




Emerging and Readily Available Technologies and National Security A Framework for Addressing Ethical, Legal, and Societal Issues

ISBN
978-0-309-29334-1

348 pages
6 x 9
PAPERBACK (2014)

Committee on Ethical and Societal Implications of Advances in Militarily Significant Technologies that are Rapidly Changing and Increasingly Globally Accessible; Computer Science and Telecommunications Board; Board on Life Sciences; Committee on Science, Technology, and Law; Center for Engineering, Ethics, and Society; National Research Council; National Academy of Engineering

 Add book to cart

 Find similar titles

 Share this PDF



Visit the National Academies Press online and register for...

- ✓ Instant access to free PDF downloads of titles from the
 - NATIONAL ACADEMY OF SCIENCES
 - NATIONAL ACADEMY OF ENGINEERING
 - INSTITUTE OF MEDICINE
 - NATIONAL RESEARCH COUNCIL
- ✓ 10% off print titles
- ✓ Custom notification of new releases in your field of interest
- ✓ Special offers and discounts

Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences. Request reprint permission for this book

Emerging and Readily Available Technologies and National Security — A Framework for Addressing Ethical, Legal, and Societal Issues

Jean-Lou Chameau, William F. Ballhaus, and Herbert S. Lin, *Editors*

Committee on Ethical and Societal Implications of Advances in Militarily
Significant Technologies That Are Rapidly Changing and Increasingly
Globally Accessible

Computer Science and Telecommunications Board
Board on Life Sciences
Committee on Science, Technology, and Law

Center for Engineering, Ethics, and Society Advisory Group

NATIONAL RESEARCH COUNCIL *AND*
NATIONAL ACADEMY OF ENGINEERING
OF THE NATIONAL ACADEMIES

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

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW 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 Defense Advanced Research Projects Agency under Award Number HR0011-11-C-0038. Any opinions, findings, conclusions, or recommendations 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.

International Standard Book Number-13: 978-0-309-29334-1

International Standard Book Number-10: 0-309-29334-0

Library of Congress Control Number: 2013958004

This report is available from

Computer Science and Telecommunications Board
National Research Council
500 Fifth Street, NW
Washington, DC 20001

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; <http://www.nap.edu>.

Copyright 2014 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. C. D. Mote, Jr., 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. C. D. Mote, Jr., are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

**COMMITTEE ON ETHICAL AND SOCIETAL IMPLICATIONS
OF ADVANCES IN MILITARILY SIGNIFICANT
TECHNOLOGIES THAT ARE RAPIDLY CHANGING
AND INCREASINGLY GLOBALLY ACCESSIBLE**

WILLIAM F. BALLHAUS, The Aerospace Corporation (retired),
Co-Chair
JEAN-LOU CHAMEAU, California Institute of Technology, *Co-Chair*
MARCUS FELDMAN, Stanford University
BRAN FERREN, Applied Minds
BARUCH FISCHHOFF, Carnegie Mellon University
MICHAEL GAZZANIGA, University of California, Santa Barbara
HANK GREELY, Stanford University
MICHAEL IMPERIALE, University of Michigan Medical School
ROBERT H. LATIFF, University of Notre Dame
JAMES MOOR, Dartmouth College
JONATHAN MORENO, University of Pennsylvania
JOEL MOSES, Massachusetts Institute of Technology
KENNETH OYE, Massachusetts Institute of Technology
ELIZABETH RINDSKOPF PARKER, University of the Pacific McGeorge
School of Law
SARAH SEWALL, Harvard University
ALFRED SPECTOR, Google, Inc.
JOHN H. TILELLI, JR., Cypress International, Inc.
STEPHEN J.A. WARD, University of Oregon

Staff

HERBERT S. LIN, Study Director and Chief Scientist, Computer Science
and Telecommunications Board (CSTB)
JON EISENBERG, Director, CSTB
ENITA WILLIAMS, Associate Program Officer, CSTB (through April
2013)
SHENAE BRADLEY, Senior Program Assistant, CSTB
ERIC WHITAKER, Senior Program Assistant, CSTB
RACHELLE HOLLANDER, Director, Center for Engineering, Ethics, and
Society
FRAZIER BENYA, Program Officer, Center for Engineering, Ethics, and
Society
JO L. HUSBANDS, Senior Program Officer, Board on Life Sciences
ANNE-MARIE MAZZA, Director, Committee on Science, Technology,
and Law

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

ROBERT F. SPROULL, University of Massachusetts, Amherst, *Chair*
LUIZ ANDRÉ BARROSO, Google, Inc.
ROBERT F. BRAMMER, Brammer Technology, LLC
EDWARD FRANK, Apple, Inc.
JACK L. GOLDSMITH III, Harvard Law School
SEYMOUR E. GOODMAN, Georgia Institute of Technology
LAURA HAAS, IBM Corporation
MARK HOROWITZ, Stanford University
MICHAEL KEARNS, University of Pennsylvania
ROBERT KRAUT, Carnegie Mellon University
SUSAN LANDAU, Google, Inc.
PETER LEE, Microsoft Corp.
DAVID LIDDLE, US Venture Partners
BARBARA LISKOV, Massachusetts Institute of Technology
JOHN STANKOVIC, University of Virginia
JOHN SWAINSON, Dell, Inc.
PETER SZOLOVITS, Massachusetts Institute of Technology
ERNEST J. WILSON, University of Southern California
KATHERINE YELICK, University of California, Berkeley

JON EISENBERG, Director
LYNETTE I. MILLETT, Associate Director and Senior Program Officer
VIRGINIA BACON TALATI, Program Officer
SHENAE BRADLEY, Senior Program Assistant
RENEE HAWKINS, Financial and Administrative Manager
HERBERT S. LIN, Chief Scientist, CSTB
ENITA WILLIAMS, Associate Program Officer (through April 2013)
ERIC WHITAKER, Senior Program Assistant

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

BOARD ON LIFE SCIENCES

JO HANDELSMAN, Yale University, *Chair*
ENRIQUETA C. BOND, Burroughs Wellcome Fund
ROGER D. CONE, Vanderbilt University Medical Center
SEAN EDDY, Howard Hughes Medical Institute
SARAH C.R. ELGIN, Washington University
DAVID R. FRANZ, Consultant, Frederick, Maryland
LOUIS J. GROSS, University of Tennessee, Knoxville
ELIZABETH HEITMAN, Vanderbilt University Medical Center
JOHN G. HILDEBRAND, University of Arizona, Tucson
RICHARD A. JOHNSON, Arnold & Porter, LLP
JUDITH KIMBLE, University of Wisconsin, Madison
CATO T. LAURENCIN, University of Connecticut
ALAN I. LESHNER, American Association for the Advancement of
Science
KAREN NELSON, J. Craig Venter Institute
ROBERT M. NEREM, Georgia Institute of Technology
CAMILLE PARMESAN, University of Texas at Austin
ALISON G. POWER, Cornell University
MARGARET RILEY, University of Massachusetts
JANIS WEEKS, University of Oregon
MARY WOOLLEY, Research!America

FRAN SHARPLES, Director
SAYYEDA "AYESHA" AHMED, Senior Program Assistant
CARL-GUSTAV ANDERSON, Program Associate
BETHELHEM M. BANJAW, Financial Associate
KATHERINE BOWMAN, Senior Program Officer
INDIA HOOK-BARNARD, Program Officer
JO L. HUSBANDS, Scholar/Senior Project Director
ANGELA KOLESNIKOVA, Temporary Program Assistant
JAY LABOV, Senior Scientist/Program Director for Biology Education
KEEGAN SAWYER, Associate Program Officer
MARILEE SHELTON-DAVENPORT, Senior Program Officer

COMMITTEE ON SCIENCE, TECHNOLOGY, AND LAW

DAVID KORN, Massachusetts General Hospital, *Co-Chair*
RICHARD A. MESERVE, Carnegie Institution for Science, *Co-Chair*
BARBARA E. BIERER, Harvard Medical School
ELIZABETH H. BLACKBURN, University of California, San Francisco
JOHN BURRIS, Burroughs Wellcome Fund
CLAUDE CANIZARES, Massachusetts Institute of Technology
ARTURO CASADEVALL, Albert Einstein College of Medicine
JOE S. CECIL, Federal Judicial Center
ROCHELLE COOPER DREYFUSS, New York University School of Law
DREW ENDY, Stanford University
MARCUS FELDMAN, Stanford University
JEREMY FOGEL, Federal Judicial Center
ALICE P. GAST, Lehigh University
BENJAMIN W. HEINEMAN, JR., Harvard Law School
D. BROCK HORNBY, U.S. District Court, District of Maine
WALLACE LOH, University of Maryland, College Park
MARGARET MARSHALL (retired), Massachusetts Supreme Judicial
Court
ALAN B. MORRISON, George Washington University Law School
CHERRY MURRAY, Harvard School of Engineering and Applied
Sciences
ROBERTA NESS, University of Texas School of Public Health
HARRIET RABB, Rockefeller University
DAVID RELMAN, Stanford University
RICHARD REVESZ, New York University School of Law
DAVID S. TATEL, U.S. Court of Appeals for the District of Columbia
Circuit

ANNE-MARIE MAZZA, Director
STEVEN KENDALL, Associate Program Officer

**CENTER FOR ENGINEERING, ETHICS, AND
SOCIETY ADVISORY GROUP**

JOHN AHEARNE, Sigma Xi, The Scientific Research Society, *Chair*
ALICE AGOGINO, University of California, Berkeley
STEPHANIE J. BIRD, Ethics Consultant and Co-Editor of *Science and
Engineering Ethics*
GLEN DAIGGER, CH2M HILL
GERALD E. GALLOWAY, JR., University of Maryland, College Park
DEBORAH JOHNSON, University of Virginia
WILLIAM KELLY, American Society for Engineering Education
FELICE LEVINE, American Educational Research Association
MICHAEL LOUI, University of Illinois at Urbana-Champaign
DONNA RILEY, Smith College
CHRIS SCHAIRBAUM, Texas Instruments, Inc.
CAROLINE WHITBECK, Case Western Reserve University
WILLIAM WULF, University of Virginia

RACHELLE D. HOLLANDER, Center Director
FRAZIER BENYA, Program Officer
SIMIL RAGHAVAN, Associate Program Officer
VIVIENNE CHIN, Administrative Assistant

Preface

In 2010, the Defense Advanced Research Projects Agency (DARPA) asked the National Academies to develop and articulate a framework for policy makers, institutions, and individual researchers that would help them think through ethical, legal, and societal issues (ELSI) as they relate to research and development on emerging and readily available technologies with military relevance.¹ The study was motivated in part by DARPA's experience earlier in the previous decade with programs that encountered difficulties related to privacy concerns and the realization that a more systematic approach to ethical, legal, and societal issues was an important ingredient for success in its mission of avoiding and creating surprise through R&D. Box P.1 contains the full charge to the Committee on Ethical and Societal Implications of Advances in Militarily Significant Technologies That Are Rapidly Changing and Increasingly Globally Accessible.

Coming from the Department of Defense (DOD), this concern—stated so explicitly—is relatively new. The DOD has long required a legal review of whether weapons are in conformance with the law of armed conflict, but this requirement applies only to weapons near procurement and

¹ DARPA's original charge to the committee used the term "democratized technologies" rather than "emerging and readily available technologies." Democratized or, equivalently, emerging and readily available technologies are those with rapid rates of progress and low barriers to entry. However, the committee believed that the term "democratized" is easily misunderstood, and this report uses the term "emerging and readily available technologies" (ERA technologies). More discussion of this topic is contained in Chapters 1 and 3.

Box P.1 The Project Statement of Task

The National Academies will develop a consensus report on the topic of ethical, legal, and societal issues relating to research on, development, and use of increasingly globally accessible and rapidly changing technologies with potential military application, such as information technologies, synthetic biology, and nanotechnology. This report will articulate a framework for policy makers, institutions, and individual researchers to think about such issues as they relate to these technologies of military relevance and to the extent feasible make recommendations for how each of these groups should approach these considerations in their research activities. A workshop to be held as early as practical in the study will be convened to obtain perspectives and foster discussion on these matters. A final report will be issued within 21 months of the project start, providing the National Research Council's and National Academy of Engineering's findings and recommendations.

not to R&D more generally. It is true that certain technologies—genome research, synthetic biology, and nanotechnology, for example—have in the eyes of the U.S. government warranted some degree of explicit attention to ethical, legal, and societal issues. In addition, there is a long history of academic work on ELSI concerns related to various civilian-oriented technologies. But for the most part, these technologies have been exploited for civilian purposes, and work on ethical, legal, and societal issues has been confined largely to that context.

ELSI concerns are inherently challenging, complex, and multidimensional, and their resolution often involves seeking common ground among individuals with deeply held but often unarticulated assumptions about ethics, culture, and epistemology. In some cases, finding common ground may be impossible to achieve in any reasonable time frame. Nevertheless, at the very least, ethical, legal, and societal issues are important enough to deserve serious exploration and attention, even if such common ground cannot be found, and in the committee's view, DARPA deserves great credit for being willing to raise such issues.

How ELSI expertise and scholarship developed in the context of civilian-oriented science and technology can be applied to the military context is a central theme of this report. But the lessons offered from that expertise and scholarship will require some modification for and adaptation to the military context—that is, they cannot be adopted wholesale, given that the military context does have a number of unique attributes.

Skeptics of the Department of Defense's attention to ELSI concerns

may well claim that any attempt to argue for uniqueness and processes different from those used for civilian-oriented research is tantamount to shoving hard issues under the table while maintaining a veneer of concern, but the committee does not share this point of view. That is, the committee recognizes the existence of real tensions between military missions (and the technology for supporting those missions) and traditional ELSI concerns. These tensions cannot be eliminated, but it is the committee's hope that this report can help senior leadership and program managers of agencies that support R&D for military and other national security purposes—including but not limited to DARPA—do a better job of managing these tensions. In addition, the report may also be of value to individual researchers, whether in the defense community or not, who work on the technologies discussed in this report and who may also be interested in the ELSI dimensions of their work.

The committee assembled for this project included individuals with expertise in risk analysis, perception, and communication; ethics; human rights; military operations; military acquisitions; national security law; organizational behavior; media/communications; bioethics; biomedical sciences; and information technology.

The committee first met in August 2011 and five times subsequently. Its earlier meetings were devoted primarily to workshops and plenary sessions for gathering input from a broad range of experts on a variety of topics related to ethical, legal, and societal issues associated with technology of different kinds used in different contexts; later meetings were devoted primarily to committee deliberations. (See Appendix A for brief biographies of committee members and staff and Appendix B for the agendas for the committee's information-gathering sessions.) The committee heard presentations related to military ethics and law, emerging contexts for military operations, future military missions and technologies for use in these missions, biomedical ethics and engineering ethics, risk assessment and communication, emerging technologies and ELSI concerns, mechanisms used by government agencies to address ethical, legal, and societal issues, approaches to embedding ethics in research and development, and non-U.S. perspectives on ethics in science and technology. In addition, the committee received input on specific emerging and readily available technologies, including information technology, neuroscience, prosthetics and human enhancement, synthetic biology, cyber weapons, robotics and automated weapons, and nonlethal weapons. Additional input included perspectives from professional conferences, the extant literature regarding ELSI concerns and science and technology, and government reports studied by committee members and staff.

ACKNOWLEDGMENTS

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 parties for presentations on the following dates:

- *August 30-31, 2011.* Shannon French (Case Western Reserve University), Ward Thomas (College of the Holy Cross), Judith Miller (formerly of the Department of Defense), Peter Schwartz (Global Business Network), Scott Wallace (U.S. Army (ret.)), George Lucas (U.S. Naval Academy), Patrick Lin (California Polytechnic State University), R. Alta Charo (University of Wisconsin Law School), and Joseph Herkert (Arizona State University).

- *November 2-3, 2011.* Peter Lee (Microsoft Research), Keith Miller (University of Illinois, Springfield), Gloria Mark (University of California, Irvine), Simson Garfinkel (Naval Postgraduate School), Scott Grafton (University of California, Santa Barbara), Craig Stark (University of California, Irvine), Martha Farah (University of Pennsylvania), Stuart Harshbarger (Contineo Robotics), Daniel Palanker (Stanford University), Gerald Loeb (University of Southern California), Nicholas Agar (Victoria University of Wellington, New Zealand), James Hughes (Trinity College), George Church (Harvard University), Drew Endy (Stanford University), Nita A. Farahany (Vanderbilt University), Judith Reppy (Cornell University), and George Khushf (University of South Carolina).

- *January 12-13, 2012.* Deborah Johnson (University of Virginia), Sheila Jasanoff (Harvard University, Kennedy School of Government), David Rejeski (Woodrow Wilson Center), Malcolm Dando (University of Bradford, United Kingdom), Kelly Moore (National Science Foundation), Jean McEwen (National Human Genome Research Institute), Valery Gordon (National Institutes of Health), Fred Cate (Indiana University School of Law), Ray Colladay (DARPA (ret.)), Mark Seiden (Yahoo!), Randall Dipert (University of Buffalo), Neil Rowe (Naval Postgraduate School), Ron Arkin (Georgia Institute of Technology), Peter Singer (Brookings Institution), Jürgen Altmann (Technische Universität Dortmund, Germany), Denise Caruso (Carnegie Mellon University), and Peter Hancock (University of Central Florida).

- *April 12-13, 2012.* Heather Douglas (University of Waterloo, Canada), Alex John London (Carnegie Mellon University), Nils-Eric Sahlin (Lund University, Sweden), Paul Fischbeck (Carnegie Mellon University), Wandu de Bruin (Carnegie Mellon University), Arthur Lupia (University of Michigan), Adam Finkel (Carnegie Mellon University), William Brinkman (U.S. Department of Energy, Office of Science), Carmen Maher (U.S. Food and Drug Administration, Office of the Chief Scientist), Edward Knipling (U.S. Department of Agriculture), Diana Hoyt (National Aeronautics and

Space Administration), Qiu Renzong (Chinese Academy of Social Science, China), Frans Brom (Utrecht University, The Netherlands), Steven Lee (Hobart and William Smith Colleges), and Montgomery McFate (U.S. Naval War College).

- *June 4, 2012.* George Perkovich (Carnegie Endowment for International Peace), David Fidler (Indiana University), and Neil Davison (International Committee of the Red Cross).

The committee also appreciates the support of Norman Whitaker from the Defense Advanced Research Projects Agency in the conduct of this project. In addition, the committee acknowledges the intellectual contributions of NRC and NAE staff: Herbert S. Lin (study director and chief scientist of the Computer Science and Telecommunications Board (CSTB)), Jon Eisenberg (director, CSTB), Enita Williams (associate program officer, CSTB), Rachele Hollander (director, Center on Engineering Ethics), Frazier Benya (program officer, Center for Engineering, Ethics, and Society), Anne-Marie Mazza (director, Committee on Science, Technology, and Law), and Jo Husbands (senior program officer, Board on Life Sciences). Shenae Bradley and Eric Whitaker (both senior program assistants for CSTB) provided administrative support. Special thanks are also due to Patricia Wrightson (associate director of the Board on Global Science and Technology), who contributed time and expertise as a staff consultant.

