of cyberattacks undertaken by the U.S. armed forces, federal law enforcement agencies, intelligence agencies, and any other agencies with authorities to conduct such attacks in sufficient detail to provide decision makers with a more comprehensive understanding of these activities. Such a periodic accounting should be made available both to senior decision makers in the executive branch and to the appropriate congressional leaders and committees.

Supporting Cyberattack Capabilities and Policy

6. U.S. policy makers should judge the policy, legal, and ethical significance of launching a cyberattack largely on the basis of both its likely direct effects and its indirect effects.

7. U.S. policy makers should apply the moral and ethical principles underlying the law of armed conflict to cyberattack even in situations that fall short of actual armed conflict.

8. The United States should maintain and acquire effective cyberattack capabilities. Advances in capabilities should be continually factored into policy development, and a comprehensive budget accounting for research, development, testing, and evaluation relevant to cyberattack should be available to appropriate decision makers in the executive and legislative branches.

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

S-5

9. The U.S. government should ensure that there are sufficient levels of personnel trained in all dimensions of cyberattack, and that the senior leaders of government have more than a nodding acquaintance with such issues.

10. The U.S. government should consider the establishment of a government-based institutional structure through which selected private sector entities can seek immediate relief if they are the victims of cyberattack.

Developing New Knowledge and Insight into a New Domain of Conflict

11. The U.S. government should conduct high-level wargaming exercises to understand the dynamics and potential consequences of cyberconflict.

12. Foundations and government research funders should support academic and think-tank inquiry into cyberconflict, just as they have supported similar work on issues related to nuclear, biological, and chemical weapons.

PREPUBLICATION COPY – SUBJECT TO FURTHER
EDITORIAL CORRECTION

Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities

William A. Owens, Kenneth W. Dam, and Herbert S. Lin, editors

Committee on Offensive Information Warfare
Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

Support for this project was provided by the MacArthur Foundation under award number 04-80965-000-GSS, the Microsoft Corporation under an unnumbered award, and the NRC Presidents' Committee under an unnumbered award.

Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the organizations that provided support for the project.

International Standard Book Number-13: 978-0-309-XXXXX-X

International Standard Book Number-10: 0-309-XXXXX-X

Additional copies of this report are available from:

The National Academies Press
500 Fifth Street, N.W., Lockbox 285
Washington, DC 20055
(800) 624-6242
(202) 334-3313 (in the Washington metropolitan area)
Internet: <http://www.nap.edu>

Copyright 2009 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

Copyright National Academy of Sciences. All rights reserved.
This executive summary plus thousands more available at <http://www.nap.edu>

COMMITTEE ON OFFENSIVE INFORMATION WARFARE

WILLIAM A. OWENS, AEA Holdings, Inc., *Co-chair*
KENNETH W. DAM, University of Chicago, *Co-chair*
THOMAS A. BERSON, Anagram Laboratories
GERHARD CASPER, Stanford University
DAVID D. CLARK, Massachusetts Institute of Technology
RICHARD L. GARWIN, IBM Fellow Emeritus
JACK L. GOLDSMITH III, Harvard Law School
CARL G. O'BERRY, The Boeing Company
JEROME H. SALTZER, Massachusetts Institute of Technology (retired)
MARK SEIDEN, MSB Associates
SARAH SEWALL, Harvard University
WALTER B. SLOCOMBE, Caplin and Drysdale
WILLIAM O. STUDEMANN, U.S. Navy (retired)
MICHAEL A. VATIS, Steptoe & Johnson LLP

Staff

HERBERT S. LIN, Study Director
KRISTEN BATCH, Associate Staff Officer
TED SCHMITT, Consultant
JANICE SABUDA, Senior Project Assistant (through March 2008)
ERIC WHITAKER, Senior Project Assistant