Jean-Lou Chameau, *Co-Chair*
William F. Ballhaus, *Co-Chair*

Committee on Ethical and Societal Implications of
Advances in Militarily Significant Technologies That Are Rapidly
Changing and Increasingly Globally Accessible

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:

Carlos Betha, United States Air Force Academy,
Kathleen Clark, Washington University School of Law,
Nancy Connell, University of Medicine and Dentistry of New Jersey,
David Fidler, Indiana University Maurer School of Law,
Shannon French, Case Western Reserve University,
Paul Gaffney, Monmouth University,
Elizabeth Heitman, Vanderbilt University Medical Center,
Deborah Johnson, University of Virginia,
David Korn, Harvard University,
Miltos Ladikas, University of Central Lancashire,
Maria Lapinski, Michigan State University,
Patrick Lin, California Polytechnic State University,
Lester L. Lyles, United States Air Force (retired),

Richard O'Meara, Rutgers University,
David Relman, Veterans Administration Palo Alto Health
Care System,
Robert F. Sproull, Oracle (retired),
Detlof von Winterfeldt, University of Southern California, and
John Weckert, Charles Sturt University.

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 Julia Phillips from Sandia National Laboratories and Kenneth Keller from the Johns Hopkins University Bologna Center. 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

SUMMARY	1
1 FRAMING THE ISSUES	15
1.1 National Security and the Role of Technology, 15	
1.2 Ethical, Legal, and Societal Issues in Science and Technology, 17	
1.3 ELSI Considerations for Science and Technology in a National Security Context, 23	
1.4 Emerging and Readily Available Technologies of Military Significance, 28	
1.5 Ethics of Armed Conflict, 34	
1.6 What Is and Is Not Within the Scope of This Report, 35	
1.7 A Roadmap to This Report, 43	
2 FOUNDATIONAL TECHNOLOGIES	45
2.1 Information Technology, 46	
2.1.1 Scientific and Technological Maturity, 46	
2.1.2 Possible Military Applications, 49	
2.1.3 Ethical, Legal, and Societal Questions and Implications, 52	
2.2 Synthetic Biology, 57	
2.2.1 Scientific and Technological Maturity, 58	
2.2.2 Possible Military Applications, 60	

2.2.3	Ethical, Legal, and Societal Questions and Implications, 61	
2.3	Neuroscience, 65	
2.3.1	Scientific and Technological Maturity, 67	
2.3.2	Possible Military Applications, 68	
2.3.3	Ethical, Legal, and Societal Questions and Implications, 74	
3	APPLICATION DOMAINS	79
3.1	Robotics and Autonomous Systems, 79	
3.1.1	Robotics—The Technology of Autonomous Systems, 80	
3.1.2	Possible Military Applications, 82	
3.1.3	Ethical, Legal, and Societal Questions and Implications, 83	
3.2	Prosthetics and Human Enhancement, 92	
3.2.1	The Science and Technology of Prosthetics and Human Enhancement, 92	
3.2.2	Possible Military Applications, 93	
3.2.3	Ethical, Legal, and Societal Questions and Implications, 94	
3.3	Cyber Weapons, 97	
3.3.1	The Technology of Cyber Weapons, 97	
3.3.2	Possible Military Applications, 98	
3.3.3	Ethical, Legal, and Societal Questions and Implications, 100	
3.4	Nonlethal Weapons, 103	
3.4.1	The Technology of Nonlethal Weapons, 104	
3.4.2	Possible Applications, 105	
3.4.3	Ethical, Legal, and Societal Questions and Implications, 106	
4	SOURCES OF ELSI INSIGHT	115
4.1	Insights from Synthesizing Across Emerging and Readily Available Technologies, 115	
4.2	Ethics, 118	
4.2.1	Philosophical Ethics, 118	
4.2.2	Disciplinary Approaches to Ethics, 120	
4.3	International Law, 129	
4.3.1	The Laws of War, 132	
4.3.2	International Human Rights Law, 138	
4.3.3	Arms Control Treaties, 140	

4.4	Social and Behavioral Sciences, 142	
4.4.1	Sociology and Anthropology, 143	
4.4.2	Psychology, 147	
4.5	Scientific and Technological Framing, 153	
4.6	The Precautionary Principle and Cost-Benefit Analysis, 154	
4.7	Risk Communication, 157	
4.8	Using Sources of ELSI Insight, 161	
5	AN ANALYTICAL FRAMEWORK FOR IDENTIFYING ETHICAL, LEGAL, AND SOCIETAL ISSUES	163
5.1	Stakeholders, 164	
5.1.1	Those Involved in or Connected to the Conduct of Research, 165	
5.1.2	Users of an Application, 168	
5.1.3	Adversaries, 168	
5.1.4	Nonmilitary Users, 171	
5.1.5	Organizations, 173	
5.1.6	Noncombatants, 174	
5.1.7	Other Nations, 175	
5.2	Crosscutting Themes, 175	
5.2.1	Scale, 175	
5.2.2	Humanity, 177	
5.2.3	Technological Imperfections, 179	
5.2.4	Unanticipated Military Uses, 180	
5.2.5	Crossovers to Civilian Use, 181	
5.2.6	Changing Ethical Standards, 182	
5.2.7	ELSI Considerations in a Classified Environment, 183	
5.2.8	Opportunity Costs, 185	
5.2.9	Sources of Insight from Chapter 4, 185	
5.3	An Example of Using the Framework, 186	
5.3.1	A Hypothetical Scenario for Analysis, 186	
5.3.2	A Process for Identifying Ethical, Legal, and Societal Issues, 186	
5.3.3	Questions Related to Stakeholders and Crosscutting Themes, 192	
5.3.4	Developing a Future Course of Action, 198	
5.4	The Framework in Context, 199	
5.4.1	A Summary of the Framework's Questions, 199	
5.4.2	Utility of the Framework, 205	
5.4.3	Identifying Fraught Technologies, 208	
5.4.4	Frequently Heard Arguments, 209	

6	GOING BEYOND INITIAL A PRIORI ANALYSIS	212
	6.1 Unanticipated Impacts, 212	
	6.2 Limits of A Priori Analysis, 213	
	6.2.1 The Limited Utility of Technology Forecasting, 213	
	6.2.2 Sources of Uncertainty in Technology Forecasting, 214	
	6.3 Broadening Predictive Analysis of Ethical, Legal, and Societal Issues, 219	
	6.3.1 Use of Deliberative Processes, 220	
	6.3.2 Anticipatory Governance, 226	
	6.3.3 Adaptive Planning, 227	
7	MECHANISMS FOR ADDRESSING ETHICAL, LEGAL, AND SOCIETAL ISSUES	230
	7.1 Characterizing Possible Mechanisms for Addressing Ethical, Legal, and Societal Issues, 230	
	7.2 What Mechanisms Have Been Used to Address Ethical, Legal, and Societal Issues?, 233	
	7.2.1 Self-regulation and Self-awareness, 233	
	7.2.2 Established Institutional Mechanisms, 235	
	7.2.3 Existing DARPA Efforts to Manage ELSI Concerns, 237	
	7.3 Considerations for Mechanisms Used to Address Ethical, Legal, and Societal Issues in the Context of Military R&D, 240	
8	FINDINGS AND RECOMMENDATIONS	245
	8.1 Synthesis, 245	
	8.2 Findings, 246	
	8.3 Recommendations, 251	
	8.3.1 Recommendations for Agencies, 251	
	8.3.2 Recommendation for Research-Performing Institutions and Individual Researchers, 265	
	8.4 Concluding Observations, 266	

APPENDIXES

A	Committee Members and Staff	271
B	Meeting Agendas and Participants	283
C	Research and Development Organizations Within the Department of Defense	298
D	Established Institutional Mechanisms for Addressing Ethical, Legal, and Societal Issues	306

Summary

FRAMING THE ISSUES

The United States faces a complex array of challenges to its national security. Technology is an essential element of the U.S. strategy for meeting those challenges, and it continues to be U.S. policy to seek technological military superiority over U.S. adversaries. To enhance and expand technological superiority, the Department of Defense and other government agencies invest in science and technology on an ongoing basis. These investments cover a broad range of efforts, from fundamental research that might eventually support national security needs, broadly defined, to specific development and eventual production of weapons and other military materiel intended to address particular national security problems. The U.S. government also adapts technologies originating in the civilian sector, initially without national security purpose, to national security needs.

Developments in science and technology (S&T) for military and national security use have often raised a variety of ethical, legal, and societal issues (ELSI). These ELSI-related challenges are accentuated in a context of emerging and readily available (ERA) technologies, that is, new technologies that are accessible at relatively low cost compared to more traditional militarily relevant technologies, such as nuclear weapons, and thus are within the reach of less technologically advanced nations, non-state actors, and even individuals. This is true because ERA technologies do not require construction of large engineered systems for their exploita-

tion, and in some cases have the potential for doing harm to U.S. interests on a large scale.

In 2010, the Defense Advanced Research Projects Agency asked the National Academies to develop a framework for policy makers, institutions, and individual researchers to use in thinking through ethical, legal, and societal issues as they relate to research and development (R&D) on ERA technologies with military or other national security relevance. What are the ethics of using autonomous weapons that may be available in the future? How should we think about the propriety of enhancing the physical or cognitive capabilities of soldiers with drugs or implants or prostheses? What limits, if any, should be placed on the development of cyber weapons, given the nature and extent of the economic damage that they can cause? Such questions illustrate the general shape of ethical, legal, and societal issues considered in this report.

This report begins with the assumption that defending and protecting national security against external threats are morally sound and ethically supportable societal goals. A related premise is that individuals who are part of the national security R&D establishment want to behave ethically.

That said, the notion of deliberately causing death and destruction, even in defense of the nation from external threats, raises ethical, legal, and societal issues for many. Those who engage in combat, those who support combatants, directly or indirectly, and those whom they defend—that is, the American public at large—all have a considerable stake in these issues and the questions they raise.

Knowledge regarding ethical, legal, and societal issues associated with R&D for technology intended for military purposes is not nearly as well developed as that for the sciences (especially the life sciences) in the civilian sector more generally. (This is generally true, even recognizing that the line between military and civilian technologies is not always entirely clear.) Some of the important differences between the two contexts include the following:

- Unlike civilian technologies, some military technologies are designed with the explicit purpose of causing harm to people and to property.
- Civilian technologies and products may unexpectedly turn out to be relevant to a military need and in that context raise the possibility of heightened and/or new ELSI implications.
- Technologies developed in a military context may turn out to have significant ELSI implications when applied in a civilian context.
- Advancing military technologies may also outpace the evolution of the laws designed to govern their use. For example, cyber weapons offer

the possibility that a nation might be brought to economic ruin without physical death and destruction.

- Some military research is conducted in a classified environment.

A full investigation of ethical, legal, and societal issues associated with technology for military or national security purposes is beyond the scope of this report. To make its task more manageable, the committee explored three areas with respect to ERA technologies:

- *The conduct of research*, which includes the selection of research areas, the design of particular research investigations (e.g., protocols, experiments), and the execution of those investigations. ELSI concerns relating to the conduct of research focus primarily on the effects of the research on parties other than those who are explicitly acknowledged as being research subjects, such as individuals living close to where the research is being performed, family members of research subjects, and so on. (ELSI concerns related to acknowledged research subjects are important, but there is today a well-developed infrastructure to address such concerns, and the adequacy of this infrastructure is not within the scope of this report.)

- *Research applications*, which relate to capabilities intended to result from research on ERA technologies. ELSI concerns associated with specified applications fall into two categories: concerns about the intended effects or purposes of the application and concerns about undesired effects (sometimes known as side effects) that might occur in addition to the intended effects. Concerns about technologies that can be used for both military and civilian purposes fall into this category.

- *Unanticipated, unforeseen, or inadvertent ELSI consequences* of either research or applications; such consequences are usually manifested by something going awry, as when research does not proceed as expected and thus causes harm outside the original bounds on the research or when unanticipated applications raise additional ELSI concerns.

FOUNDATIONAL TECHNOLOGIES AND APPLICATIONS

For illustrative purposes, this report considers three foundational technologies (foundational sciences and technologies) that enable progress and applications in a variety of problem domains: information technology, synthetic biology, and neuroscience. In addition, four application domains associated with specific operational military problems are addressed: robotics, prosthetics and human enhancement, cyber weapons, and nonlethal weapons. These technologies and applications are examples of ERA technologies as defined above—a multitude of state and nonstate

actors, friendly or not, can adopt and adapt such technologies for a multitude of purposes even without large budgets and infrastructures. The report examines each illustrative ERA technology and application domain from the perspective of technology maturity (how close the science or technology is to producing useful applications) and possible military applications, and it highlights some of the ELSI implications that emerge for each technology or application.

SOURCES OF INSIGHT ON ETHICAL, LEGAL, AND SOCIETAL ISSUES AND AN ANALYTICAL FRAMEWORK

A number of ideas, intellectual disciplines, and related efforts are sources of ELSI insight into both new and existing technologies and their applications. These include philosophical and disciplinary ethics; international law (especially the law of armed conflict and various arms control treaties); social and behavioral sciences; scientific and technological framing; the precautionary principle and cost-benefit analysis; and risk science and communication. Considered together, they help to provide an analytical framework consisting of three types of questions:

- *Questions regarding various stakeholders* that might have a direct or indirect interest in particular ELSI concerns and perspectives. Among these stakeholders are subjects of research, military users of a technology or application, adversaries, nonmilitary individuals or groups that might use a technology or application once R&D has been completed, organizations, noncombatants, and other nations.
- *Questions that cut across these stakeholder groups* and that cluster around a number of themes reflecting ELSI impacts related to scale, including, for example, degree of harm; humanity, including what it means to be human; technological imperfections; unintended military uses; and opportunity cost, among others.
- *Questions that arise from a consideration of the different sources of ELSI insight* described in Chapter 4.

Drawing on ELSI-related insights from the consideration of the three foundational ERA technologies and four ERA technology-based applications discussed in Chapters 2 and 3, the report sets forth a framework to help identify ethical, legal, and societal issues that might not otherwise be apparent to program officials. Addressing the relevant questions associated with each stakeholder should help to develop useful knowledge on ethical, legal, and societal issues regarding specific military R&D programs and projects. Such knowledge can be used to determine how and to what extent, if any, a program or project might be modified—or in

extreme cases abandoned—because of ELSI concerns. Use of this framework can thus provide input to policy makers, who will then have to make judgments about how, if at all, to proceed with a particular program or project; such judgments should be undertaken after, and not before, the policy makers have examined the issues raised by the questions posed in the framework.

GOING BEYOND AN INITIAL ANALYSIS

Using the analytical framework offered by this report is likely to bring to light some, although not all, of the ethical, legal, and societal issues associated with R&D on ERA technologies of military significance. Literally anticipating unanticipated ethical, legal, and societal issues is oxymoronic. But the ability to respond quickly to unanticipated issues that do arise can be enhanced by addressing in advance a wide variety of identified issues, because that exercise provides building blocks upon which responses to unanticipated ELSI concerns can be crafted.

In general, the task of anticipating ethical, legal, and societal issues that might emerge in the future would be much easier if the specific path of a given science or technology development were known in advance. However, the history of technology forecasting suggests that inaccurate technology forecasts are not unusual, because a variety of paths for any given scientific or technological development are possible. Also, it sometimes happens that military technologies are used in ways that differ significantly from the original conceptions of use.

Taking an approach that complements predictive analysis, policy makers have sometimes turned to deliberative processes that seek to include a broad range of perspectives and possible stakeholders in discussions of a given issue. From these different perspectives may well come the identification of new risks, questions of fact that have not previously been addressed, and specific knowledge or information that might not have been considered before.

To improve their ability to identify and respond to previously unanticipated ethical, legal, and societal issues that may emerge during the course of an R&D effort, policy makers have sometimes also used adaptive planning that allows them to respond quickly as new information and concerns arise in the course of technology development. Adaptive planning can be a useful way of proceeding despite profound uncertainties about the future. Policies for coping with uncertain environments should take into account the possibility of new information and/or new circumstances emerging tomorrow that can reduce these uncertainties, thus allowing (and indeed including planning for) midcourse corrections.

MECHANISMS FOR ADDRESSING ETHICAL, LEGAL, AND SOCIETAL ISSUES

Various organizations, both public and private, use a number of mechanisms to address different types of ethical, legal, and societal issues. Perhaps the most important mechanism for identifying problematic ELSI concerns that may be associated with a given research project is good judgment. That is, project proposers are expected to exercise good judgment in not submitting proposals that are unethical with respect to either the conduct of the research that would be supported or the applications that might result from that research. The same applies to program officials, who are expected not to approve or support projects that are unethical.

To support, develop, and enhance the judgment of individual project proposers and program officials, a number of mechanisms, sometimes topic specific, have been used to address ethical, legal, and societal issues—some apply to research, and some to actual deployments of technology. Mechanisms discussed in Chapter 7 and Appendix D include self-regulation and self-awareness; DOD law-of-armed-conflict review and treaty compliance; codes of ethics and social responsibility in science, engineering, and medicine; ELSI research; oversight bodies (such as institutional review boards); advisory boards; research ethics consultation services; chief privacy officers; environmental assessments and environmental impact statements; and drug evaluation and approval. However, these mechanisms have been developed for use primarily in civilian environments.

Adapting these ELSI mechanisms for the military R&D context must take into account the special characteristics of the military environment. In addition, those responsible must have an awareness of potential ethical, legal, and societal issues in the R&D effort; clear accountability and responsibility for addressing them; access to necessary expertise in ethics, law, and the social sciences, and to ELSI experts who in turn have access to relevant scientific and technical information; time to address ELSI concerns; and finally the involvement of a wide variety of perspectives, as well as comprehensiveness of and cooperation in attention to ethical, legal, and societal issues. Depending on their goals, policy makers will have to decide how far to go in any of these dimensions.

FINDINGS AND RECOMMENDATIONS¹

This report finds that **some developments in emerging and readily available technologies in a military context are likely to raise complex**

¹ Boldface below includes findings of the report.

ethical, legal, and societal issues, some of which are different from those associated with similar technologies in a civilian context. ERA technologies by their nature are associated with a very high degree of uncertainty about their future developmental paths, and thus a correspondingly broad range in the ethical, legal, and societal issues that are likely to emerge. Such breadth means that **the ELSI concerns that may be associated with a given technology development are very hard to anticipate accurately at the start of that development.** Using a diversity of sources of input with different intellectual and political perspectives on a given technology increases the likelihood that relevant ethical, legal, and societal issues will be revealed. Of course, when a particular technology development effort is classified, the universe of sources from which ELSI insights can be derived is more limited, and mechanisms for addressing ethical, legal, and societal issues that are predicated on the relative openness of civilian R&D (that is, unclassified work) are not likely to work as well.

Sustainable policy—policy whose goals and conduct can be supported over the long run—regarding science and technology requires decision makers to attend to the ELSI aspects of the S&T involved. High-quality science is one of the more important and obvious factors that contribute to the success of any particular R&D effort involving that science or technology. But inattention to ELSI aspects of an R&D endeavor can undermine even scientifically sound R&D efforts and call into question policy decisions that led to those efforts, regardless of their initial intent.

Public reaction to a given science or technology effort or application is sometimes an important influence on the degree of support it receives. A lack of support may manifest itself through adverse journalistic and editorial treatment, greater political scrutiny, reduced budgets (especially in a time of constrained finances), additional restrictions on research, and so on. On the other hand, a positive perception regarding the ethics of an R&D project may enhance public support for pursuit of that science or technology, irrespective of the scientific or technical basis for such pursuit.

Finally, any approach to promote consideration of ethical, legal, and societal issues in R&D of military significance will have to address how such plans are implemented at both the program and the project levels. Controversy and concern can easily be fueled by inadequate attention to detail and the manner of implementing oversight processes. For example, it is important that policies for addressing ethical, legal, and societal issues systematically have a “light footprint” when they are implemented by program managers. The intent of the committee’s findings and recommendations is not to impose undue compliance requirements on program managers or agencies, but rather to help well-meaning program manag-

ers in these agencies do their jobs more effectively and to help ensure that basic American ethical values (such as those embodied in the U.S. Constitution's Bill of Rights) are not compromised. The exercise of common sense, judgment, and understanding of the fundamental intent of policies to address ethical, legal, and societal issues—not simply formal compliance—is the goal and is an important foundation for developing an ELSI-sensitive culture.

The foregoing findings (shown in boldface type) help to shape the committee's five recommendations, the first four of which are directed to agencies sponsoring research with military significance. The term "interested agency" as used below means agencies interested in addressing ethical, legal, and societal issues associated with the research they support.

Recommendation 1: The senior leaders of interested agencies that support R&D on emerging and readily available technologies of military significance should be engaged with ethical, legal, and societal issues in an ongoing manner and declare publicly that they are concerned with such issues. Such a public declaration should include a designation of functional accountability for ethical, legal, and societal issues within their agencies.

High-level support from senior agency leadership is required if an agency is to seriously address ethical, legal, and societal issues associated with the research it funds. Such support must be visible and sustained over time; in its absence, little will happen. An agency's senior leadership sets the tone by publicly communicating to the organization and its stakeholders the importance of addressing ethical, legal, and societal issues, the willingness of the agency to learn from outside perspectives, and the intent of the ELSI-related processes. In the long run, these are key elements in creating an institutional culture that is sensitive to ELSI concerns.

Accountability at all levels of an agency, including at the senior management level, is necessary to ensure that attending to ethical, legal, and societal issues is not haphazard and uncoordinated. To maximize the likelihood that ethical, legal, and societal issues will be addressed, an agency's senior leadership should designate a point of functional accountability for this responsibility. Parties with functional accountability provide a second line of defense against overlooking ELSI concerns that complements the primary role played by project teams in executing a program.

Recommendation 2: Interested agencies that support R&D on emerging and readily available technologies of military significance should develop and deploy five specific processes to enable these

agencies to consider ethical, legal, and societal issues associated with their research portfolios.**2.a–Initial screening of proposed R&D projects**

Before supporting any research in a particular S&T area, agencies should conduct a preliminary assessment to identify ethical, legal, and societal issues that the research might raise. In addition, all researchers should identify in their proposals to an agency plausible ELSI concerns that their research might raise. Using such information as a starting point, the funding agency should then make its own assessment about the existence and extent of such issues. Note that this initial assessment should be carried out for all R&D projects (both classified and unclassified).

At this stage, the goal is to identify explicitly whether the research would raise significant ethical, legal, and societal issues that require further consideration. Mostly, the answer will be “no,” and assessment of the proposed research project will proceed without any further consideration of ethical, legal, and societal issues. For the proposals that warrant a “yes,” the process in Recommendation 2.b comes into play.

2.b–Reviewing proposals that raise ELSI concerns

Once an agency has identified research proposals or projects that may raise significant ethical, legal, and societal issues, some closer scrutiny is needed to ascertain how likely it is that such issues will arise, how serious they are likely to be, and whether there are ways to mitigate them. Use of a systematic methodology, such as the analytical framework described in this report, can be helpful for identifying ethical, legal, and societal issues.

If and when such issues are identified, program managers should have the opportunity to take action in response. (Of course, program managers are themselves subject to higher authorities, and the latter may take action as well.) Possible responses include not pursuing a given R&D effort, pursuing it more slowly, pursuing it in a modified form that mitigates the identified ethical or societal concerns, pursuing the original effort but also pursuing research to better understand the ethical or societal impacts, and so on. The responses should not be limited simply to a decision to proceed or not to proceed.

Furthermore, it should be expected that the initial assessment will not be correct in all aspects. But the initial assessment will assemble resources that are likely to be helpful in formulating a response to unforeseen circumstances, even if these resources are used in ways that are very different from what an original plan specified. In addition, the initial assessment is a concrete point of departure for evolving an approach to handling ethi-

cal, legal, and societal issues as circumstances change. Information from the assessment should be made available to modify the research proposal for mitigating ELSI concerns should that be appropriate.

2.c—Monitoring R&D projects for the emergence of ethical, legal, and societal issues and making midcourse corrections when necessary

Perfect prediction of significant ELSI concerns is virtually impossible, especially in an area as fraught with uncertainty as research on emerging and readily available technologies. Projects that seemed to raise significant ethical, legal, and societal issues may turn out to raise none; projects that seemed to have no ethical or societal implications may turn out to have hugely important consequences.

A process for monitoring the course of R&D projects is thus essential to help agencies to adjust to such changing realities. If the perceived ethical, legal, and societal issues change significantly during the course of a project (that is, if and when new issues are identified or previous attempts to address already-identified issues prove inadequate), the program or project plan can be modified accordingly. Such an adaptive approach plans for and relies on continual (or at least frequent) midcourse changes in response to such feedback.

A monitoring process could, in principle, be similar to the initial screening process, with the important proviso that the baseline be updated to take into account what has been learned since the project was last considered. To catch ethical, legal, and societal issues that may have appeared in the interim, the monitoring process should touch all projects in the agency's R&D portfolio, so that projects that were previously determined not to raise ethical, legal, and societal issues can be reexamined. But the intent of this requirement is not to reopen a debate over a project as initially characterized but rather to see if new issues have arisen since the last examination—and in most cases, a project originally determined to not raise ethical, legal, and societal issues will retain that status upon reexamination. It may also be the case that projects originally determined to raise ethical, legal, and societal issues have evolved in such a way that it becomes clear that they do not.

2.d—Engaging with various segments of the public as needed

With the stipulation that engagement with various segments of the public does not necessarily mean coming to consensus with them, an agency's ELSI deliberations will often benefit from such external engagement. For example, public concerns about a given R&D project are often formulated in ELSI terms rather than in technical terms. Policy makers

must be prepared for the emergence of unforeseen outcomes and thus must have structures in place that will detect such outcomes and focus attention on them in a timely way. When unforeseen outcomes do emerge, policy makers must be prepared to communicate with the public using proven techniques. A developed strategy for public communication is also useful when anticipated ELSI concerns become public. Government actions in the United States ultimately depend, legally and practically, on the consent of the governed. Building public understanding of an agency's actions, the reasons for those actions, and the precautions the agency has taken will normally be the best strategy, for democracy and for the agency.

In addition, members of the public (including, for example, technical experts, experts on risk assessment and communication, and those with ELSI expertise broadly defined) may have points of view that were not well represented in an agency's internal deliberations about a given R&D project. Ongoing engagement throughout the course of a project may reveal the impending appearance of initially unanticipated ethical, legal, and societal issues, and thus provide early warning to program managers and enable a more rapid response if and when these new issues do appear. Finally, the mere fact of consultation and engagement with a wide range of stakeholders helps to defuse later claims that one perspective or another was ignored or never taken into account.

Finally, a relevant stakeholder group is the community of researchers themselves. An agency should not suddenly introduce substantive changes in its requirements for proposals without informing the research community about what those changes mean. What is the rationale for these changes? How, if at all, will research projects have to change? What, if anything, does "attending to ethical, legal, and societal issues" mean in the context of decisions about specific proposals?

For R&D projects that are classified, public engagement is obviously constrained to a certain extent. Nevertheless, even if such projects can be discussed only with the cleared subsets of the various stakeholder groups, the result will still be more robust and defensible than if the project had not been discussed at all.

2.e—Periodically reviewing ELSI-related processes in an agency

Well-meaning policy statements are sometimes translated into excessively bureaucratic requirements. To ensure that ELSI-related processes do not place undue burdens on researchers or on program managers in an agency, these processes should themselves be reviewed periodically to ensure that they are consistent with the intent of high-level policy statements regarding the agency's handling of ethical, legal, and societal issues.

Recommendation 3: Interested agencies supporting R&D on emerging and readily available technologies of military significance should undertake an effort to educate and sensitize program managers to ethical, legal, and societal issues.

If funding agencies are to screen, assess, and monitor research proposals and projects for possibly significant ethical, legal, and societal issues, they will need people with the ability to recognize those issues. The fields that assess ELSI concerns arising with various technologies have their own vocabularies. At the very least, the agency personnel dealing with these issues will have to understand, at some level, the relevant “language.” At the same time, those with ELSI responsibilities and/or expertise must have some understanding of the underlying research in order to identify issues that may or may not emerge.

One crucial, and easily overlooked, aspect of building internal expertise is building history. If an agency has no institutional memory of what ethical, legal, and societal issues it has faced in its history, how it dealt with those issues, and what the consequences were, its ability to learn from that past is diminished. This diminished capability will be a particular problem for agencies that have frequent turnover. An interested agency needs to make it a priority to collect—and to use—information about how it has dealt with these issues. The agency person or group in charge of screening proposals or projects for ethical, legal, and societal issues might be in a good position to collect and organize that kind of information.

Recommendation 4: Interested agencies supporting R&D on emerging and readily available technologies of military significance should build external expertise in ethical, legal, and societal issues to help address such issues.

Not all expertise should be, or can be, internal to an agency. Agencies should seek advice from external experts because properly addressing some ELSI concerns will require a depth of knowledge that cannot realistically be expected of program managers or scientists. If such expertise is not immediately available, it should be cultivated. Such cultivation would have both immediate and longer-term benefits. It would help the agency directly by providing that expertise, but, in the longer run, it could also build knowledge, expertise, and even trust outside the agency about what it does about ethical, legal, and societal issues, and why.

The committee also makes one recommendation to research-performing institutions.

Recommendation 5: Research-performing institutions should provide assistance for researchers attending to ethical, legal, and societal issues in their work on emerging and readily available technologies of military significance.

Recommendations 1 through 4 address government agencies that fund research on emerging and readily available technologies of military significance. To the extent that these recommendations are adopted, researchers supported by these agencies may need assistance in identifying and responding to ethical, legal, and societal issues with which they may be unfamiliar. The committee believes that universities and other research-performing organizations should provide such assistance when needed by the researchers working under their aegis, in much the same way that they provide other functional support to these researchers.

In addition, many institutions performing research on emerging and readily available technologies with military significance already have in place policies and procedures to address a variety of ethical, legal, and societal issues that arise in S&T research. For example, institutional review boards for research involving human subjects are quite common. Leveraging policies and procedures already in place to address ELSI concerns associated with certain kinds of research will help to minimize unnecessary overhead in institutions performing research on ERA technologies with military significance, and where policies and procedures already exist to address ethical, legal, and societal issues that are common to both military and civilian-oriented research, new ones should not be created to address them.

1

Framing the Issues

1.1 NATIONAL SECURITY AND THE ROLE OF TECHNOLOGY

The United States faces a broad and complex array of challenges to its national security. Its potential adversaries cover a broad range, including nations large and small, organized terrorist groups, drug cartels, organized crime, and even individual terrorists. The weapons they use (or wish to use) cover an equally broad range and include conventional military weapons, weapons of mass destruction and disruption, improvised explosive devices, and cyber/information warfare. Moreover, the scope and the nature of threats facing the nation are constantly evolving.

The armed forces of the United States exist to deter its adversaries from threatening action against it, its allies, and its interests more broadly. In the words of the *National Security Strategy 2010*, “We are strengthening our military to ensure that it can prevail in today’s wars; to prevent and deter threats against the United States, its interests, and our allies and partners; and prepare to defend the United States in a wide range of contingencies against state and nonstate actors.”¹ In the event that deterrence fails, the United States structures and equips its armed forces with the personnel and tools they need to defeat adversary threats, although U.S. policy calls for a military approach only when other approaches, such as diplomacy, are unsuccessful in resolving disagreements between nations or controlling threats to U.S. national security.

¹ See http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

America's experience at war and in planning for war since the end of World War II has persuaded military planners that technological military superiority is the best way to approach this goal. That is, the U.S. approach to national security emphasizes technologically derived qualitative advantages over its adversaries, and technology is an integral aspect of national security. (By contrast, the U.S. approach to armed conflict during World War II generally placed much greater emphasis on the large-scale production of weapons rather than technological superiority.)

Technology supports a number of military functions. For example, weapons are the tools that cause direct effects against an adversary, such as when a bomb explodes on the battlefield. Technologies for command, control, intelligence, surveillance, and reconnaissance (C4ISR) help decision makers ensure that these effects occur when and where they are intended to occur; for example, a system for data analysis identifies an important target that would otherwise be overlooked or collateral damage that might result from an attack. Countermeasures seek to frustrate an adversary's use of weapons and C4ISR systems. Logistics provide indirect support for the personnel involved, such as food, fuel, transportation, and medical assistance.

Adversaries also seek technologically enabled capabilities for their own purposes, and sometimes they are influenced by demonstrations that a given technology has proven useful in practice. Indeed, sometimes the utility of such a technology is demonstrated by the United States itself. Those adversaries can acquire and adapt for their own use the technologies that the United States develops, can find alternative technologies that are more available or less expensive (e.g., commercial products), and can identify ways to negate U.S. technological advantages. They may also give the technology or the ability to create the technology to others for use against the United States.

To enhance and expand technological superiority, the Department of Defense (DOD) and other government agencies invest in science and technology (S&T) on an ongoing basis. (Investment in technologies for military purposes sometimes has benefits for the civilian world as well.) These investments cover a broad range from fundamental science that might eventually support national security needs, broadly defined, to specific development and eventual production efforts intended to address particular national security problems. (In some cases, the national security problem for the United States is the possibility that an actual or potential adversary will develop a new capability.) In addition, the U.S. government adapts technologies originating in the civilian sector, without national security in mind, to national security needs.

The development of technology for national security needs is a complex endeavor, given the strategy of technological superiority as well as

changes in the technological and societal environment. These changes are discussed in greater detail in Section 1.4, “Emerging and Readily Available Technologies of Military Significance.”

The U.S. Office of Management and Budget uses the following definitions for research and development:²

- Basic research is defined as “systematic study directed toward fuller knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications toward processes or products in mind. Basic research, however, may include activities with broad applications in mind.” An example might be research in quantum computing, a field that is at the forefront of basic research even as its potential for revolutionary advancements in computing is acknowledged [even without specific applications in mind].
- Applied research is defined as “systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met.” An example is research to improve flight control for remotely piloted aircraft.
- Development is defined as “systematic application of knowledge or understanding, directed toward the production of useful materials, devices, and systems or methods, including design, development, and improvement of prototypes and new processes to meet specific requirements.” An example is technical work needed to meet a particular range requirement for a particular remotely piloted aircraft.

The categories of activity described above speak to how the DOD may invest in S&T research, from which may emerge findings and results that can lead to military applications. But, of course, the DOD does not live in a closed environment, and today it also keeps track of civilian S&T that might have military application. Indeed, civilian S&T are sometimes more mature and developed than S&T overtly developed for military purposes. Civilian science and technology may be introduced at any appropriate stage.

1.2 ETHICAL, LEGAL, AND SOCIETAL ISSUES IN SCIENCE AND TECHNOLOGY

U.S. investment in science and engineering research and development (R&D) has been substantial, and its results have helped to shape physi-

² Executive Office of the President, Office of Management and Budget Circular No. A-11 (2012), Section 84, page 11, available at http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a_11_2012.pdf.

cal and social landscapes throughout the world. Policy makers seek new science and technology largely because of the larger range of policy and programmatic options they afford. But efforts to develop new S&T have also raised concerns about a variety of ethical, legal, and societal issues (ELSI).³ Furthermore, many such concerns emerge from the increasingly global scope of certain new technologies and the applications these technologies enable.

This report uses the adjective “ethical” to describe issues that are matters of principle (what people regard as right). By contrast, “social” or “societal” is used in reference to issues that are matters of interests (what people regard as desirable). Often the two will overlap. People should always desire the things that they believe are right. However, they may also desire things without invoking a moral principle. Both can refer to how choices are made, which actions are taken, and what outcomes arise. Ethical issues are often illuminated by analysis (e.g., philosophy) and social issues by empirical research (e.g., psychology, sociology). However, each can inform the other (as when analysis suggests topics for empirical research or when such research identifies behavior worth analyzing).

As for the relationship between law and ethical/societal issues, it is true that law is intrinsically a part of those issues. Law establishes authority to decide questions (who decides), set substantive limits on the content of decisions (what gets decided), and create processes or procedures for decision making (how decisions get made). Law can channel how policy makers make decisions when ethical or societal consensus is lacking, and indeed law is often the essential point of departure for a consideration of ethical or societal issues. Legal concerns often become more salient as a given weapons concept unfolds from R&D to deployment to use.

However, against the backdrop of an evolving legal context and understanding is the reality that law and ethics are not identical, and even well-established law cannot be the final word on ethical and societal issues for several reasons:

- Established law may not even address ethical or societal issues that are important in any given instance. The relationship of legal, ethical, and societal factors is not always straightforward, although they do overlap in some cases. In general, the law is supposed to reflect the ethical, as well as the practical, values of the community to which it applies. Law can thus be an expression of both ethical and societal concerns, but it is not always so. By contrast, ethical and societal considerations are not bounded by their expressions in law; indeed, some are not captured by law at all,

³ The acronym ELSI stands for “ethical, legal, and societal issues” and is strictly speaking a noun. However, this report uses the acronym as an adjective.

perhaps because it may not be possible to condense an ethical or societal concern to a simple expression of black-letter law. Most importantly, in many cases the emergence of ethical and societal concerns leads the development of law. In this interval, decision makers have to cope with such concerns and the controversies they may engender in the absence of formal (e.g., legal) guidance for their decisions.

- The interpretation of established law may depend on the particular facts and circumstances of any research problem. For example, a law may prohibit the use of human subjects under conditions that expose those subjects to significant danger. What counts as “significant” danger? Resolving this question is, by definition, not a matter for law unless the law provides some specific definition for “significant”—which it often does not. Moreover, there is often profound disagreement in many instances about what is ethical, a disagreement often reflected in laws that are ambiguous or incomplete. Law, which is usually designed to withstand rapid changes in popular opinion, may be unclear in its practical application. Thus, a debate rages today within the United States about the scope of constitutional protections when drones are used to carry out targeted killings, and disagreement about the morality or “rightness” of that use is even more heated. That is, new circumstances may highlight tensions between ethical and legal constructs that might otherwise be overlooked.

- The ethical and societal environment extant at the time a law might be applied could be very different from that at the time the law was formulated. Although some degree of ethical or societal consensus may have to be present when a given law is enacted or otherwise goes into force, that consensus may no longer be operative at the moment policy makers must make a decision about a given research effort. That is, laws themselves are sometimes overtaken by events that call into question some of their underlying but unstated ethical assumptions. Similar considerations apply for new technological capabilities that may not have been anticipated in the initial formulation of a law.

- Strategic or tactical concerns also may not line up well with ethical considerations. For example, a decision to develop a new weapon system for use under particularly exigent circumstances might be considered by some to be ethically objectionable (e.g., because of the bad precedents its use might set) and by others to be tactically necessary (e.g., because of the lives its use might save in a particular situation).

If any of these reasons is relevant to a given decision-making situation, the law may not by itself be in any way final or dispositive. In such cases, decision makers have no choice but to refer to the ethical principles that they believe were inherent in the initial formulations of the law.

Research and deliberation can guide the examination of ethical, legal, and societal concerns. Without such examination, public policies and programs may not be stable and sustainable. Law and regulation are expressions of public policy that reflect societal concerns and establish norms or standards regarding how to address those concerns.

ELSI concerns regarding S&T are not new.⁴ For example, in the years after World War II, governments have made efforts to come to grips with some of the ethical concerns that result from developments and research practices in S&T. These efforts span a broad range, and they include (but are not limited to) the following:

- In 1946, the postwar Nuremberg trials resulted in the convictions of a number of German physicians and bureaucrats who conducted or facilitated horrific medical experiments on concentration camp prisoners. These trials have become an important point of departure for international discussions on bioethics issues.