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

v

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

JOSEPH F. TRAUB, Columbia University, *Chair*
PRITHVIRAJ BANERJEE, Hewlett Packard Company
FREDERICK R. CHANG, University of Texas, Austin
WILLIAM DALLY, Stanford University
MARK E. DEAN, IBM Almaden Research Center
DEBORAH L. ESTRIN, University of California, Los Angeles
KEVIN C. KAHN, Intel Corporation
JAMES KAJIYA, Microsoft Corporation
RANDY H. KATZ, University of California, Berkeley
JOHN E. KELLY III, IBM Research
SARA KIESLER, Carnegie Mellon University
JON KLEINBERG, Cornell University
PETER LEE, Carnegie Mellon University
TERESA H. MENG, Stanford University
WILLIAM H. PRESS, University of Texas, Austin
PRABHAKAR RAGHAVAN, Yahoo! Research
DAVID E. SHAW, D.E. Shaw Research
ALFRED Z. SPECTOR, Google, Inc.
ROBERT F. SPROULL, Sun Microsystems, Inc.
PETER SZOLOVITS, Massachusetts Institute of Technology
ANDREW J. VITERBI, Viterbi Group, LLC
PETER WEINBERGER, Google, Inc.

JON EISENBERG, Director
RENEE HAWKINS, Financial and Administrative Manager
HERBERT S. LIN, Chief Scientist, CSTB
LYNETTE I. MILLETT, Senior Program Officer
NANCY GILLIS, Program Officer
ENITA A. WILLIAMS, Associate Program Officer
MORGAN R. MOTTO, Program Associate
SHENAE BRADLEY, Senior Program Assistant
ERIC WHITAKER, Senior Program Assistant

For more information on CSTB, see its website at <http://www.cstb.org>, write to CSTB, National Research Council, 500 Fifth Street, N.W., Washington, DC 20001, call (202) 334-2605, or e-mail the CSTB at cstb@nas.edu.

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

Preface

Given the reality of a densely interconnected information society, much has been written about the possibility that adversaries of the United States such as terrorists or hostile nations might conduct very damaging cyberattacks against critical sectors of the U.S. economy and critical national infrastructure that depend on reliably functioning, secure computer systems and networks. For some years, the topic of cybersecurity has been an important part of the report portfolio of the National Research Council,¹ and a great deal of national attention has been given, in public, to the problem of how to protect U.S. information technology systems and networks against such attacks—that is, how to defend these systems and networks in both military and non-military contexts.² But, perhaps reflecting the common wisdom of the time, these efforts have focused almost exclusively on the cyberdefense side of the equation.

The possibility that the United States might choose to engage in cyberattacks to serve its own national interests—in cyberdefense as well as in other areas—is rarely discussed in public. One recent public hint of U.S. government interest in the topic can be found in the still-classified Comprehensive National Cybersecurity Initiative (CNCI), which was adopted as national policy in January 2008 as part of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). According to the director of national intelligence in February 2009, “The CNCI addresses current cybersecurity threats, anticipates future threats and technologies, and develops a framework for creating in partnership with the private sector an environment that no longer favors cyber intruders over defenders. The CNCI includes defensive, *offensive* [emphasis added], education, research and development, and counterintelligence elements.”³ Press reports indicated that the CNCI involves 12 components designed to protect computer networks and systems and to improve information technology processes and policies.⁴ These components included a program to reduce the number of connections from federal agencies to external computer networks to 100 or fewer. The other 11 programs address intrusion detection; intrusion prevention; research and development; situational awareness (involving the coordination of information from all agencies to help secure cyber networks and systems); cyber counter intelligence; classified network security; cyber education and training; implementation of information security technologies; *deterrence strategies* [emphasis added]; global supply chain security; and public/private collaboration.

There is some public writing on the subject of cyberattack. Starting in the mid-1990s, the first papers on the topic emerged, many of them focusing on the legal issues involved in

¹ An old but still quite relevant report on this topic is CSTB/National Research Council, *Computers at Risk*, 1991; other relevant NRC reports include *Trust in Cyberspace*, 1999, and *Toward a Safer and More Secure Cyberspace*, 2007 (The National Academies Press, Washington, D.C.).

² See, for example, CSTB/National Research Council, *Information Technology for Counterterrorism*, 2003; *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, 2002; and *Realizing the Potential of C4I: Fundamental Challenges*, 1998 (The National Academies Press, Washington, D.C.).

³ Dennis Blair, Director of National Intelligence, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, February 12, 2009, available at <http://intelligence.senate.gov/090212/blair.pdf>.