- In 1972, the United States signed the Convention on the Prohibition of the Development, Production and Stockpiling of Biological and Toxin Weapons and on Their Destruction (usually known as the Biological Weapons Convention (BWC)),⁵ in part for ethical reasons.⁶ The BWC bans “the development, production, stockpiling, acquisition and retention of microbial or other biological agents or toxins, in types and in quantities that have no justification for prophylactic, protective or other peaceful purposes,” and “weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict.” The actual use of biological weapons is prohibited by the 1925 Geneva Protocol.⁷

- In 1979, the Belmont report of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research presented three basic ethical principles regarding the conduct of biomedical research involving human subjects: respect for persons (e.g., research subjects should be treated as autonomous), beneficence (e.g., research subjects should not be harmed), and justice (benefits and costs of research

⁴ An overview of this subject can be found in Carl Mitcham, *Encyclopedia of Science Technology and Ethics*, Macmillan Reference, Detroit, Mich., 2005.

⁵ See <http://www.opbw.org/>.

⁶ The U.S. decision to sign the BWC was also influenced by the conclusion of the U.S. military that biological weapons had little military utility and that signing the convention would not deprive the United States of a significant military capability.

⁷ The 1925 protocol is formally known as the Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare. See <http://www.un.org/disarmament/WMD/Bio/1925GenevaProtocol.shtml>.

should be shared equitably).⁸ The Belmont report and other reports by the National Commission formed the basis of regulations implementing these principles that govern the conduct of most federally supported research involving human subjects. These regulations, usually known collectively as the Common Rule, require institutions to establish institutional review boards (IRBs) that approve, modify, or reject such research.

- In the late 1980s, the Human Genome Project (HGP) established a program of research on ethical, legal, and societal issues associated with sequencing the human genome. Such issues include questions of how genetic information should be interpreted and used, who should have access to it, and how people could be protected from the harm that might result from the improper disclosure or use of such information.

- In 1993, the United States signed the Chemical Weapons Convention (CWC),⁹ in part for ethical reasons. The CWC bans the development, production, stockpiling, and use of chemical weapons, although the CWC acknowledges the benefits of peaceful chemistry and the desire to promote free trade in chemicals and international cooperation in chemical activities not prohibited by the convention.

- In 2001, the National Nanotechnology Initiative (NNI) was launched. One of the NNI's goals is promoting the responsible development of nanotechnology, an important component of which is the consideration of the ethical, legal, and societal implications associated with nanotechnology research and development, and the development of plans for addressing environmental, health, and safety implications as well. Some of the issues include how applications of nanotechnology research are introduced into society; how transparent the related decision-making processes are; and how sensitive and responsive policies are to the needs of the full range of stakeholders. To help explore the ethical, legal, and societal issues associated with nanotechnology research, NNI agencies support two centers for nanotechnology in society, at Arizona State University and the University of California, Santa Barbara, and also incorporate ELSI components in their new nanotechnology R&D programs.

Nongovernmental organizations and individuals have also mounted important efforts, which include the following:

- In 1955, the Russell-Einstein manifesto addressed the dangers of nuclear war, arguing that the use of nuclear weapons threatened the continued existence of mankind.

⁸ The Belmont report can be found at <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>.

⁹ See <http://www.opcw.org/chemical-weapons-convention/about-the-convention/>.

- In 1964, the Declaration of Helsinki was adopted by the World Medical Association as a statement of ethical principles for medical research involving human subjects, including research on identifiable human material and data. Since then, the declaration has undergone several revisions and clarifications.

- In 1974, the paramouncy clause was first included in a code of engineering ethics. It obligates engineers to “hold paramount the safety, health and welfare of the public and protect the environment in performance of their professional duties.”¹⁰

- In 1983, the U.S. Catholic Bishops issued their Pastoral Letter on War and Peace, a document that spoke to the dangers of nuclear war from an ethical perspective grounded in Catholic theology.¹¹

- In 2005, the National Council of Churches issued an open letter titled “God’s Earth Is Sacred: An Open Letter to Church and Society in the United States,” an ecumenical statement on the environment that argued “the central moral imperative of our time is the care for Earth as God’s creation.”¹²

- In 2009, the National Academies issued the third edition of *On Being a Scientist*, which notes that “the standards of science extend beyond responsibilities that are internal to the scientific community. Researchers also have a responsibility to reflect on how their work and the knowledge they are generating might be used in the broader society.”¹³

In some instances, the efforts of government and nongovernment bodies have been intimately intertwined. A well-known example is the story of the National Institutes of Health (NIH) Recombinant DNA Advi-

¹⁰ See Carl Mitcham, *Encyclopedia of Science Technology and Ethics*, Macmillan Reference, Detroit, Mich., 2005, p. 265; and Charles E. Harris, Jr., Michael S. Pritchard, and Michael Jerome Rabins, *Engineering Ethics: Concepts and Cases*, Wadsworth Publishing, Belmont, Calif., 1995.

¹¹ The letter can be found at <http://old.usccb.org/sdwp/international/TheChallengeofPeace.pdf>.

¹² The letter can be found at <http://www.ncccusa.org/news/godsearthissacred.html>.

¹³ The second edition of *On Being a Scientist*, issued in 1995, said:

Even scientists conducting the most fundamental research need to be aware that their work can ultimately have a great impact on society . . . [and] tremendous societal consequences. The occurrence and consequences of discoveries in basic research are virtually impossible to foresee. Nevertheless, the scientific community must recognize the potential for such discoveries and be prepared to address the questions that they raise. If scientists do find that their discoveries have implications for some important aspect of public affairs, they have a responsibility to call attention to the public issues involved. . . . science and technology have become such integral parts of society that scientists can no longer isolate themselves from societal concerns.

See National Research Council, *On Being a Scientist*, National Academy Press, Washington, D.C., 1995, pp. 20-21.

sory Committee and the Asilomar conference in the early 1970s. In 1973, a letter published in *Science* described the recommendations of the National Academy of Sciences' Committee on Recombinant DNA Molecules,¹⁴ including a recommendation that life scientists voluntarily refrain from conducting certain kinds of experiments involving recombinant DNA until the potential hazards were better understood. Largely in response to this letter, the NIH in 1974 established the Recombinant DNA Advisory Committee to address public concerns regarding the safety of manipulating genetic material through the use of recombinant DNA techniques.¹⁵ In 1975 and with the support of the NIH and others, the Asilomar conference hosted many of the world's leading researchers on recombinant DNA to consider the hazards of such research. One key outcome of the conference was the establishment of voluntary guidelines to improve the safety of recombinant DNA technology.¹⁶

1.3 ELSI CONSIDERATIONS FOR SCIENCE AND TECHNOLOGY IN A NATIONAL SECURITY CONTEXT

The development of any new science or technology often raises ELSI concerns. But the scope and nature of these concerns depend on the specific science or technology in question and the context in which it is found. This report focuses on the ethical, legal, and societal issues that may be associated with science and technology (S&T) of relevance to military problems.

The report assumes that defending and protecting national security and protecting the individuals involved are widely regarded as morally sound and ethically supportable societal goals. A related premise is that individuals who are part of the national security establishment (that is, those who make decisions for the government relevant to national security) want to behave ethically.

As noted at the outset of this chapter, technology plays a critical role in the U.S. approach to national security, and technologically derived advantages can help both to defeat adversaries and to reduce friendly

¹⁴ Paul Berg, David Baltimore, Herbert W. Boyer, Stanley N. Cohen, Ronald W. Davis, David S. Hogness, Daniel Nathans, Richard Roblin, James D. Watson, Sherman Weissman, and Norton D. Zinder, "Potential Biohazards of Recombinant DNA Molecules," *Science* 185(4148):303, 1974, available at https://www.mcdb.ucla.edu/Research/Goldberg/HC70A_W11/pdf/BergLetter.pdf.

¹⁵ National Institutes of Health, "About Recombinant DNA Advisory Committee (RAC)," available at http://oba.od.nih.gov/rdna_rac/rac_about.html.

¹⁶ Paul Berg et al., "Summary Statement of the Asilomar Conference on Recombinant DNA Molecules," *Proceedings of the National Academy of Sciences* 72(6):1981-1984, 1975, available at <http://authors.library.caltech.edu/11971/1/BERpnas75.pdf>.

and noncombatant casualties. At the same time, individuals may disagree about what national security requires, and how best to promote and achieve it. Some of those disagreements are ethical in origin. That is, a nation that behaves ethically has to find an appropriate balance between national security and the protection of “national rights” versus the protection of individual rights and other ethical norms.

Still, the notion of deliberately causing death and destruction, even in defense against external threats, gives many people pause. How much death or destruction? Whose death and destruction? What kinds of destruction and death (e.g., quick and painless death versus slow and painful death)? Under what circumstances? At their core, such questions are ethical questions, and those who engage in combat, those who support combatants, directly or indirectly, and the citizenry whom they defend have a considerable stake in the answers to these questions.

Ethical concerns about military technology are not new. Deuteronomy 20:19 says that one should not cut down fruit trees in preparing for the siege of a city. Daniel Headrick notes that in 1139 Pope Innocent II banned as a religious matter the use of crossbows because they were so devastating, even by an untrained fighter, against the powerful, noble, and revered knight in plate armor.¹⁷ (This ban applied only to use against Christians.¹⁸) In the wake of World War I, the London Naval Treaty of 1930 outlawed unrestricted submarine warfare, a practice that allowed submarines to sink civilian ships without warning or providing for the safety of their crews.¹⁹

As a more recent example of ELSI concerns regarding science and technology for military and national security use, it is instructive to consider revelations of Senate committee hearings in the 1970s. These hearings revealed that the CIA had been conducting experiments involving the administration of hallucinogenic drugs to nonconsenting subjects who were U.S. citizens. According to the 1977 Senate Report of the Select Committee on Intelligence and Committee on Human Resources,²⁰

¹⁷ Daniel R. Headrick, *Technology: A World History*, Oxford University Press, New York, 2009. Cited in Patrick Lin, “Robots, Ethics, & War,” Stanford Law School, 2010, available at <http://cyberlaw.stanford.edu/blog/2010/12/robots-ethics-war>.

¹⁸ Bernard Brodie and Fawn M. Brodie, *From Crossbow to H-Bomb: The Evolution of the Weapons and Tactics of Warfare*, Indiana University Press, Bloomington, Ind., 1973.

¹⁹ See http://www.microworks.net/pacific/road_to_war/london_treaty.htm. In the case of both crossbows and submarines, these bans were subsequently ignored as the military value of using these weapons in the forbidden ways became more important.

²⁰ U.S. Senate Select Committee on Intelligence and Committee on Human Resources, “Project MKUltra, The CIA’s Program of Research in Behavioral Modification,” Joint Hearing before the Committee on Intelligence and Committee on Human Resources, 95th Congress, 1st session, August 3, 1977, available at <http://www.intelligence.senate.gov/pdfs/95mkultra.pdf>.

[CIA] research and development programs to find materials which could be used to alter human behavior were initiated in the late 1940s and early 1950s. These experimental programs originally included testing of drugs involving witting human subjects, and culminated in tests using unwitting, nonvolunteer human subjects. These tests were designed to determine the potential effects of chemical or biological agents when used operationally against individuals unaware that they had received a drug. . . .

The research and development program, and particularly the covert testing programs, resulted in massive abridgments of the rights of American citizens, sometimes with tragic consequences. The deaths of two Americans can be attributed to these programs; other participants in the testing programs may still suffer from the residual effects. While some controlled testing of these substances might be defended, the nature of the tests, their scale, and the fact that they were continued for years after the danger of surreptitious administration of LSD to unwitting individuals was known, demonstrate a fundamental disregard for the value of human life.

The report noted that the original rationale for this and other similar programs was based on U.S. concern over the use of chemical and biological agents by the Soviet Union and the People's Republic of China in interrogations, brainwashing, and in attacks designed to harass, disable, or kill Allied personnel. Such concerns created pressure for "a 'defensive' program to investigate chemical and biological agents so that the intelligence community could understand the mechanisms by which these substances worked and how their effects could be defeated."

But the 1977 report went on to note that "the defensive orientation soon became secondary. Chemical and biological agents were to be studied in order 'to perfect techniques . . . for the abstraction of information from individuals whether willing or not' and in order to 'develop means for the control of the activities and mental capacities of individuals whether willing or not.'"

According to the 1977 report, the program of clandestine testing of drugs on U.S. citizens is believed to have been suspended in 1963. Then-CIA Director Richard Helms argued that

because of the suspension of covert testing, the Agency's "positive operational capability to use drugs is diminishing, owing to a lack of realistic testing. With increasing knowledge of the state of the art, we are less capable of staying up with Soviet advances in this field. This in turn results in a waning capability on our part to restrain others in the intelligence community (such as the Department of Defense) from pursuing operations in this area." Helms attributed the cessation of the unwitting testing to the high risk of embarrassment to the Agency as well as the

“moral problem.” He noted that no better covert situation had been devised than that which had been used, and that “we have no answer to the moral issue.”

The national security context for S&T has a number of characteristics that differentiate it from a civilian environment for S&T. These differences raise the question regarding the extent to which insights regarding ethical, legal, and societal issues associated with S&T accumulated in the context of *civilian* S&T apply in a military context. For example:

- *The nature of destructive military technologies.* Whereas civilian technologies are usually designed not to do harm, certain military technologies are designed with the explicit purpose of reducing the capabilities and willingness of adversaries to fight further, and are often intended to cause harm to people and property. In the context of nonpacifist responses to threats, the goal becomes to design technologies that do the least harm to innocent parties and that do not inflict unnecessary harm on the adversary.

- *Civilian casualties.* The use of many military technologies can result in civilian deaths (e.g., “collateral damage” from military operations), and at times civilian casualties may outnumber military casualties.²¹ During armed conflict, the laws of war acknowledge that some degree of collateral damage is inevitable and that it is unrealistic to expect zero collateral damage from military operations. Controversy regarding civilian casualties often arises over whether an “armed conflict” (in the legal sense of the term) is indeed underway and the magnitude of collateral damage that is regarded as legally acceptable in any given military operation in an armed conflict.

- *Technologies and products developed by the private sector for civilian use.* These technologies and products may prove relevant to a military need and in the latter context raise heightened and/or new ethical, legal, and societal issues for policy makers to address. Because these technologies and products are developed by the private sector, there are few opportunities for addressing or even characterizing ethical or societal issues before they are adopted for military use. One example is the adversary use of cell phones as remote detonators of improvised explosive devices. A second example is the military/intelligence use of data mining techniques, developed first in the context of analyzing large data sets for commercial purposes.

²¹ Taylor B. Seybolt, Jay D. Aronson, and Baruch Fischhoff, eds., *Counting Civilian Casualties: An Introduction to Recording and Estimating Nonmilitary Deaths in Conflict*, Oxford University Press, Oxford, 2013.

- *Civilian adaptation of military technologies.* Military technologies may be adapted for use in civilian contexts (e.g., surveillance, drones) and in those contexts raise issues such as privacy and civil liberties. Such dual use is part of the calculus for examining ethical, legal, and societal issues that arise from military R&D.²²

- *Time urgency.* The timelines available for developing military technologies for specific applications may be compressed for a variety of reasons. For example, urgent military needs may emerge under the pressure of operations (e.g., new adversary weapons or tactics), and R&D is sometimes needed quickly to develop an appropriate response.²³ (The same considerations apply, with somewhat less force, to new intelligence that may indicate that an adversary is close to deploying a new weapon or employing new tactics that might undermine U.S. military capabilities.)

Also, when time is limited (as is often the case during times of crisis or actual conflict), policy makers are likely to consider long-term ethical or societal considerations to a lesser degree if they believe that such considerations may delay a useful response.

- *Rapid changes in militarily relevant technologies.* Given rapid technological change in some of the tools of warfare, the nature of conflict can also be expected to change rapidly. But because international law (especially the laws of war) are built on social consensus, definitions and understandings of what is and is not justified during conflict may change on much longer time scales. In the current “war on terrorism,” legal matters are further complicated by a lack of consensus as to whether counterterrorism is subject to the international law of armed conflict (LOAC), international humanitarian law, or domestic law enforcement principles—or some combination thereof. For example, the United States has asserted

²² This report adopts a “traditional” definition of dual-use technology that has both civilian and military application that is consistent with the usage of the U.S. government (<http://www.gpo.gov/fdsys/pkg/CFR-2010-title15-vol2/xml/CFR-2010-title15-vol2-sec730-3.xml>) and the European Commission (<http://ec.europa.eu/trade/creating-opportunities/trade-topics/dual-use/>). Other reports and analysts define dual-use technology as technology intended for beneficial purposes that can also be misused for harmful purposes. For this latter usage, see National Research Council, *Biotechnology Research in an Age of Terrorism*, The National Academies Press, Washington, D.C., 2004, and Seumas Miller and Michael J. Selgelid, “Ethical and Philosophical Consideration of the Dual-Use Dilemma in the Biological Sciences,” *Science and Engineering Ethics* 13(4):523-580, 2007.

²³ For example, military commanders during the first Gulf war realized that they needed the capability to destroy deeply buried Iraqi bunkers, and existing ordnance was inadequate for this task. Texas Instruments and Lockheed mounted an effort that resulted in the first combat use of the GBU-28 laser-guided bomb 17 days after the initiation of the development effort. See “Guided Bomb Unit-28 (GBU-28),” available at <http://www.globalsecurity.org/military/systems/munitions/gbu-28.htm>.

that its use of armed drones complies with LOAC.²⁴ A competing position is put forward by those who assert that a blend of international humanitarian/human rights law and the principles of domestic law enforcement should govern the use of drones when they are employed outside a “hot” battlefield to kill Al-Qaeda leaders and also those who argue that even if LOAC is the correct framing, U.S. policy is not compliant. Advocates of this competing position argue that the present strategy causes unnecessary suffering,²⁵ violates national sovereignty, and amounts to extrajudicial killing.²⁶ In general, these advocates would tend to prefer a “capture and detain” strategy, which they would regard as more humane. Other concerns point to the frequency of civilian deaths and the asymmetric military advantage that use of this technology creates.²⁷

1.4 EMERGING AND READILY AVAILABLE TECHNOLOGIES OF MILITARY SIGNIFICANCE

Emerging and readily available (ERA) technologies are the primary focus of this report. Such technologies are important for three essential reasons. First, the pathways on which these technologies will evolve (and the applications that may be enabled) are much less predictable than would be the case if access to these technologies were more limited. Second, these technologies are more readily available to a much wider array

²⁴ See, for example, John Brennan, Assistant to the President for Homeland Security and Counterterrorism, “The Efficacy and Ethics of U.S. Counterterrorism Strategy,” Wilson Center, April 30, 2012, available at <http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy>.

²⁵ For example:

If the State is not operating within the self-defense or armed conflict paradigms, it must be operating in the human rights paradigm. Simply put, if a State does not meet the legal criteria of self-defense or armed conflict, but uses force without Security Council authorization, it is doing so unlawfully. Thus, it becomes imperative for a State utilizing military force to justify and legitimize its actions as either a lawful right to self-defense or engagement in an armed conflict.

See Molly McNab and Megan Matthews, “Clarifying the Law Relating to Unmanned Drones and the Use of Force: The Relationships Between Human Rights, Self-Defense, Armed Conflict, and International Humanitarian Law,” *Denver Journal of International Law and Policy* 39(4, Fall):665, 2011; and Mary Ellen O’Connell, “Remarks: The Resort to Drones Under International Law,” *Denver Journal of International Law and Policy* 39(4, Fall):585, 2011.

²⁶ See, for example, Philip Alston’s statement that “[m]y concern is that these drones, these Predators, are being operated in a framework which may well violate international humanitarian law and international human rights law. “U.S. Warned on Deadly Drone Attacks,” BBC.com, October 28, 2009, available at <http://news.bbc.co.uk/2/hi/americas/8329412.stm>.

²⁷ “Secrecy of U.S. Drone Strikes in Pakistan Criticized,” MSNBC.com, January 29, 2010, available at http://www.msnbc.msn.com/id/35149384/ns/world_news-south_and_central_asia/t/secrecy-us-strikes-pakistan-criticized/#.UJVVzsXR5go.

of nations and possibly subnational groups than many of the traditionally important, militarily relevant technologies. Third, international legal regimes that may affect how nations use such technologies must reflect the reality that by definition, ERA technologies are readily available to nonstate entities—and to the extent that nonstate entities can use these technologies to cause significant effects, they perturb at least some of the traditional understandings underlying international law.

ERA sciences and technologies share most or all of the following basic characteristics:

- *Low barriers to entry.* At least by comparison to previous industrial-age technologies, advances in and exploitation of ERA technologies often do not require large investments or infrastructure. In other cases (in particular, in information technology), the incremental costs for developing any specific application are low because of significant investment in the commercial sector. That is, there are few or no technical chokepoints through which all necessary information or resources must pass, and thus access to these technologies is difficult or impossible to limit. The resources required for significant R&D efforts in these areas are relatively modest. Relevant specialized knowledge, once limited to articles published in paper-based journals, is now often accessible through the Internet, with little regard for national borders or distance. And whereas in the past building useful artifacts required great technical skill, kits are now often available that reduce the knowledge and skills needed to do so. A consequence is that advantages gained by the United States through a monopoly on military and other national security applications based on these technologies are likely to be transient. A second consequence is that nation-states themselves have less control over sensitive data regarding these technologies, data that might ultimately have military application. The bottom line is that both non-industrialized states and certain nonstate actors now have significantly greater access to ERA technologies, and these technologies can be used in ways that are contrary to U.S. national security interests.

- *Rapid change.* Again by comparison to most industrial-age technologies, advances in these technologies (especially information technology (IT), and those technologies that depend on IT) occur often, and significant advances on time scales measured in months are not uncommon. These time scales for advancement are short compared to the time scales on which nontechnical concerns such as law, policy, and ethics have traditionally been addressed, which means that advances associated with these technologies are likely to stress existing processes for policy formulation and/or arouse public concern. In short, fast, frequent, and significant

advances in a technology limit the time available for societal response and evaluation.

- *Blurring of lines between basic research and applied research.* As noted above, the OMB definitions draw categorical lines between basic and applied research, in which basic research develops fundamental knowledge without any specific application in mind and subsequent applied research expands and applies knowledge to develop useful materials, devices, and systems or methods and is sometimes oriented ultimately toward the design, development, and improvement of prototypes. In some cases (notably software), what emerges from applied research may already be very close to an artifact with operational utility.

The model embodying a sharp distinction between basic and applied research captures some elements of scientific progress in some fields, but it is particularly inapplicable to ERA technologies. For example, in practice but especially so when ERA technologies are involved, “applied” research may uncover problems that require additional “basic” research to solve; such feedback loops are common rather than rare. In addition, that model overlooks an important mode of progress increasingly common in today’s R&D environment—what is often called “use-inspired” basic research. One canonical example of such work was done by Louis Pasteur; driven by concerns related to public health, that work laid many of the foundations of microbiology.²⁸ In this context, the potential to solve a societal problem drives basic research in specific domains. The knowledge it produces can be regarded as fundamental and is likely to be as broadly applicable to multiple problem domains as “pure” basic research.

- *High uncertainty about how the future trajectories of ERA technologies will evolve and what applications will be possible.* Rapid evolution of a field implies that the periods of time between fundamental research and potential applications are shorter. In addition, the underlying scientific paradigms exhibit considerable instability—new discoveries often cause researchers to question previously accepted basic understandings. Because of the interconnectedness of various technologies, no single discipline is “in charge,” and the influences on research direction and application are even more diverse than when only one discipline is involved. In turn, uncertainty about the future trajectories of a given technology is a significant contributor to the technological risk that may be faced by any particular applications-development effort involving that technology. Thus, empirical evidence can go only so far in mitigating such risk.

²⁸ Donald E. Stokes, *Pasteur’s Quadrant: Basic Science and Technological Innovation*, Brookings Institution Press, Washington, D.C., 1997.

This report distinguishes between two categories of ERA science and technology: the category of foundational sciences and technologies and the category of specific application domains.

Foundational sciences and technologies enable progress and applications in a variety of application domains. They support, facilitate, drive, and may even be essential to other technologies, leading to a high degree of interconnectedness between many technologies. For example, many ERA technologies (e.g., neuroscience, cyber weaponry, synthetic biology, human enhancement technologies, robotics) depend on information technology to process and manipulate large amounts of data in short periods of time. Neuroscience is likely to be an enabler for robotics and prosthetics. The consequence of such interconnectedness is that advances in one area may in some cases help to stimulate advances or even eliminate severe bottlenecks in another. Furthermore, these fields share the characteristic that they are malleable—that is, they can be used in many different ways to address many different types of problems.²⁹

Chapter 2 discusses three foundational sciences and technologies for illustrative purposes:

- *Information technology.* Nearly any aspect of military operations today is dependent on the effective processing of information, and visions for IT applications (if not the practicality of such applications) are limited primarily by the imagination of potential users of information. IT is the foundational and enabling technology underlying two application domains discussed in this report, autonomous military systems and cyber weapons. IT is also fundamental to various intelligence applications, such as predictive analysis.³⁰

- *Synthetic biology.* Although there are today few civilian or military products with their origins in synthetic biology, the field holds great promise for new drugs, materials, and fuels. But the technology also may lead to the construction of new organisms with dangerous properties that might be harmful to the public and/or the environment.

- *Neuroscience.* Advances in neuroscience may be able to help wounded soldiers recover from traumatic brain injuries, but they may also be able to help uninjured soldiers process information more quickly, operate equipment through a direct brain-machine interface, and remember

²⁹ Notions of technological malleability and technology interconnectedness are further explored in James H. Moor, “Why We Need Better Ethics for Emerging Technologies,” *Ethics and Information Technology* 7:111-119, 2005.

³⁰ Predictive analysis seeks to make predictions about significant events in the future based on correlations found in patterns of data. An introduction to predictive analytics can be found in Eric Siegel, *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die*, John Wiley & Sons, Inc., Hoboken, N.J., 2013.

more information. Nor is neuroscience limited to these enhancements of normal function—various proposals have emerged suggesting that false human memories can be created and different emotional states induced (e.g., reduced or increased fear, feelings of anger or calm). It may also be possible to turn neuroscience-based applications on adversaries, and a number of such applications are conceptualized in particular as possibly effective nonlethal weapons.³¹

By contrast, an application domain is associated with a set of specific operational military problems, the solutions to which may draw on many different technologies. Four application domains are discussed in Chapter 3, again for illustrative purposes:

- *Robotics and autonomous systems.* In many conflict scenarios, unmanned weapons systems with varying degrees of autonomy are preferred for reasons of operational effectiveness and efficiency and minimizing casualties among noncombatants and friendly forces.
- *Prosthetics and human enhancement.* Human beings engage in combat with capabilities that are limited by biology and degraded through injury. The use of prostheses is one approach to restoring human capabilities lost through injury and enhancing human capabilities above and beyond biological limits.
- *Cyber weapons.* Given the increasing dependence of adversaries on computer and communications technology, cyber weapons provide a potentially important means by which adversary systems can be destroyed, degraded, disrupted, denied, and usurped.
- *Nonlethal weapons.* In many scenarios involving U.S. military forces engaged in military operations other than war (e.g., policing secured territory), it is desirable to have operational options other than the use of deadly force. Nonlethal weapons are often conceptualized as providing one such option.

The societal environment in which science and technology are embedded today has characteristics different from those in the past: increasing globalization and higher degrees of connectivity are two of its most prominent characteristics. Unlike the state of affairs immediately after World War II, the United States is no longer always and automatically the dominant and leading actor in all fields of S&T. Other nations have invested

³¹ The Chemical Weapons Convention constrains the use of chemical nonlethal weapons in a military context. However, certain kinds of directed-energy weapons might be developed for the purpose of affecting neurological function in some (nonlethal) way. See <http://royalsociety.org/policy/projects/brain-waves/conflict-security/>.

heavily in S&T, and foreign as well as domestic expertise drives important advancements in many fields. For example, in 2009, eight Asian countries had collectively caught up with U.S. investment in R&D.³² Nonetheless, the United States remains by far the largest national investor in R&D.

The impact of globalization is magnified by the phenomenon of increasing connectivity throughout the world. An ever denser and faster global Internet connects more and more scientists and technologists of many nationalities, allowing them to learn from each other. Of equal and perhaps greater significance is the fact that rapid communications of all kinds between individuals and groups are increasingly possible, enabling small groups to reach large audiences with information that may affect public opinion and social movements, including information that governments might prefer to keep out of public view. Social media in particular provide unprecedented opportunities for groups to organize and grow, a fact that can create enormous public pressures on government policy makers.

Economic considerations—faced by all governments and nations today—also increase pressures on governments and nations to justify support for scientific research in terms of its potential payoff and on researchers to justify their efforts in terms of positive economic and social effects. In this environment, policy makers feel strong pressures to shorten the time from government-supported research to useful applications—and such pressures reduce the time available for thoughtful consideration of how these applications might fit into a larger societal context.

Furthermore, much of the progress in certain ERA technologies—information technology stands out as a notable example—is the result of private-sector activity. Thus, government controls and influences on technological trajectories are weaker than they have been in the past.³³ And, of course, R&D conducted by the private sector must usually be justified on the basis of return-on-investment projections, which also inevitably emphasize nearer-term payoffs. Companies seek to gain a competitive advantage in the marketplace as a result of their R&D investment.

The parties that can take advantage of ERA technologies include parties that are neither wealthy nor technologically advanced. This definition spans a wide range, including relatively poorer or less technologically

³² The United States, the largest single R&D-performing country, accounted for about 31 percent of the 2009 global total. Asian countries—including China, India, Japan, Malaysia, Singapore, South Korea, Taiwan, and Thailand—represented 24 percent of the global R&D total in 1999 but accounted for 32 percent in 2009. See <http://www.nsf.gov/statistics/seind12/c4/c4h.htm>.

³³ Defense Science Board, “The Defense Science Board 1999 Summer Study Task Force on 21st Century Defense Technology Strategies, Volume 1,” U.S. Department of Defense, 1999, available at <http://www.dtic.mil/docs/citations/ADA433941>.

advanced nation-states, private organizations such as nongovernmental welfare organizations but also crime cartels and well-funded terrorist organizations, small groups of independent “freelance” actors, and even individuals. Of course, within this wide range, there is significant variation in their ability to take advantage of these technologies—with greater ability being associated with greater access to resources and talent.

1.5 ETHICS OF ARMED CONFLICT

The conduct of war has always raised ethical and societal concerns—and to the extent that technology is an instrument of war, the use of military technologies raises such concerns as well. For example, international law (the law of armed conflict as expressed in the UN Charter and the Hague and Geneva Conventions as well as a number of other treaties) today governs the conduct of armed conflict. The UN Charter describes the circumstances under which nations are permitted to engage in armed conflict. The Hague and Geneva Conventions and associated protocols govern how states may use force once conflict has started. A number of other international agreements ban the use of certain weapons, such as chemical and biological weapons,³⁴ land mines,³⁵ and blinding lasers.³⁶ These international conventions—and arms control agreements more generally—are motivated in part by ELSI considerations. Chapter 4 provides some history and discusses LOAC and other international law in greater detail.

As the nature of conflict, technology, and the larger world environment have evolved over the last several decades, a number of these changes pose a variety of new ethical challenges to existing international legal regimes and to our understanding of conflict. These changes include:

- *Nonstate adversaries.* State-on-state conflict, at least between industrialized nations, has given way to what some have called “violent peace.” Although nation-states are the primary focus of international treaties and agreements (and the Geneva Conventions bind *nations*), actual and potential adversaries of the United States include not only near-peer nation-states but also developing nations and terrorist groups that are not affiliated with any particular nation. Additional Protocol II of the Geneva Conventions (1977) fleshes out LOAC as it applies to non-international armed conflict (that is, armed conflict not involving two states). In addi-

³⁴ Geneva Protocol, 1925; Chemical Weapons Convention; Biological Weapons Convention.

³⁵ The Ottawa Treaty, 1999. The United States is not a party to this treaty, although as a matter of policy, it has mostly complied with its main provisions.

³⁶ Blinding Laser Protocol of the Convention on Conventional Weapons, 1995.

tion, the United Nations acknowledges the significance of nonstate actors in United Nations Security Council Resolution 1540,³⁷ which specifically obliges states “to refrain from supporting by any means non-State actors from developing, acquiring, manufacturing, possessing, transporting, transferring or using nuclear, chemical or biological weapons and their delivery systems.”

- *Asymmetric warfare.* U.S. advantages in conventional military power have led many adversaries to seek other ways to challenge the United States on the battlefield. Rather than seeking to overcome U.S. strengths, asymmetric tactics seek to take advantage of U.S. weaknesses, vulnerabilities, and dependencies—and one element of such tactics may be to ignore, disregard, or even take advantage of constraints imposed by traditional understandings of the laws of war. A historical example is that terrorists and insurgents may deliberately blend with noncombatant civilians on an expanded and nontraditional battlefield, and distinctions between the two categories are increasingly blurred in many situations of conflict. More recently, concerns have arisen that U.S. military forces may be excessively vulnerable to cyber threats because of their great dependence on information technology.

- *Volunteer service in the armed forces.* In the last 50 years, U.S. policy regarding military service has changed dramatically, from near-universal conscription of male citizens to all-volunteer armed forces. Today, an increasingly small fraction of the population has served directly in the armed forces. Most U.S. civilians lack firsthand knowledge of issues (some of them ethical) that may be associated with armed conflict, and fewer civilians know others who have served in the armed forces. Thus, many do not have a basis for making informed ELSI judgments about technologies that may be useful in modern warfare. In addition, current members of the armed forces have voluntarily relinquished certain rights to personal autonomy in choosing to be subject to a military chain of command, although the scope and nature of the rights they have surrendered are not necessarily clear in all cases. The fact of volunteering means that these individuals cannot say that they did not choose to be subject to military rules, which may require them to do things that they could not be required to do in civilian life.

1.6 WHAT IS AND IS NOT WITHIN THE SCOPE OF THIS REPORT

In 2010, the Defense Advanced Research and Projects Agency asked the National Academies to develop and articulate a framework for policy

³⁷ The resolution can be found at [http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540%20\(2004\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540%20(2004)).

makers, institutions, and individual researchers to use to think through ethical, legal, and societal issues as they relate to democratized technologies with military relevance. In DARPA's usage, "democratized technologies" are technologies with rapid rates of progress and low barriers to entry, as illustrated in Chapters 2 and 3. However, the committee believed that the term "democratized technologies" is easily misunderstood, and this report thus uses the term "emerging and readily available technologies" (ERA technologies).

The ethical, legal, and societal scope of this report encompasses three categories of concern that in the committee's judgment are central to any consideration of the ethics associated with new military technologies:

- *The conduct of research.* Conduct includes the selection of research areas, the design of particular research investigations (e.g., protocols, experiments), and the execution of those investigations. ELSI concerns relating to the conduct of research focus primarily on the impact of doing the research on the subjects that may be involved, whether by choice or by chance. "Subjects" here are defined broadly—communities, animals, individuals concerned about the environment, and workers in addition to those parties that are explicitly acknowledged as being research subjects.³⁸ (ELSI concerns related to acknowledged research subjects are important, but there is today a well-developed infrastructure to address such concerns.) In a military context, ethical, legal, and societal issues related to the conduct of research also include matters of classification and the impact that such classification may have on oversight and review.

- *The applications of research as they relate to intended capabilities enabled by research.* ELSI concerns associated with specified applications fall into two categories: concerns over the intended effects or purposes of the application and concerns over undesired effects ("side effects") that might occur when the application has its intended effects. An example of the first category is R&D intended to develop a laser to blind soldiers on the battlefield—one ELSI concern relates to whether it is in fact ethical to develop a weapon for such a purpose. (Some of the history regarding an international ban on the use of lasers designed to blind soldiers is recounted in Chapter 3.) An example of the second category is R&D on a vaccine against a biological weapon. In this case, there is little ELSI controversy over the intended result, namely, some degree of immunity to that weapon. However, if the side effects of the vaccine (which might include severe allergic reactions, pain, or muscle weakness) were signifi-

³⁸ The term "subject" in this context is used informally, and in particular is not tied to any legal definition of the term, as might be provided (for example) by regulations of the Department of Health and Human Services.

cant and widespread, ELSI concerns could arise over whether the benefits were worth the costs (e.g., how to account for benefits to the individual soldier versus benefits to the fighting force as a whole). Widely adopted applications may also require, impede, facilitate, or encourage institutional or organizational changes, and there may be ethical dimensions to such changes as well.

ELSI concerns related to technologies that can be used for both military and civilian purposes are an important subset of the second category. A decision to pursue one technology for an application in one context (a military context) may well raise ELSI concerns about its use in another context (e.g., a civilian context) because of different societal norms and laws/regulations that might be operative in the latter. One contemporary example is the law enforcement use of surveillance drones developed for military purposes, a use that has raised public concerns about privacy.³⁹

- *Unanticipated, unforeseen, or inadvertent ELSI consequences* of either research or applications. These consequences are usually manifested by something going awry, as when research does not proceed as expected (e.g., experimental control is lost) and thus causes harm outside the original bounds on the research or when unanticipated applications raise additional ELSI concerns.⁴⁰ ELSI concerns in this domain often relate to applications that are not intended by the proponents of such research. For example, an application may be used in ways entirely unanticipated or unimagined by its creators, and thus bring into play a set of side effects that were also unanticipated. These concerns are thus particularly difficult to imagine ahead of time. After due diligence has been exercised, it is also necessary to put into place a process that monitors how applications are used and that can respond quickly when unanticipated ELSI side effects manifest themselves. Chapter 4 discusses approaches for reducing the likelihood of unpleasant surprises.

For these categories of concern, the committee sought to build on previous work that addresses ethical, legal, and societal issues associated with S&T and with the military. In many cases, however, the committee found little work at the nexus of ethics, emerging technologies, and military applications. Nevertheless, some relevant work includes the following:

³⁹ See http://www.cbsnews.com/8301-201_162-57521768/more-than-a-third-fear-drone-use-in-u.s.-poll/.

⁴⁰ “Unforeseen” in this context means unforeseen by the proponents or the performers of the research.

- Work sponsored by the International Society of Military Ethics (ISME), which was established to examine professional military ethics in all dimensions, including but not limited to military technology.⁴¹ Of particular note is a special issue of the *Journal of Military Ethics* (Volume 9, Issue 4, 2010), published by the ISME, entitled *Ethics and Emerging Military Technologies*, with articles such as:

- “Postmodern War,” by George R. Lucas, Jr.;
- “The Ethics of Killer Applications: Why Is It So Hard to Talk About Morality When It Comes to New Military Technology?,” by P.W. Singer;
- “Ethical Blowback from Emerging Technologies,” by Patrick Lin;
- “The Case for Ethical Autonomy in Unmanned Systems,” by Ronald C. Arkin;
- “Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles,” by Bradley Jay Strawser;
- “Saying ‘No!’ to Lethal Autonomous Targeting,” by Noel Sharkey;
- “The Ethics of Cyberwarfare,” by Randall R. Dipert; and
- “‘Cyberation’ and Just War Doctrine: A Response to Randall Dipert,” by Colonel James Cook.