⁴ See Jill R. Aitoro, “National Cyber Security Initiative Will Have a Dozen Parts,” *Government Executive*, August 1, 2008, available at http://www.nextgov.com/nextgov/ng_20080801_9053.php.

military uses of cyberattack.⁵ One of the first studies to address the strategic implications of cyberattack was published by the RAND Corporation in 1996 (*Strategic Information Warfare: A New Face of War*).⁶ A later study covering the same topic in much more detail was published as *Strategic Warfare in Cyberspace*.⁷ A flurry of writing began to appear in the professional military literature in the late 1990s and early 2000s, but little or nothing can be found in this body of literature since around 2002 or 2003.

THIS STUDY—FOCUS, APPROACH, AND PURPOSE

Most of the writing to date has not brought together information technology experts who are knowledgeable in detail about what can and cannot be done from a technical standpoint with senior individuals who have policy experience, and has not addressed the topic in an interdisciplinary manner that integrates expertise from the disciplines and fields that are relevant to the subject. The National Research Council undertook the present study (Box P.1) believing in the value of an integrated treatment that would help shed much-needed light on various important dimensions of cyberattack (and secondarily on the topic of cyberexploitation, a term that refers to the penetration of adversary computers and networks to obtain information for intelligence purposes). Such a treatment would provide a point of departure for others so that a broad variety of independent intellectual perspectives can be brought to bear on it.

The Committee on Offensive Information Warfare first met in July 2006 and five times subsequently. Its earlier meetings were devoted primarily to briefings on a variety of topics related to cyberattack, and later meetings were devoted primarily to committee deliberations.

The authoring committee did not receive classified information in the course of this study. What is sensitive about cyberattack 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 or a particular vulnerability); or capabilities and intentions of specific adversaries. None of these specific areas are particularly relevant to a study that focuses on the articulation of an intellectual framework for thinking about cyberattack.

It is important to delineate the scope of what this report does and does not do. This report does not provide a detailed explication of U.S. policy and practice regarding cyberattack

⁵ See for example, Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, *Information Warfare and International Law*, National Defense University Press, 1998; Michael Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law*, 37:885-937, 1999; Christopher C. Joyner and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework," *European Journal of International Law*, 12(5):,2001; Jason Barkham, "Information Warfare and International Law on the Use of Force," *New York University International Law and Politics*, 34:57-113, 2001; Davis Brown, "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict," *Harvard International Law Journal* 47(1):179-221, Winter 2006; Duncan B. Hollis, "New Tools, New Rules: International Law and Information Operations," pp. 59-72 in G. David and T. McKeldin, eds., *Ideas as Weapons: Influence and Perception in Modern Warfare*, Potomac Books Inc., 2009.

⁶ Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic information Warfare: A New Face of War*, National Defense Research Institute, RAND, Washington, D.C., 1996, available at http://www.rand.org/pubs/monograph_reports/2005/MR661.pdf.

⁷ Gregory J. Rattray, *Strategic Warfare in Cyberspace*, MIT Press, Cambridge, Mass., 2001.

or cyberexploitation, nor does it describe cyberattack/cyberexploitation capabilities available to the U.S. government. Instead, it provides a framework for understanding cyberattack that describes the basic technologies of cyberattack and cyberexploitation, articulates basic principles of what cyberattack and cyberexploitation might do, and discusses some of the policy goals that these actions might serve. It addresses some of the legal and ethical considerations that such uses might entail, and it suggests some analytical tools that might be useful for thinking about cyberattack from a policy perspective. It includes a number of findings and recommendations.

Just as other areas of national security have benefited from a vigorous public airing of issues, the authoring committee hopes that this report will stimulate debate and discussion on cyberattack as an instrument of national policy at the nexus of technology, policy, law, ethics, and national security both inside and outside government and thus bring to bear on these knotty issues the best intellectual thought and consideration.

A historical analogy might be drawn to the study of nuclear issues. In many ways, today's state of affairs regarding public discourse on cyberattack is analogous to the nuclear debate of 50 years ago. At that time, nuclear policy issues were veiled in secrecy, and there was little public debate on it. Herman Kahn's books (*On Thermonuclear War*, *Thinking the Unthinkable*) were the first that addressed in the open literature what it might mean to fight a nuclear war. These seminal pieces did much to raise the public profile of these issues and stimulated an enormous amount of subsequent work outside government that has had a real impact on nuclear policy.

From our perspective as the co-chairs of this study, the topic of cyberattack is so important across a multitude of national interests—not just defense or even just national security—that it deserves robust and open discussion and debate, both among thoughtful professionals in the policy, military, intelligence, law enforcement, and legal fields and among security practitioners in the private sector. But for such discussion and debate to be productive, they must be based on some common foundation of information about the topic at hand. Thus, the report's role in providing education and background is in our view its most important function.