- A February 2012 publication by the Royal Society entitled *Neuroscience, Conflict and Security*.⁴² This study examined the ethics of neuroscience for military purposes and was charged with reviewing the current policy, legal, and ethical frameworks governing military applications of neuroscience.

- A RUSI publication, circa 2008,⁴³ which addressed the ethics and legal implications of military unmanned vehicles.

- A framework outlined by the Consortium for Emerging Technologies, Military Operations and National Security (CETMONS) for assessing the implications of emerging technologies for military capability and national security.⁴⁴ This framework considers issues related to a technology’s implications for civil society; civil reaction affecting military

⁴¹ See <http://isme.tamu.edu>. A European perspective on military ethics can be found at <http://www.euroisme.org>.

⁴² See <http://royalsociety.org/policy/projects/brain-waves/conflict-security/>.

⁴³ Elizabeth Quintana, *The Ethics and Legal Implications of Military Unmanned Vehicles*, British Computer Society, Royal United Services Institute, available at http://www.rusi.org/downloads/assets/RUSI_ethics.pdf.

⁴⁴ Consortium for Emerging Technologies, Military Operations, and National Security, “Framework for Assessing the Implications of Emerging Technologies for Military Capability and National Security,” 2013, available at <http://lincolncenter-dev.asu.edu/CETMONS/index.php/research-areas/framework-assessment>.

missions or civil society; external threats to U.S. security; the impact on treaties and military law; and the impact on military doctrine, military culture, military education, and military operations.

- A 2004 report of the National Research Council titled *Biotechnology Research in an Age of Terrorism* (aka the Fink report), which addressed “technologies [in the life sciences that] can be used legitimately for human betterment and [also] misused for bioterrorism [through the creation of biological weapons].”⁴⁵ In this context, the 2004 report noted that ““biological scientists have an affirmative moral duty to avoid contributing to the advancement of biowarfare or bioterrorism. . . . scientists can and should take reasonable steps to minimize this possibility [that knowledge they generate will assist in advancing biowarfare or bioterrorism].”

In addition, a 2008 report of the National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment*,⁴⁶ developed a framework for the systematic assessment of information-based programs being considered or already in use for counterterrorist purposes. This framework posed a set of questions focused on the effectiveness, lawfulness, and consistency with U.S. values of such programs, the answers to which would be useful to those making decisions about such programs.

The committee notes that perspectives on ethical, legal, and societal issues related to science, technology, and military affairs are hardly unitary. Even within a single nation such as the United States, different constituencies are likely to have different ethical stances toward the same issue. Furthermore, perspectives on ethics may vary with military might. A nation that is accustomed to military superiority on the battlefield may well have an ethical perspective different from that of other nations without such power (Box 1.1). The ethical perspectives of allies, adversaries, and neutral observers may well be different from that of the United States; under some circumstances, the differences may have consequences for U.S. freedom of action.

Addressing differences in ethical perspectives has two aspects, only one of which is covered in any detail in this report. Chapters 2 through 5 of this report address the first aspect, namely, the identification and articulation of possibly competing ethical perspectives. To properly consider ethical, legal, and societal issues, decision makers must begin by understanding the scope and nature of those issues. Part of that understanding

⁴⁵ National Research Council, *Biotechnology Research in an Age of Terrorism*, The National Academies Press, Washington, D.C., 2004.

⁴⁶ National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment*, The National Academies Press, Washington, D.C., 2008.

Box 1.1 Possible Ethical, Legal, and Societal Implications of Seeking Technological Superiority

As a matter of U.S. policy, superior military technology is

a cornerstone of the U.S. military's strategic posture. . . . DOD Research and Engineering (R&E) programs are needed to create, demonstrate, and partner in the transition to operational use of affordable technologies that can provide a decisive military superiority to defeat any adversary on any battlefield. . . . [Furthermore] continued technology development should enable future military superiority.¹

The U.S. declaratory policy of seeking technological military superiority over U.S. adversaries has an overarching impact on ethical, legal, and societal issues that involve the R&D associated with new technologies of military relevance. But a detailed examination of the ELSI implications of this policy is not within the scope of this project's statement of task, which implicitly asks the committee to assume the validity of this policy. Some aspects of this policy that may have ELSI implications include the following:

- Weapons to implement the policy of technological superiority have to conform to the laws of war, but since technology often outstrips the laws of war, the laws of war per se may not be much of a constraint. Thus, the development of such weapons stresses existing understandings of law and ethics that may be operative before the introduction of such weapons.
- Technological superiority may provide transient rather than long-lasting advantage as adversaries learn to counter or obtain the technologies available to the United States. However, even transient advantages can be tactically significant in the short term (in terms of enabling U.S. forces to perform missions at lower human and economic cost), especially if they come as a surprise to an unprepared adversary.
- Adversaries, both real and potential, react to the introduction of new U.S. military technologies. The availability of such technologies to the United States may deter adversaries from taking hostile actions against U.S. interests, may cause adversaries to seek to adopt those technologies for their own use, or may cause them to seek to counter the advantages conferred by U.S. use. Indeed, the first

is an explicit decision regarding whose ethical perspectives should be considered and taken into account.

The second aspect of addressing differing ethical perspectives is just as important. Once competing ethical perspectives have been identified, how should they be weighed and who should weigh them? Furthermore, on what basis should a party whose ethical perspectives are not adequately included in any policy decision, however inclusive and honest

successful uses of a technologically superior weapon may themselves be signals to adversaries about the utility of such weapons. Observed and anticipated adversarial responses to technological superiority and associated effects on stability may have ELSI implications.

- Because transient advantages dissipate (by definition), additional work is always needed to find new generations of technologically superior weapons—and enduring advantages can be secured only by making a commitment to constant reinvestment in technology.
- The first user of a weapon often sets precedents that other nations follow for the circumstances under which such a weapon can be used. Indeed, such precedents may be the initial seeds out of which international law and rules of the road governing such use can grow.
- A focus on technological superiority may cause the United States to neglect the “soft power” dimensions of its security strategy. In 2007, Secretary of Defense Robert Gates argued that in the future, “success [in asymmetric warfare] will be less a matter of imposing one’s will and more a function of shaping behavior—of friends, adversaries, and most importantly, the people in between.”²
- Presumptions of technological superiority may deflect attention from consideration of ethical, legal, and moral issues associated with military applications of technology. The prospect of reciprocal use has historically been a spur for reflection on the ethical implications of military applications of technologies, whereas asymmetric advantage has historically had the effect of deferring and diffusing ethical deliberation.

Because it treats the policy of seeking technological superiority over U.S. adversaries as a given, this report does not assess or even address the issues described above in any systematic way. Nevertheless, policy makers may wish to consider this policy as an area for future ELSI analysis that may have impacts on ELSI considerations of individual technologies or research projects.

¹ Thomas M. McCann, *Defense Manufacturing Management Guide for Program Managers*, October 16, 2012, p. 230, available at <https://acc.dau.mil/docs/plt/pqm/mfg-guidebook-10-16-12.pdf>.

² See <http://www.defense.gov/speeches/speech.aspx?speechid=1199>.

the decision-making process, be expected to trust and acquiesce in that decision?

In both national and international law, legal practitioners and scholars have developed approaches to balancing competing or conflicting interests, even when those conflicting interests are well grounded and legitimate. Examples of such approaches include procedural requirements such as burden-of-proof obligations; criteria to ensure that the impact on the interests that are adversely affected is minimized to the extent feasible

given the conflicting interests at stake; and appeal to case law to identify binding or guiding precedents.

As a broad generalization, approaches to balancing competing ethical claims and to comparing the ethics of different courses of action are considerably less developed. As a practical matter, it is often true that individuals presented with an ethical dilemma in a specific case come to similar conclusions about the appropriate course of action, even if they would disagree vehemently on the underlying reasoning or ethical theories. And in some cases, examination of similar cases from the past may help to shed some light on ethical matters. But to the extent that any party's ethical beliefs are deeply held, one might expect that party to be predisposed toward opposing any decision-making process that does not result in the accommodation of those beliefs.

In the end, if and when agreement cannot be found in contemplating any given dilemma, participants will usually engage in some ad hoc process that resolves it one way or another. It is not too strong to describe such a process as being political (and hence outside the scope of this report), and the political nature of this process serves as a reminder of the very complex milieu in which decision makers operate.

This report does not evaluate or assess the ethical, legal, and societal issues in any part of DARPA's technology R&D portfolio. That is, although the report does identify ethical issues that are associated with some of the technologies of interest to DARPA, it does not come to any specific conclusions about the ethical, legal, or societal propriety of any particular research program or project in the DARPA portfolio.

Also, this report does not address specific operational programs. While research programs are supported because they might enable important capabilities (and thus an ELSI assessment of a given research effort necessarily entails a consideration of applications), it is rarely clear at the outset how those capabilities might be integrated into an operational program. The reason is that the latter involves many specific decisions about how the program must operate—specific personnel, specific logistics, specific command-and-control configurations, specific rules of engagement, specific mechanisms for oversight, and so on. There are of course ethical, legal, and societal issues associated with these arrangements (e.g., a given arrangement may or may not raise ELSI concerns), but because these arrangements cannot be anticipated at the research stage, addressing the ethical, legal, and societal issues associated with operational programs is not within the scope of this report.

Furthermore, research-supporting agencies have general counsels that are charged with ensuring that all programs and projects by those agencies, both external and internal, are conducted in accordance with all applicable legal requirements. Processes intended to fulfill this mandate are not addressed in this report, except insofar as they are points of

departure as mechanisms for considering ethical, legal, and societal issues more broadly.

Other topics not addressed in this report under the broad rubric “the ethics of science” include scientific misconduct (e.g., data falsification, plagiarism, improper allocation of publication credit), specific laws and regulations as they might apply to specific research projects, financial conflicts of interest, the perspectives of specific religions on matters of war and peace, and the impact of classification on intellectual inquiry and academic freedom.

Last and as noted above in this chapter, this report assumes that some precursor efforts (whether basic research or applied research/development efforts) that may lead to advanced military technologies are appropriate for the nation to pursue and can be morally justified. Thus, any debate over the fundamental ethics of doing military research at all is outside its scope.

1.7 A ROADMAP TO THIS REPORT

So that it could base its analysis, findings, and recommendations on real-world trends, the committee examined seven illustrative S&T areas: information technology, synthetic biology, neuroscience, robotics, prosthetics, cyber weapons, and nonlethal weapons. Other relevant technology domains that the committee could have chosen to address include space technologies, geoengineering technologies, and nanotechnology.⁴⁷

Chapter 2 addresses the first three, which are foundational sciences and technologies that enable progress and applications in a variety of problem domains. Chapter 3 address the last four, which are application domains associated with specific operational military problems. To varying degrees, each of the S&T areas above has many or most of the characteristics of ERA technologies in the sense defined above. That is, even without large investment, a multitude of state and nonstate actors, friendly or not, can adopt and adapt their results to a multitude of purposes. Chapters 2 and 3 examine each of these S&T areas from the perspective of technology maturity (that is, how close the science or technology in question is to producing useful applications) and possible military applications. Without attempting to be comprehensive, it highlights some of the ELSI implications that emerge in each domain.

⁴⁷ Although the statement of task mentioned nanotechnology as an illustrative technology for this report, the committee did not examine nanotechnology explicitly. The reason was that the U.S. government does support the National Nanotechnology Initiative—and, as noted above, within that initiative is embedded a significant ELSI component. That dedicated effort is well resourced and positioned to make meaningful statements about ethical, legal, and societal issues associated with nanotechnology.

Chapter 4 describes sources of ELSI insight, including a variety of theoretical and disciplinary approaches to ethics and insights from social sciences such as anthropology and psychology.

Chapter 5 uses the sources of Chapter 4 and ELSI commonalities that appear in many of the technologies discussed in Chapters 2 and 3 to articulate questions for various stakeholders that might be used when contemplating the development of a technology or an application. These questions are useful for identifying possible ethical, legal, and societal issues that might arise from such development, and they are the heart of the framework requested in DARPA's charge to the committee.

Chapter 6 considers the limitations of a priori analysis and proposes two additional techniques for augmenting and increasing the value of what such analysis can provide. The chapter explores deliberative processes as a way to expand the scope of ELSI insights that might be relevant, and an adaptive approach to planning that can mitigate some of the ELSI uncertainties that can accompany any given development.

Chapter 7 describes various mechanisms that have been used to address ethical, legal, and societal issues arising from S&T endeavors, as well as considerations for the use of such mechanisms in a military context.

Chapter 8 provides the report's findings and recommendations.

2

Foundational Technologies

Foundational technologies (more properly, foundational science and technologies) are by definition those that can enable progress and applications in a variety of problem domains. Even in a military or national security context, it is rare that research on foundational technologies is entirely classified. Work on foundational technologies is mostly unclassified, or else classified work and unclassified work on such technologies happen contemporaneously. Lastly, useful applications based on a foundational technology often take a long time to emerge. Even then, one foundational technology may be used in combination with other technologies, both foundational and specialized, to create useful applications.

Each of the three main sections of this chapter addresses the scientific and technological maturity, describes some possible military applications, and discusses some illustrative ELSI questions that may be associated with each of the three technologies selected by the committee for examination (or applications that might be enabled through the technologies). The reader is cautioned that ELSI concerns related to these technologies—information technology, synthetic biology, and neuroscience—are not handled uniformly from section to section, reflecting the fact that different kinds of ethical, legal, and societal issues arise with different foundational technologies and the applications they enable. This chapter and Chapter 3 (on application domains) provide case studies for empirically grounding the framework of ELSI-related questions laid out in Chapter 5.

2.1 INFORMATION TECHNOLOGY

In general, information technology is designed to store, process, manipulate, and communicate information rendered in digital form. Information technology includes computing and communications technology. Both hardware and software fall under the rubric as well. The academic disciplines of computer science and computer engineering provide much of the intellectual underpinning of information technology.

2.1.1 Scientific and Technological Maturity

Information technology as a field is simultaneously mature, in the sense that the underlying technologies of information technology are sufficiently stable and well understood to support useful applications, and also newly emerging, in the sense that innovation and invention in information technology continue apace as they have for several decades.

The fundamental trends underlying advances in information technology hardware have for several decades been characterized by exponential growth in processor power and storage capacity, with doubling times measured in periods ranging from 9 months to 2 years. And there has been a corresponding flowering of applications resulting from the general public's easy access to computing power.

The same is true for communications technologies. These technologies support increasingly ubiquitous interconnectivity between computing devices, and it is not an exaggeration to suggest that most computing devices in the world are connected—although perhaps with a significant time lag—to most other computing devices. Such connectivity has led to exponential increases in the numbers of computers (and individuals) that communicate with each other.

With respect to the “packaging” of the fundamental hardware components of information technology, there are three hardware trends of note today.

- *Mobile computing and communications.* To an ever-increasing degree, users are demanding and vendors are supplying a wide variety of mobile computing and communications platforms, ranging from smart phones and tablet computing devices that are familiar to many consumers to ubiquitous sensor networks that are physically distributed over wide areas. Wireless data services needed to support mobile applications are proliferating as well. One form of mobile computing of particular note is wearable computing, as discussed in Box 2.1.

Box 2.1 Wearable Computing

In contrast to handheld computing devices such as smart phones and personal data assistants, wearable computing devices are generally integrated into a human's clothing or accessories (e.g., watches, glasses, belts). As such, they are less conspicuous as they are carried or used, and onlookers are more likely to miss them in casual observation. Moreover, the placement of these devices means that computing capability and large volumes of information are nearly instantaneously available.

Such devices have both military and civilian applications. Wearable computing and communications are already used to provide tactical information to soldiers in the field, and the canonical person in the street can often make use of instantaneous knowledge about geography (mapping), products on sale, and a wide variety of other consumer applications. Advances in such technology can also be used to provide bidirectional real-time translation between English and other languages.

But the inconspicuousness of wearable computing also raises many privacy issues. For example, one oft-raised privacy concern involves the possibility of instant facial recognition. A camera mounted on a user's glasses connected to a computer can allow the user to look at another person, capture an image of his or her face, and using facial recognition software, identify that person—along with any other information associated with that identity. Especially in an environment in which everyone does not have equal access to such capabilities, the potential for information asymmetry is large.

Another wearable computing application is the electronic capture of everything that a person can see or hear. Under most circumstances, video and audio events are fleeting—and people's memories of these events are known to be of questionable reliability under many circumstances. Those participating in such events often count on some degree of transience to make it safer for them to engage in such participation. The availability of potentially permanent records of previously transient phenomena thus has a potential for inhibiting a large range of behavior, most of which is not illegal. Again, the possibility of such an outcome most certainly carries ELSI implications.

- *Cloud computing.* For reasons of efficiency and economy, cloud computing is becoming increasingly popular among corporate users. Cloud computing provides computing power on demand, and because cloud computing is managed centrally, important IT support functions, such as security and maintenance, are simpler for many enterprises to obtain.

- *Embedded computing.* A modern automobile today has several dozen central processing units that control the braking, navigation, steering, entertainment, and power-train systems. (Indeed, safe computer-controlled driving has been demonstrated in a number of instances, and driv-

ing laws in some states are being updated to allow for this possibility.¹⁾ Computing power is also increasingly embedded in myriad devices and artifacts such as refrigerators and watches to make more effective use of the physical resources at hand and to provide desired services.

In the applications space, one of the most significant trends is the emergence of social computing and networking. Broadly speaking, social computing and networking support cooperative relationships for sharing information, and they take advantage of such shared information. In addition, information technology today is such that end users find it easier than ever before to assemble do-it-yourself applications for their own purposes.

Another important trend is the increasing use of a “big data” approach to solving a broad class of computational problems. Data storage capabilities have increased more rapidly than the processing power increases described by Moore’s law. And as technology is increasingly used in everyday life, more data can be and are collected. When such data are appropriately represented and structured, obtaining value from large data collections is often possible.

Processing these large data sets has required many additions to traditional computer processing algorithms and engineering paradigms (e.g., as in the paradigm used by programmers whereby they abstract, encapsulate, and re-use encapsulated objects). In particular, computer scientists now apply machine learning and knowledge discovery algorithms to large data sets and continually refine these algorithms based on evaluation of their results, and certain branches of computer science today have a substantial empirical basis.

Roughly speaking, machine learning involves methods that allow computers to make inferences from known relationships and patterns. For example, machine learning can be involved when a computer looks at many pictures of vehicles and identifies which pictures contain tanks. Here, the presumption is that tanks have distinguishing characteristics (e.g., vehicles with a gun sticking out of a turret that is mounted on a tracked chassis).

Knowledge discovery seeks to identify previously unknown relationships hidden in large volumes of heterogeneous data collected from myriad sources (text-based databases, video surveillance cameras, and so on). For example, knowledge discovery can be involved when a computer looks at a large volume of phone call records to identify networks of fre-

¹ See, for example, Maggie Clark, “States Take the Wheel on Driverless Car,” *USA Today*, June 29, 2013, available at <http://www.usatoday.com/story/news/nation/2013/07/29/states-driverless-cars/2595613/>.

quent communicators with geographical locations in Yemen or Somalia. Machine learning may, of course, be used in knowledge discovery—for example, systems can be “trained” on many examples and then asked to identify new patterns consistent with the examples in those training sets.

The result has been programs that are highly adaptive, even to the point of being able to learn. Direct consumer impact has occurred in everything from search engines, to classic artificial intelligence applications like speech recognition and translation, to modern e-commerce applications like interest-based advertising.

Finally, one of the most important truths about developments in information technology is that despite the origins of modern information technology in military R&D, advances in IT for the last few decades have been driven primarily by the private sector. This is not to deny the role of military R&D for certain very specialized technologies, but increasingly the military (and intelligence) communities seek ways of adapting commercially developed technologies for their own purposes, rather than building those base technologies from scratch. Such adaptations take advantage of an extensive IT R&D infrastructure developed in the civilian sector.

For example, scientists and engineers from the Massachusetts Institute of Technology Artificial Intelligence Laboratory founded a company in 1990 to commercialize their expertise in robotics—the fruits of their work include both bomb disposal robots and robotic vacuum cleaners. And this example is just one of the myriad developments originating in the private sector, including information retrieval and ubiquitous information, three-dimensional modeling, the “internet of things,”² and natural language and image understanding.

2.1.2 Possible Military Applications

U.S. military forces are highly dependent on information technology in a wide variety of contexts. To take the most basic example of such dependence, much of the IT used by DOD personnel for administrative and management purposes is essentially technology that can be obtained more or less unadorned from commercial vendors. But the DOD also has specialized needs for weaponry, command and control, training, and intelligence analysis.

- Modern military forces use systems and equipment that are controlled by computer for navigation, propulsion, communications, sur-

² The “internet of things” refers to a densely connected array of objects imbued with computing power that share information to work more effectively and efficiently together.

veillance, fire control, and so on. One of the most significant examples of applying information technology to military problems in the past several decades is the trend toward “smarter” guided munitions. IT is used to guide such a weapon after release directly to its target, thus vastly increasing the probability of a hit. IT is also used to effectuate smart fusing (e.g., optimal timing for when an explosive should detonate), thus increasing the probability that a hit will actually destroy the target. Another advantage is that the use of such weapons instead of “dumb” munitions potentially reduces the collateral damage of certain kinds of military operations by orders of magnitude.

- The movements and actions of military forces are increasingly coordinated through IT-based systems for command, control, communications, and intelligence (C³I) that allow information and common pictures of the battlefield to be shared and through analytical tools that help commanders make better decisions. C³I is an enabler for commanders to place (and thus use) their forces where and when they are needed, multiplying the operational effectiveness of those forces. Smaller forces are thus needed to create the same military effects.

- Training of U.S. military forces at many levels relies heavily on simulation, from training of individual soldiers to large-scale exercises that bring together many units. By definition, a simulation is a computer-generated representation of parts of a real environment. The use of simulation reduces costs of training and limits risks to individuals (e.g., from training accidents) but obviously does not substitute entirely for “live” training. In many cases, training simulations have their roots in gaming applications from the civilian sector.

- Intelligence analysis is based on finding connections in large disparate data sets. For example, machine learning and big data applications may be able to help predict major impending events, such as an assault or a jump in insurgent activity. Analysis of surveillance videos may identify an individual leaving a bomb in a public place or about to conduct a suicide attack. Authoritarian nations may use such technologies to identify dissidents. Adversaries might use predictive data mining to uncover putatively secret information, such as operational deployments of U.S. military units or identities of U.S. undercover operatives. High-quality facial recognition that can operate on degraded or obscured signals or can penetrate attempts at disguise has obvious value, especially in environments in which surveillance cameras are plentiful.³

As an illustration of some of the applications that new trends in com-

³ See https://www.fbibiospecs.org/facialrecogforum/_Uploads/Forum%203%20Media%20Articles_1.pdf.

puting might enhance, a presentation to the committee by Peter Lee from Microsoft Research suggested three important classes of application that have military or security implications and also present ethical, legal, and societal issues.

- *Prediction.* Large volumes of data can often be used to make predictions about future events (e.g., human behavior, outcomes of processes), the paradigm known as “big data” mentioned above. For example, based on the data routinely collected by electronic medical records systems in hospitals, it is possible to predict quite accurately the likelihood that a discharged patient will be readmitted. Prediction has also been demonstrated in software development (predicting the most likely locations of software defects and schedule delays); in Web browsing (predicting the Web pages that a user is likely to access); and in consumer buying behavior (predicting buying decisions in the near future).

- *Extraction of information from degraded sensor data.* In many sensing applications, data streams are highly redundant. Such redundancy can be used to compensate for missing or degraded data. For example, a group at the University of Illinois at Urbana-Champaign has applied the technique of compressive sensing to face recognition⁴ and has achieved a success rate for correct face recognition above 80 percent even operating on a severely degraded signal. (Compressive sensing is a signal-processing technique for reconstructing in certain contexts a relatively complete signal from relatively sparse measurements.)

- *Behavioral inference.* Computers increasingly can infer meaning from data that originate from people, whether such data takes the form of physical gestures, words, pictures, and so on. Even today, software can scan e-mail (for example) and make inferences about one’s schedule and travel plans. Microsoft’s Kinect uses various cameras to look at a human’s movements and gestures and specialized software that provides interpretation of those gestures. Kinect has also been used in a number of applications, including the use of gestures to direct the music of a computerized orchestra and enabling a small drone to avoid obstacles in its immediate surroundings.⁵ Other commercial applications have emerged: helping shoppers find the right size of clothing; assisting drivers in parallel parking; spotting suspicious human behavior in a casino. Intent-inferring technologies may be able to assist in situations relevant to national security as

⁴ John Wright, Allen Y. Yang, Arvind Ganesh, S. Shankar Sastry, and Yi Ma, “Robust Face Recognition via Sparse Representation,” *IEEE Transactions on Pattern Analysis and Machine Intelligence* 31(2):210-227, 2009.

⁵ Rob Walker, “Freaks, Geeks and Microsoft,” *New York Times*, May 31, 2012, available at <http://www.nytimes.com/2012/06/03/magazine/how-kinect-spawned-a-commercial-ecosystem.html>.

well—recognizing when a person is about to give a package to another person, when someone is pulling out a gun, or what events are being planned from a trail of e-mail.

Two of the most prominent application domains involving IT for military purposes—autonomous military systems and cyber weapons—are discussed in Chapter 3.

2.1.3 Ethical, Legal, and Societal Questions and Implications

Information technology alters many traditional concepts and activities by separating out and amplifying the information dimensions of such concepts and activities. IT is often used in situations and problem domains for which there is no accepted law, policy, or ethical stance. Moreover, these situations and problem domains themselves evolve and change at a very rapid rate. To understand what ethical behavior is when IT is involved, traditional principles of ethics are relevant but often not sufficient by themselves, and considerable interpretation and analogical thinking are needed to understand how those principles apply in any given situation.⁶

In a civilian context, some of the ethical, legal, and societal issues raised with IT concern privacy; intellectual property; accountability; trust; loss of control; and software dependability, including safety and reliability. In a military or national security context, each of these issues can sometimes play out differently than it might in a civilian context.

Privacy

In the United States, many individuals place a significant value on privacy, especially privacy against government intrusion.⁷ Privacy is often an issue in the context of certain national security applications of IT. When contemplating the use of some IT application against an adversary, it is not so much the privacy rights of adversaries at issue (they have few or none), but rather the possibility that a given application may compromise the privacy rights of innocent individuals (that is, ordinary citizens).

⁶ These ideas are explored in two papers written in 1985 and 1998 by James Moor (a member of the committee): James H. Moor, "What Is Computer Ethics?," pp. 266-75 in *Computers and Ethics*, Terrell Ward Bynum, ed., Blackwell Publishers, Ltd., 1985, published as the October 1985 issue of *Metaphilosophy*; and James H. Moor, "Reason, Relativity, and Responsibility in Computer Ethics," *Computers and Society* 28(1):14-21, March 1998.

⁷ National Research Council, *Engaging Privacy and Information Technology in a Digital Age*, James Waldo, Herbert S. Lin, and Lynette I. Millett (eds.), The National Academies Press, Washington, D.C., 2007.

Much of the tension regarding privacy and national security applications of IT focuses on managing the tradeoff between the intended security benefits of an IT application and the unintended “collateral damage” to the privacy of innocent citizens.

To the extent that privacy exists as an enforceable right, privacy rights of individuals have been enforced in the past both by law and by the practical difficulty of finding certain kinds of personal information. However, information technology reduces the practical difficulties of finding information, and much of what might have previously been hard to learn about an individual can in fact be learned by analyzing large amounts of data that reside in a number of different places. Protecting privacy through obscurity is increasingly difficult.

Considering the big data applications described above, one might note that with compressive sensing, the task of automating facial recognition in noisy environments (e.g., where cameras might not be able to obtain unobstructed images) will become easier. Compressive sensing would thus be an important component of a system capable of tracking the public movement of individuals on a large-scale basis. Intent detection potentially turns innocent movements into suspicious events, perhaps unjustly singling out individuals for examination and possible detention. Predictive analysis thus raises privacy concerns, because it requires the collection of data about an individual’s behaviors and history to make inferences about that person’s intent when he or she does something anomalous. Furthermore, privacy concerns—which themselves may evolve as people become more familiar with new technologies—may be accentuated if or when individuals improperly suffer negative consequences (e.g., arrest, loss of jobs) because putatively private information is revealed.

An extended discussion of privacy impacts of information technology can be found in the 2007 National Research Council report *Engaging Privacy and Information Technology in a Digital Age*.⁸

Intellectual Property

With modern information technology, the cost of replicating digital property (sometimes also known as digital objects) is essentially zero. Replications of digital property can be perfect, unlike replications of material property. These two aspects of digital property upend many traditional understandings of property, such as ownership, that have been

⁸ National Research Council, *Engaging Privacy and Information Technology in a Digital Age*, 2007.

developed primarily for property manifested as tangible objects consisting of arrangements of atoms.

Traditional concepts associated with intellectual property may have to be modified (and in many cases simply recognized as inapplicable) when “property” is manifested as arrangements of binary digits (bits). For example, information “objects” such as data files are much more easily transported than physical objects. Although much more convenient to store and search, information objects are also much easier to misappropriate—and in the civilian world, a wide range of economic and societal interests have a stake in striking the right balance between how to protect and how to provide access to information objects.

Issues of intellectual property protection have also become important for national security in three ways:

- The use of various IT applications to create, manage, and store digitally represented intellectual property of all kinds has proliferated tremendously in the past 50 years—and so have the opportunities for misappropriation of such property. In this context, intellectual property is construed broadly to include product information, software, business plans, proprietary R&D, and economic forecasts—and when competitors are able to misappropriate such information, individual U.S. firms can be placed at a significant disadvantage. In recent years, the scale of the problem has expanded in such a way that the inability to keep such intellectual property secure and confidential is no longer just an issue for individual companies but has also become a national security concern because of how it threatens U.S. economic leadership and primacy.
- The misappropriation of intellectual property specifically related to national security (e.g., weapons blueprints and specifications, military plans, and so on) creates direct risks to national security. Adversaries may learn of vulnerabilities in U.S. weapons or operational procedures, may be able to anticipate U.S. military moves, and so on—all such information in the wrong hands constrains the freedom of action that is otherwise enjoyed by U.S. military forces.
- Adversaries exploring the IT systems and networks controlling critical infrastructure facilities could acquire certain kinds of intellectual property (e.g., facility configurations, communications links between parts of a plant, and so on) that would help them to attack these facilities.

Accountability

Today’s computers can process inputs and then take different actions based on the specific inputs received. In common parlance and understanding, such computers are making decisions—choosing between alter-

native courses of action. Information technology underlies increasing automation of many functions previously delegated to people,⁹ but today and more so in the future, computers will make decisions that have traditionally been made by responsible humans in positions of authority. This phenomenon is not limited to civilian systems, and there are many pressures today toward increasing the role of computer-based decision making in operational military scenarios, especially those that involve highly compressed timelines.

Notions of accountability and responsibility, as applied to individuals, have focused on the ability of humans to make appropriate decisions under various circumstances. How and to what extent, if any, are such notions applicable to computers? This question is especially complicated in light of three facts: humans program computers (or program computers to program other computers); an IT system is sometimes so complex that no single individual can have a complete understanding of it; and users of such programs often have less understanding of the program than do the creators. In a military context, such facts call into question traditional notions of command and accountability, and thus the organizational structures built around these notions.

Trust

Many human relationships (e.g., commercial relationships) are built on trust. But trust relationships can be difficult to establish at a distance, and a great deal of information technology is used to enable connections at a distance. Information technologists have developed a wide variety of mechanisms for developing and enhancing trust, which in this context refers in part to assurances that an asserted identity does indeed correspond to an actual identity. Personal trust that depends on face-to-face interaction cannot be fully accommodated by technologies that connect individuals over long physical distances.

Even so, some of the limitations of long-distance interaction can be mitigated by technical improvements, such as increased bandwidth. Larger bandwidth is an enabler for video and audio connections with higher fidelity, making it easier for individuals on both ends of a connection to see and hear subtleties in the expressions of their counterparts. Reputations and social networks can also facilitate the establishment of trust. For example, John may assert that *X* is true. I may not know John,

⁹ For example, the World War II *Baltimore*-class cruiser (CA-68) displaced 13,600 tons and carried a crew ranging from 1650 to 1950 individuals. By contrast, the planned DDX *Zumwalt*-class destroyer (DDG-1000) is expected to displace approximately 14,500 tons and carry a crew of 140 individuals.

but if I know that he is friends with and trusted by Bob and Mary, whom I know well and trust, then I might infer with greater accuracy that John is trustworthy than I could in the absence of my own connections to Bob and Mary.

In an operational military context, consider that trust is an essential element that binds commanders and the troops that they command. In many instances, command relationships cannot be reduced simply to superiors passing orders to subordinates and subordinates passing information to superiors. Commanders need to know, for example, that a subordinate is apprehensive about an upcoming operation—and that information technology systems to support command and control that do not allow for direct unmediated communication between commander and subordinate may well be less effective operationally than systems that do.

Loss of Control

The possibility of excessive automation leading to a loss of human control in nuclear weapons systems has been particularly problematic. Much of nuclear strategy has focused on ensuring retaliation against an adversary, regardless of what that adversary might attempt to do. A “launch on warning” strategy—rejected by most strategists as being too risky—was based in part on the idea that a largely automated system of sensors could provide highly reliable warning about a nuclear attack in progress and thus enable nuclear missiles to be launched before they were destroyed on the ground.

Software Dependability

According to a 2007 NRC report, a system is dependable when users can rely on it to produce the consequences for which it was designed, and no adverse effects, in its intended environment.¹⁰ Although information technology hardware has been characterized for several decades by exponential growth in its sophistication, advances in software technology and the corresponding ability to build complex networked computer systems have been relatively scarcer. Today, it is a given that any complex computer system will not be entirely dependable under all possible circumstances of operation.

The 2007 NRC report *Software for Dependable Systems* argues that demonstrating software dependability is essentially a social process—that a developer must convince the user of such software that the software

¹⁰ National Research Council, *Software for Dependable Systems: Sufficient Evidence?*, The National Academies Press, Washington, D.C., 2007.

is dependable, using both technical and nontechnical evidence. A software system should be regarded as dependable only if the developer has made a credible case for its dependability, which includes a compilation and presentation of relevant evidence that the software behaves as it is expected to behave. Further, the level of dependability required for any given software system is not a technical matter alone, but is determined instead by a mix of factors, some of which are societal (and sometimes ethical) in nature. As one example, software developers may have to make tradeoffs between increased software functionality and the increased difficulty of making an adequate case for the software's dependability.

The DOD has special needs in software, such as the need for software dependability in the presence of highly sophisticated adversaries; manageability of the complex architectures needed to fulfill mission requirements; criticality with respect to safety, availability, and responsiveness; and overall complexity and scale.¹¹ Thus, software dependability is particularly significant in a military context.

As an illustration, consider the problems inherent in a 1998 computing problem aboard the USS *Yorktown*, an Aegis-class cruiser designated as an information technology testbed for the U.S. Navy, that disabled all onboard propulsion systems.¹² Such a glitch, occurring in the midst of battle, may well have had catastrophic consequences.

2.2 SYNTHETIC BIOLOGY

As is true of much research in genetic engineering and recombinant DNA, research in synthetic biology is in general concerned with the design and construction of biological systems not found in nature. Synthetic biology and these other approaches to construction of new systems offer the hope of new drugs, materials, and fuels. They may also lead to the creation of new organisms with dangerous properties that might be harmful to the public and/or the environment. In addition, adversaries have pursued biological weapons for use against the United States, despite international agreements prohibiting the development and use of biological weapons.¹³

¹¹ National Research Council, *Critical Code: Software Producibility for Defense*, The National Academies Press, Washington, D.C., 2010.

¹² Gregory Slabodkin, "Software Glitches Leave Navy Smart Ship Dead in the Water," GCN.com, July 13, 1998.

¹³ For example, the Director of Central Intelligence testified to the Senate Select Committee on Intelligence on February 6, 2002, that "documents recovered from al-Qa'ida facilities in Afghanistan show that Bin Laden was pursuing a sophisticated biological weapons research program." See https://www.cia.gov/news-information/speeches-testimony/2002/senate_select_hearing_03192002.html.

Synthetic biology, as a member of a family of genetic engineering technologies, thus implicates many of the ethical, legal, and societal issues that arise in the context of such technologies.

2.2.1 Scientific and Technological Maturity

A field with a coherent set of research objectives and methodologies, synthetic biology uses design principles from engineering, such as standardization, decoupling, and abstraction, to understand, take apart, rebuild, and construct new biological systems.¹⁴ Synthetic biologists are working to construct and catalog a set of biological components with known and predictable properties and performance qualities. When assembled on a “chassis” into a functional cellular or acellular “machine,” these standard biological parts then are expected to act and interact predictably, even when used in varying combinations, thus reducing the cost of designing new biological systems.

The cost of the technological infrastructure needed to conduct serious work in synthetic biology—technologies for DNA sequencing and synthesis—has followed an exponentially decreasing cost curve similar to Moore’s law (although with different time constants). Consequently, technological capabilities for such work are much more widespread than ever before.

A major goal of synthetic biology is the construction of “minimal cells” possessing only the genetic program necessary to sustain essential cellular functions.¹⁵ In a minimal cell, the functional redundancy and complexity arising from the long evolutionary history of natural organisms might be eliminated through reverse engineering. In fact, a synthetic minimal cell need not be built from the same “parts” as natural cells at all. For example, the genetic instructions encoded in a product could be entirely different from natural genetic codes. Downstream, the instructions could specify the assembly of a protein from custom amino acids that do not occur in natural systems. Such a product could then serve as a cellular chassis to which genetic applications could be added, for example to produce a hydrocarbon or an enzyme of choice.

In 2010, *Science* published a paper from the J. Craig Venter Institute describing the construction of the first self-replicating, synthetic bacterial

¹⁴ Steven A. Benner and Michael A. Sismour, “Synthetic Biology,” *Nature Reviews Genetics* 6(7):533-5431, 2005.