It is because of the potential relevance of cyberattack across a broad spectrum of national interests that it was necessary to constitute a study committee whose members had very diverse backgrounds and many different perspectives on various aspects of cyberattack. The committee assembled for this project included individuals with expertise in networking, computer security, large-scale computer systems and architecture, national security and defense policy, intelligence and military operations, international law governing war and conflict, human rights, international relations and diplomacy, constitutional law and civil liberties, and domestic law enforcement as it relates to cybersecurity. Nonetheless, no one person had all of the necessary expertise across all relevant areas, and the committee expended considerable effort to bring all of its members to a common (if basic) level of understanding in these areas. The committee was by design highly heterogeneous and interdisciplinary, a characteristic intended to promote discussion and synergy among its members. As for the two co-chairs, one of us (Owens) has extensive military experience and the other (Dam) has extensive experience in foreign affairs—and both of us have served in the private sector.

We hope that a second function of this report is to help establish the awareness needed in the elected government (executive and legislative) for making good decisions and providing proper oversight of capabilities for cyberattack. As the report points out, the U.S. government does not appear to be well organized to manage these capabilities, either in an employment sense (when and under what circumstances a particular kind of cyberattack should be used) or

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

in an acquisition sense (how to obtain capabilities for cyberattack). Many of the report's findings and recommendations focus on taking some first steps for better organization of the government in this regard.

How will the presentation and analysis in this report endure over time? The question is natural given the inevitability of changes in the technological and global environment. Based on historical experience, it is highly likely that in a decade the technological substrate underlying information technology applications will be very different by one, two, or three orders of magnitude in a number of dimensions—processor power, cost, bandwidth, storage, and so on. Deployments of information technology will be more pervasive. Connectivity among individuals, embedded computers, and organizations is likely to increase dramatically, and myriad applications that are entirely unimagined now will be commonplace. The importance of the Internet (or its follow-on) to society will be greater as well.

The global environment is also likely to be substantially different, although *how* it will be different cannot be predicted in the same way that Moore's law predicts circuit densities. Many analysts of international affairs predict a rise in the significance of actors not tied or only loosely tied to nation-states, or of adversaries that do not share U.S. or Western values or legal traditions with respect to the conduct of conflict.

Few portions of the report are tied explicitly to current technologies, although a genuine breakthrough in technologies to support non-cooperative high-precision attribution of attacks to bad actors in cyberspace would have significant implications for several findings in this report. A rise in the non-state actor cyberthreat would be significant as well—and although the committee has attempted to grapple with that issue in its analysis, it would be the first to admit that a great deal more work is needed in that area. Thus, it is the committee's hope that the framework established in this report for understanding cyberattack will endure for some time to come.

ACKNOWLEDGMENTS

This study could not have been undertaken without the financial support of the MacArthur Foundation and the Microsoft Corporation, both of which recognized the potential legal, policy, and ethical significance of new technologies for cyberattack. The National Research Council itself also provided some funding for this project.

The complexity of the issues explored in this report meant that the committee had much to learn from its briefers. The committee is grateful to many individuals:

- For briefings on cyberattack technologies, Steven Bellovin of Columbia University and William Howard, independent consultant;
- For briefings on operational dimensions of cyberattack, Patrick D. Allen of General Dynamics Advanced Information Systems, Lt General Bill Donahue, U.S. Air Force (retired) and Sam Gardiner, U.S. Air Force (retired);
- For briefings on the various legal dimensions of cyberattack and cyberexploitation, Thomas Wingfield of the Potomac Institute, LTC Eric Jensen of the Office of the Judge Advocate General, U.S. Army, Joe Dhillon of the McGeorge School of Law at the University of the Pacific, Jeff Smith (former CIA General Counsel), Jim Dempsey of the Center for Democracy and Technology, Richard Salgado of Yahoo!, Eugene Volokh of the UCLA School of Law, and Robert Weisberg and Helen Stacy of the Stanford University Law School;
- For briefings on the ethics of cyberattack, Jeff McMahan of Rutgers University and Father J. Bryan Hehir of Harvard University;

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

- For briefings on current DOD perspectives on cyberattack, Admiral Elizabeth Hight of the JTFGNO, LTC Forrest Hare of the U.S. Air Force, and Dr. Linton Wells of the Department of Defense;
- For briefings on policy issues regarding nonlethal weapons, David Koplow of Georgetown University;
- For briefings on private sector perspectives, Rod Wallace of Nortel, Milo Medin of M2Z Networks, Jeffrey I. Schiller of MIT, and Naveen Jain of Intelius;
- For a briefing on deterrence theory as it might be applied to cyberattack, Thomas Schelling of the University of Maryland; and
- For a variety of now-independent perspectives on the subject of cyberattack, Stephen Cambone (former Undersecretary of Defense for Intelligence), James N. Miller, Jr. (former Deputy Assistant Secretary of Defense for Requirements, Plans, and Counterproliferation), Dan Kuehl of the National Defense University, Stuart Starr of the Center for Technology and National Security Policy at the National Defense University, K.A. Taipale of the Center for Advanced Studies in Science and Technology Policy, Neal Pollard of Georgetown University and the National Counterterrorism Center, and Dorothy E. Denning of the Naval Postgraduate School.

Throughout the study, the committee's complex and challenging technical and political discussions encompassed a wide range of thought and perspectives offered by those who appeared before the committee, the committee itself, and participants in the review process. In addition, from the CSTB staff, we thank Ted Schmitt, Kristen Batch, and David Padgham for substantial research assistance, and Janice Sabuda and Eric Whitaker for administrative support. Lastly, this report would not have been possible without the leadership and stamina of Herb Lin, whose organizational skills, leadership of the staff, and thoughtful, complete agendas for committee discussion exceeded the excellent standards established by the National Academies. Both of us are indebted to Herb for his counsel, his policy and technical knowledge, his ability to find "just the right wording" for contentious areas, and for the character and chemistry he has shown us in our personal dealings. The National Research Council is fortunate to have leaders of Herb Lin's quality. This study and we co-chairs have benefited greatly from his deep involvement.

Kenneth W. Dam and William A. Owens, *Co-chairs*
Committee on Offensive Information Warfare

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

BOX P.1 Statement of Task

The National Research Council will appoint an ad hoc committee to examine policy dimensions and legal/ethical implications of offensive information warfare, informed by expert perspectives on and knowledge of the underlying technologies. These policy dimensions include but are not limited to factors that differentiate between cyberattack as a law enforcement matter versus cyberattack as a national security matter, the extent to which the U.S. Department of Defense is constrained from acting in response to cyberattack of uncertain origin, appropriate definitions of concepts such as "force" or "armed attack" as they apply to different forms of offensive information warfare, the standards of proof required to establish the origin of a cyberattack, the nature and extent of actions that the United States may take unilaterally against a foreign cyberattacker, the possible utility of offensive information warfare as a mode of attack that is different than kinetic or physical attack, the nature and extent to which offensive information warfare may be a part of conventional military operations, and the extent to which a nation undertaking offensive information warfare may increase the likelihood that it would be attacked in response, either similarly or dissimilarly. Project products will be directed at policy makers and researchers, the former so that decision-making can occur in a more informed manner and the latter so that other independent researchers will have a firm base on which to ground their own work.

Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Matt Blaze, University of Pennsylvania,
W. Earl Boebert, Sandia National Laboratories (retired),
Lewis M. Branscomb, Independent Consultant, La Jolla, California,
Jogindar (Joe) Dhillon, State of California,
Stephen Dycus, Vermont Law School,
Michael Froomkin, University of Miami School of Law,
Dan Geer, Geer Risk Services,
Ronald Lee, Arnold and Porter,
Martin Libicki, RAND Corporation,
James McCarthy, USAF Academy,
John McLaughlin, Johns Hopkins University,
Richard Mies, SAIC,
Gregory Rattray, Independent Consultant, San Antonio, Texas,
Abe Sofaer, Stanford University,
Eugene Spafford, Purdue University,
Phil Venables, Goldman Sachs & Co.,
Peter Weinberger, Google, Inc., and
Marc J. Zwillinger, Sonnenschein Nath & Rosenthal.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by William A. Press, University of Texas at Austin, and Eugene Volokh, University of California at Los Angeles. Appointed by the National Research Council, they were responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

SYNOPSIS	S-1
1 OVERVIEW, FINDINGS, AND RECOMMENDATIONS	1-1
1.1 What Is Cyberattack and Why Is It Important?	1-1
1.2 Focus of and Motivation for This Report	1-4
1.3 Cyberattack in the Context of an Information Strategy for the United States	1-6
1.4 Important Characteristics of Cyberattack and Cyberexploitation	1-8
1.5 Illustrative Applications of Cyberattack	1-9
1.6 The Legal Framework Governing Cyberattack	1-10
1.7 The Dynamics of Cyberconflict	1-11
1.8 Findings	1-12
1.8.1 Technologies as Instruments of U.S. National Policy	1-12
1.8.2 Overarching Findings	1-14
1.8.3 Legal and Ethical Findings	1-20
1.8.4 Policy Findings	1-25
1.8.5 Technical and Operational Findings	1-29
1.8.6 Organizational Findings	1-38
1.9 Recommendations	1-40
1.9.1 Fostering a National Debate on Cyberattack	1-41
1.9.2 Organizing the Decision-Making Apparatus of the U.S. Government for Cyberattack	1-45
1.9.3 Supporting Cyberattack Capabilities and Policy	1-49
1.9.4 Developing New Knowledge and Insight into a New Domain of Conflict	1-55
1.10 Conclusion	1-57

PART I

Framing and Basic Technology

2 TECHNICAL AND OPERATIONAL CONSIDERATIONS IN CYBERATTACK AND CYBEREXPLOITATION	2-1
2.1 Important Characteristics of Cyberattack and Cyberexploitation	2-1
2.2 The Basic Technology of Cyberattack	2-3
2.2.1 Information Technology and Infrastructure	2-3
2.2.2 Vulnerability, Access, and Payload	2-3
2.2.3 Scale and Precision	2-9
2.2.4 Critical Periods of Cyberattack	2-10
2.2.5 Approaches for Cyberattack	2-12
2.2.6 Propagating a Large-Scale Cyber Offensive Action	2-23
2.2.7 Economics	2-25
2.3 Operational Considerations	2-27
2.3.1 The Effects of Cyberattack	2-27
2.3.2 Possible Objectives of Cyberattack	2-31

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

2.3.3	Target Identification	2-32
2.3.4	Intelligence Requirements and Preparation	2-34
2.3.5	Effects Prediction and Damage Assessment	2-36
2.3.6	Complexity, Information Requirements, and Uncertainty	2-42
2.3.7	Rules of Engagement	2-43
2.3.8	Command and Control	2-44
2.3.9	Coordination of Cyberattack Activities with Other Institutional Entities	2-46
2.3.10	A Rapidly Changing and Changeable Technology and Operational Environment for Cyberattack	2-48
2.4	Characterizing an Incoming Cyberattack	2-49
2.4.1	Tactical Warning and Attack Assessment	2-49
2.4.2	Attribution	2-52
2.4.3	Intent	2-55
2.5	Active Defense for Neutralization as a Partially Worked Example	2-56
2.6	Technical and Operational Considerations for Cyberexploitation	2-61
2.6.1	Technical Similarities in and Differences Between Cyberattack and Cyberexploitation	2-61
2.6.2	Possible Objectives of Cyberexploitation	2-61
2.6.3	Approaches for Cyberexploitation	2-63
2.6.4	Some Operational Considerations for Cyberexploitation	2-64
2.7	Historical Precedents and Lessons	2-67

PART II

Mission and Institutional Perspectives

3	A MILITARY PERSPECTIVE ON CYBERATTACK	3-1
3.1	U.S. Military Doctrine and Cyberattack	3-1
3.2	Department of Defense Organization for Cyberattack	3-2
3.3	Rules of Engagement	3-2
3.4	Some Historical Perspective	3-2
3.5	Cyberattack in Support of Military Operations—Some Hypothetical Examples	3-2
3.5.1	Cyberattack in Support of Defense, Exploitation, and Other Information Operations	3-2
3.5.2	Cyberattack in Support of Traditional Military Operations	3-2
3.5.3	Cyberattack in Support of Other Operations	3-2
3.6	Operational Planning	3-2
3.7	Human Capital and Resources	3-2
3.8	Weapons Systems Acquisition	3-2
4	AN INTELLIGENCE COMMUNITY PERSPECTIVE ON CYBERATTACK AND CYBEREXPLOITATION	4-1
4.1	Intelligence Collection and Analysis	4-1
4.1.1	Governing Principles	4-1
4.1.2	How Cyberexploitation Might Be Used to Support Intelligence Collection	4-3
4.2	Covert Action	4-5
4.2.1	Governing Principles	4-5
4.2.2	How Cyberattack Might Be Used in Covert Action	4-7

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

4.3	Possible Intelligence Community Interest in Cyberattack and Cyberexploitation	4-10
5	Perspectives on Cyberattack Outside of National Security	5-1
5.1	Cyberattack and Domestic Law Enforcement	5-1
5.2	Threat Neutralization in the Private Sector	5-2
5.2.1	Possible Response Options for Private Parties Targeted by Cyberattack	5-2
5.2.2	Self-Defense by Private Parties	5-3
5.2.3	Regulating Self-Defense by Private Parties	5-7
5.2.4	Negative Ramifications of Self-Defense by Private Parties	5-8
5.3	Cyberexploitation in the Private Sector	5-11
5.4	Threat Neutralization on Behalf of Non-military Government Agencies	5-12
6	Decision Making and Oversight	6-1
6.1	Executive Branch	6-1
6.1.1	Declaratory Policy	6-1
6.1.2	Acquisition Policy	6-6
6.1.3	Employment Policy	6-9
6.1.4	Operational Oversight	6-14
6.2	Legislative Branch	6-16
6.2.1	War-making Powers	6-16
6.2.2	Budget	6-18
6.2.3	Oversight (and Notification)	6-19

PART III

Intellectual Tools for Understanding and Thinking About Cyberattack

7	Legal and Ethical Perspectives on Cyberattack	7-1
7.1	The Basic Framework	7-1
7.2	International Law	7-2
7.2.1	The Law of Armed Conflict	7-3
7.2.2	Applying the Law of Armed Conflict to Cyberattack	7-7
7.2.3	International Law and Non-state Actors	7-22
7.2.4	The Convention on Cybercrime	7-26
7.2.5	Human Rights Law	7-28
7.2.6	Reciprocity	7-29
7.3	Domestic Law	7-30
7.3.1	Covert Action and Military Activity	7-30
7.3.2	Title III and the Foreign Intelligence Surveillance Act	7-33
7.3.3	Posse Comitatus	7-35
7.3.4	The Computer Fraud and Abuse Act and Other Federal Law	7-35
7.3.5	The War Powers Resolution	7-37
7.3.6	Executive Order 12333 (United States Intelligence Activities)	7-37
7.4	Foreign Domestic Law	7-38
8	Insights from Related Areas	8-1
8.1	Nuclear Weapons and Nuclear War	8-1

PREPUBLICATION COPY – SUBJECT TO FURTHER EDITORIAL CORRECTION

8.2	Space	8-3
8.3	Biological Weapons	8-5
8.4	Non-Lethal Weapons	8-6
9	Speculations on the Dynamics of Cyberconflict	9-1
9.1	Deterrence and Cyberconflict	9-1
9.2	Escalatory Dynamics of Cyberconflict Between Nation-States	9-3
9.2.1	Crisis Stability	9-3
9.2.2	Escalation Control and Management	9-4
9.2.3	Complications Introduced by Patriotic Hackers	9-6
9.2.4	Incentives for Self-Restraint in Escalation	9-7
9.2.5	Termination of Cyberconflict	9-7
9.2.6	The Role of Transparency	9-8
9.2.7	Catalytic Cyberconflict	9-8
9.3	Cyberconflict Between the United States and Non-State Actors	9-8
9.4	The Political Side of Escalation	9-10
10	Alternative Futures	10-1
10.1	Regulatory Regimes—Basic Principles	10-1
10.2	Regulatory Regimes for Cyberattack	10-3
10.2.1	Direct Approaches Based on Traditional Arms Control	10-3
10.2.2	Indirect Approaches Based on Regulation of Non-Military Domains	10-7
10.3	Foreign Perspectives on Cyberattack	10-8

APPENDIXES

A	Committee Members and Staff	A-1
B	Meeting Participants and Other Contributors	B-1
C	Illustrative Criminal Cyberattacks	C-1
D	Views on the Use of Force in Cyberspace	D-1
E	Technical Vulnerabilities Targeted by Cyber Offensive Actions	E-1