¹⁵ Anthony C. Forster and George M. Church, “Toward Synthesis of a Minimal Cell,” *Molecular Systems Biology* 2:45, 2006.

cell.¹⁶ The institute reported the synthesis, assembly, cloning, and successful transplantation of the 1.08 million base pair *Mycoplasma mycoides* JCVI-syn1.0 genome to create a new cell controlled by this synthetic genome and capable of replication. In the words of an accompanying press release, the synthetic cell provided “the proof of principle that genomes can be designed in the computer, chemically made in the laboratory and transplanted into a recipient cell to produce a new self-replicating cell controlled only by the synthetic genome.”¹⁷

By late 2011, another group of scientists, having experimented with larger and more complex yeast chromosomes that are harder to synthesize than the bacterial chromosome, announced that they were able to replace all of the DNA in the “arm” of a yeast chromosome with synthetically produced computer-designed DNA that is structurally distinct from its original DNA to produce a healthy yeast cell.¹⁸

Such advances, coupled with federal and private investments in research and development, are helping synthetic biology to develop into an ever more promising field. The many potential applications of synthetic biology include production of pharmaceuticals and biofuels, specialty chemicals and enzymes, and customized synthetic DNA sequences as well as minimal cell chassis. The real and/or perceived efficacy of the synthetic biology paradigm for these applications has led to the growth of a new bioengineering sector. The global market for this synthetic biology sector was \$1.6 billion in 2011 and is forecast to exceed \$10 billion within 5 years.¹⁹

Nevertheless, at the time of this writing, synthetic biology has yielded few commercially viable products, and it is fair to say that synthetic biology is not a mature technology. However, given that the barriers to entry for R&D in synthetic biology are so low, the field may mature quite rapidly and unexpectedly.

¹⁶ Daniel G. Gibson et al., “Creation of a Bacterial Cell Controlled by a Chemically Synthesized Genome,” *Science* 329(5987):52-56, 2010, available at <http://www.sciencemag.org/content/329/5987/52.full>.

¹⁷ See <http://www.jcvi.org/cms/press/press-releases/full-text/article/first-self-replicating-synthetic-bacterial-cell-constructed-by-j-craig-venter-institute-researcher/>.

¹⁸ Jessica S. Dymond, Sarah M. Richardson, Candice E. Coombes, Timothy Babatz, Heloise Muller, Narayana Annaluru, William J. Blake, Joy W. Schwerzmann, Junbiao Dai, Derek L. Lindstrom, Annabel C. Boeke, Daniel E. Gottschling, Srinivasan Chandrasegaran, Joel S. Bader, and Jef D. Boeke, “Synthetic Chromosome Arms Function in Yeast and Generate Phenotypic Diversity by Design,” *Nature* 477(7365):471-476, 2011.

¹⁹ John Bergin, “Synthetic Biology: Emerging Global Markets,” *BCC Research*, November 2011.

2.2.2 Possible Military Applications

In September 2011, DARPA issued a broad agency announcement (DARPA-BAA-11-60) for innovative research proposals to develop new tools, technologies, and methodologies to transform biology into an engineering practice. The Living Foundries program is intended to revolutionize manufacturing by enabling the rapid development of previously unattainable technologies and products. In 2012, DARPA awarded \$15.5 million to six different organizations to carry out research projects that eventually will create new on-demand manufacturing production, thus providing the military with access to “new materials, novel capabilities, fuel and medicines.”²⁰

Many of the civilian applications imagined for synthetic biology would be useful to the military as well. The Presidential Commission for the Study of Bioethical Issues identified several broad application domains for synthetic biology: renewable energy sources, health care, food and agriculture, and environmental remediation.²¹

- *Renewable energy sources.* Synthetic biology researchers hope to develop organisms that can produce alcohols, oils, and hydrogen gas, all of which can be used for fuel. The U.S. military is a prodigious user of fuel and would benefit from technologies that could help to secure its access to sources of such fuels.

- *Health care.* Synthetic biology researchers hope to develop the means for improved production of drugs and vaccines, advanced mechanisms for personalized medicine, and novel, programmable drugs and devices for prevention and healing. Again, the U.S. military provides a very large volume of health care services, both for active duty personnel and for their families, and improvements in health care technology will have a significant effect on the services thus provided. In addition, the U.S. military has specialized medical needs, because it must cope with a variety of injuries and ailments that are not common among civilians. As-yet-unimagined applications of synthetic biology may provide new treatments for such conditions.

- *Food and agriculture.* Synthetic biology researchers hope to develop crops that produce higher yields, are more disease-resistant, or have higher levels of food-grade protein. To the extent that troops in the field have specialized nutritional needs, synthetic biology may be able to speed the development of foods that are better able to meet these needs.

²⁰ See <https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=d70f94af2f98e65620d1f089f35f375b&cview=1>.

²¹ Presidential Commission for the Study of Bioethical Issues, *New Directions: The Ethics of Synthetic Biology and Emerging Technologies*, Washington, D.C., December 2010.

- *Environmental remediation.* Synthetic biology researchers have focused on developing organisms capable of performing certain clean-up functions, such as the digestion of oil slicks and the removal of heavy metals from soil. A military application of clean-up organisms might be the removal of nerve gas residues from contaminated surfaces or the use of enzymes that can neutralize nerve agents if the human body is exposed to them.

2.2.3 Ethical, Legal, and Societal Questions and Implications

Many of the ELSI concerns raised by synthetic biology are quite similar to those raised earlier in considerations of recombinant DNA technology—R&D on both technologies seek to create biological entities that are not found in nature. In both cases, these issues involve safety construed broadly (applications of synthetic biology or recombinant DNA getting out of control or harming the environment), undesirable side effects if such applications are used, and malicious use.²²

What sets synthetic biology apart from other technologies developed with similar intent is the approach it takes to creating these new biological entities. Modularization of biological components with predictable behavior is intended to make creation of such entities easier, less expensive, and more reliable. These properties are expected to enable a broad spectrum of work in synthetic biology—much broader than what might be possible in the absence of these properties.

Recognizing the inherent ethical and societal issues that might arise from its investment in synthetic biology, DARPA created in 2011 an advisory committee modeled after its Privacy Panel to advise the Living Foundries program staff. Members of the advisory committee receive compensation from DARPA and are leading authorities in diverse fields including ethics, biosecurity, intellectual property, and environment risk and regulation. The advisory committee reviews all proposals and highlights potential areas of concern, which may include how the research is conducted and disseminated as well as how the research might be used.²³ Additional discussion of the advisory committee is provided in Chapter 7.

The discussion below of ethical, legal, and societal issues draws heavily on two sources: a 2009 report from the Hastings Center and the Woodrow Wilson Center titled *Ethical Issues in Synthetic Biology: An*

²² See, for example, Jonathan Tucker and Raymond Zilinskas, “The Promise and Perils of Synthetic Biology,” *The New Atlantis* 12(Spring):25-45, 2006, available at <http://www.thenewatlantis.com/publications/the-promise-and-perils-of-synthetic-biology>.

²³ Conversation with Alicia Jackson, DARPA, Ken Oye, and Anne-Marie Mazza, June 25, 2012.

*Overview of the Debates*²⁴ and the 2010 report *New Directions: The Ethics of Synthetic Biology and Emerging Technologies*,²⁵ issued by the Presidential Commission for the Study of Bioethical Issues. (Shortly after the announcement by the Venter Institute of its successful construction of a synthetic bacterial cell, President Obama asked the Commission to review the emerging field of synthetic biology and to address the ethical issues associated with this new field so as to maximize public benefits and minimize risks.)

Environmental and Safety Risks

As with other genetic engineering technologies, synthetic biology raises concerns about how new biological entities will interact with and affect human beings and the natural environment:

- Engineered microbes introduced into the human body may trigger unanticipated adverse effects, such as infections or unexpected immune responses, or may displace the natural microbiome.
- New organisms that escape into the environment may pose novel risks resulting from their potential to reproduce or evolve. Such organisms may alter the ecology of areas they are inadvertently introduced to, affecting local food webs and perhaps displacing natural species, including animals and plants as well as microbes. In addition, because organisms produced by synthetic biology may have entirely novel genetic makeups, they may have altered rates of evolution and may adapt to new environments in unpredictable ways. Synthetic organisms may transfer one or more engineered genes to naturally occurring species, with unknown and perhaps irreversible consequences.²⁶
- In the case of engineered organisms for the production of renewable energy, concerns arise from the need to dedicate large amounts of land and other natural resources to the production of biomass as feedstock for biofuels. Such use could crowd out other uses of land, affecting food production, communities, and current ecosystems.

Furthermore, because the evolutionary or ecological history of a

²⁴ The full report can be found at <http://www.synbioproject.org/process/assets/files/6334/synbio3.pdf>.

²⁵ See <http://bioethics.gov/synthetic-biology-report>.

²⁶ Genya V. Dana, Todd Kuiken, David Rejeski and Allison Snow, "Four Steps to Avoid a Synthetic Biology Disaster," *Nature* 483:29, 2012; Markus Schmidt, Agomoni Ganguli-Mitra, Helge Torgersen, Alexander Kelle, Anna Deplazes, and Nikola Biller-Andorno, "A Priority Paper for the Societal and Ethical Aspects of Synthetic Biology," *Systems and Synthetic Biology* 3(1-4):3-7, 2009.

novel organism will likely be incompletely known or entirely nonexistent, risks of escape and contamination may be extremely difficult to assess in advance.

ELSI concerns in this category appear to relate to both civilian and military applications of synthetic biology equally.

Humanity and the Sanctity of Life

Different religious groups may have different answers to the question of whether there is an inherent sanctity of life or of living systems, and whether this sanctity is violated by the construction of novel life-forms. The Wilson Center report addresses this issue under the heading of “non-physical” harms, which are primarily “concerns about the appropriate attitude to adopt toward ourselves and the rest of the natural world.”²⁷ The report notes that these concerns involve “the possibility of harm to deeply held (if sometimes hard-to-articulate) views about what is right or good, including . . . the appropriate relationship of humans to themselves and the natural world.”

Further, the Wilson Center report argues, many people disagree about “whether a particular activity threatens these values, how we should reduce nonphysical harm, who should be responsible and what may be sacrificed along the way. . . . We do not always agree about what counts as a nonphysical harm, because we disagree about what is human well-being . . . [and this is because we embrace] different ethical frameworks.”

The Wilson Center report cites work by Boldt and Müller²⁸ as the most ambitious attempt to date to articulate these concerns in the synthetic biology literature. Boldt and Müller argue that

if we begin to create lower forms of life and to think of them as “artifacts” (as researchers in synthetic biology propose), then we “may in the (very) long run lead to a weakening of society’s respect for higher forms of life.” That is, if we continue down this road, we risk undermining our respect for animals and, ultimately, humans as they naturally occur. They [Boldt and Müller] also argue that when creatures like us adopt the attitude of creators, we are making a category mistake—a mistake about the sorts of beings we really are. Less self-conscious, nonacademic authors would have used an unfashionable phrase about “playing God” to describe this mistake.

As in the category of environmental and safety risks related to the

²⁷ See <http://www.synbioproject.org/process/assets/files/6334/synbio3.pdf>.

²⁸ Joachim Boldt and Oliver Müller, “Newtons of the Leaves of Grass,” *Nature Biotechnology* 26(4):387-389, 2008.

sanctity of living systems, ELSI concerns related to the sanctity of life appear to relate to both civilian and military applications of synthetic biology equally.

New Adversary Threats

All of the risks described above are framed as inadvertent and unintentional. But some biological research conducted in the 2000s—including the laboratory creation of infectious polio virus,²⁹ the creation of a cell with a synthesized mycoplasma genome,³⁰ the re-creation of the 1918 strain of influenza virus,³¹ and the creation of a highly transmissible avian flu³²—led to concerns that an adversary could have undertaken

²⁹ Jeronimo Cello, Aniko V. Paul, and Eckard Wimmer, “Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template,” *Science* 297(5583):1016-1018, 2002. One member of the research team argued that the experiment demonstrated the risk of further viruses being created from just their genetic code—by bioterrorists, for example. See <http://www.nature.com/news/2002/020712/full/news020708-17.html>.

³⁰ Daniel E. Gibson et al., “Creation of a Bacterial Cell Controlled by a Chemically Synthesized Genome,” *Science* 329(5987):52-56, 2010. Concerns were raised about bioterrorism and environmental disaster, as discussed in <http://www.jyi.org/issue/synthetic-biology-an-era-of-promised-uncertainty/>.

³¹ Terrence M. Tumpey et al., “Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus,” *Science* 310(5745):77-80, 2005. On October 17, 2005, in a *New York Times* op ed, Ray Kurzweil and Bill Joy, both information technologists, called the publication of this paper a “recipe for destruction” and characterized the genome of the virus as the design of a weapon of mass destruction whose realization would be easier than that of an atomic bomb. See <http://www.nytimes.com/2005/10/17/opinion/17kurzweiljoy.html>.

³² Masaki Imai et al., “Experimental Adaptation of an Influenza H5 HA Confers Respiratory Droplet Transmission to a Reassortant H5 HA/H1N1 Virus in Ferrets,” *Nature* 486:420-428, 2012; Sander Herfst et al., “Airborne Transmission of Influenza A/H5N1 Virus Between Ferrets,” *Science* 336(6088):1534-1541, 2012. In the lead-up to publication, the National Science Advisory Board for Biosecurity (NSABB) expressed security concerns to two journals, *Science* and *Nature*, about unrevised versions of these manuscripts, and requested that these papers be published only with the redaction of certain “experimental details and mutation data that would enable replication of the experiments.” These papers demonstrated the isolation of highly pathogenic avian H5N1 viruses that were capable of aerosol transmission between mammals. This research went through both scientific peer review and programmatic review at the NIH, as well as review by local institutional biosafety committees; none of these reviews were designed to consider ethics apart from issues of safety or misuse. It was not until the manuscripts were submitted for publication that any concerns arose, and even then these were largely about biosafety and biosecurity, the fear being that accidental or deliberate release of an agent with >50 percent mortality could cause a severe pandemic. Their authors subsequently submitted revised manuscripts (cited above), and the papers were published in full with the support of the NSABB. The NSABB cited two reasons for its reversal. First, it noted that “[t]he data described in the revised manuscripts do not appear to provide information that would immediately enable misuse of the research in ways that would endanger public health or national security,” and

these experiments with the deliberate intent of creating harmful organisms, even though these experiments were not in fact performed with any harmful intent. To varying degrees, these experiments used traditional recombinant DNA techniques, although arguably some used techniques from synthetic biology when they employed synthesized DNA.

As in the previous category, ELSI concerns in this category appear to relate to both civilian and military applications of synthetic biology equally. Nonetheless, the notion of adversary threats based on synthetic biology is relevant to national security.

Impact of Classification

A recommendation of the President's Commission was that the federal government should start to coordinate and oversee agency activities in synthetic biology.³³ It called for no new oversight function at that time but rather recommended that the government stay abreast of any major advances in the field, especially those that offer potential benefits and risks to the public.

But the commission was not charged specifically with addressing the oversight of classified research in synthetic biology, should any such research be contemplated. (The committee does not know of classified research in synthetic biology, but it undertook its information-gathering efforts in an entirely unclassified environment.) Some of the issues that arise when research is classified include the degree of coordination that is feasible when there may be different levels of secrecy associated with the research, and how to establish effective oversight in these environments. Staying abreast of developments and the associated benefits and risks can also be difficult because the research, by definition, is shielded from public view.

ELSI concerns related to classification appear to relate primarily to military applications of synthetic biology.

2.3 NEUROSCIENCE

The term "neuroscience" refers to the interdisciplinary study of the nervous system. The Society for Neuroscience describes neuroscience as

it cited new evidence "that understanding specific mutations may improve international surveillance and public health and safety." See http://oba.od.nih.gov/oba/biosecurity/PDF/NSABB_Statement_March_2012_Meeting.pdf. More recently, however, there has been a call to broaden the discussion about this type of gain-of-function experiments to include ethics. See Simon Wain-Hobson, "H5N1 Viral-Engineering Dangers Will Not Go Away," *Nature* 495(7442):411, 2013.

³³ See <http://bioethics.gov/synthetic-biology-report>.

the entire range of scientific research endeavors aimed at understanding the nervous system and translating this knowledge to the treatment and prevention of nervous system disorders. It fosters the broad interdisciplinarity of the field that uses multiple approaches (e.g., genetic, molecular, cellular, anatomical, neurophysiological, system, comparative, evolutionary, computational, and behavioral) to study the nervous system of organisms ranging from invertebrates to humans across various stages of development, maturation, and aging.³⁴

In its 2008 report *Emerging Cognitive Neuroscience*, the National Research Council describes neuroscience as “includ[ing] the study of the central nervous system and somatic, autonomic, and neuroendocrine processes,” and defines the term “cognitive” as covering “psychological and physiological processes underlying human information processing, emotion, motivation, social influence, and development. . . . It [neuroscience] includes contributions from behavioral and social science disciplines as well as contributing disciplines such as philosophy, mathematics, computer science, and linguistics.”³⁵

Modern neuroscience is thus an interdisciplinary field that combines new knowledge of molecules, cells, neural circuits, and cognition; is allied with clinical medicine; and uses methodologies of mathematics, molecular biology, genomics, neuroendocrinology, neuroimaging, and the social and behavioral sciences. Some important achievements and ongoing goals of neuroscience are the mathematical modeling of systems of electrical signals and of electrochemical transmission from one neuron to another via synapses, and of the ways that brain cells store memories.

Acknowledging the importance of this emerging field, both the United States and the European Union have launched large-scale science programs in neuroscience. In April 2013, the Obama Administration committed \$100 million in the FY 2014 budget to the BRAIN (Brain Research through Advancing Innovative Neurotechnologies) Initiative.³⁶ The White House fact sheet on this initiative notes that its ultimate aim is to “help researchers find new ways to treat, cure, and even prevent brain disorders, such as Alzheimer’s disease, epilepsy, and traumatic brain injury.” Further, the fact sheet says, the initiative will

accelerate the development and application of new technologies that will enable researchers to produce dynamic pictures of the brain that show how individual brain cells and complex neural circuits interact at the

³⁴ Society for Neuroscience, Strategic Plan, available at <http://www.sfn.org/index.aspx?pagename=strategicPlan>. Last updated September 30, 2010.

³⁵ National Research Council, *Emerging Cognitive Neuroscience and Related Technologies*, The National Academies Press, Washington, D.C., 2008.

³⁶ See <http://www.whitehouse.gov/the-press-office/2013/04/02/fact-sheet-brain-initiative>.

speed of thought. These technologies will open new doors to explore how the brain records, processes, uses, stores, and retrieves vast quantities of information, and shed light on the complex links between brain function and behavior.

In January 2013, the European Union announced that as part of its effort to advance future and emerging technologies, it was proposing to devote €1 billion over 10 years to the Human Brain Project,³⁷ which is intended to create the world's largest experimental facility for developing the most detailed model of the brain for "studying how the human brain works and ultimately to develop personalized treatment of neurological and related diseases."

2.3.1 Scientific and Technological Maturity

One measure of the field's maturation is the growth in the annual number of neuroscience publications, which has increased by a factor of 8 to 10 over the past 20 years.³⁸ In that period the membership of the Society for Neuroscience more than doubled, from 18,976 in 1991 to 42,576 in 2011, and annual meeting attendance increased from 16,447 in 1991 to 32,357 in 2011.³⁹

Advances in the neuroscience of memory (with ramifications for some of the applications discussed below) provide one illustration of scientific progress in the field. The neuroscience of memory addresses neurological processes for encoding information for storage and future retrieval. It is understood today that short-term memory capacity resides in the hippocampus, encoded by measurable strengthening or weakening of synapses, long-term potentiation, and long-term depression. Components of memories are transferred to cortical structures, where they are consolidated into their long-term, stable, protein-synthesis-dependent form during sleep and rest. Neuroscience research using functional magnetic resonance imaging (fMRI) has demonstrated functional connections between the hippocampus and the medial prefrontal cortex. Genetic knock-out studies

³⁷ See http://europa.eu/rapid/press-release_IP-13-54_en.htm.

³⁸ This factor is derived from data extracted by the committee from the Web of Knowledge/ Web of Science with the following query:

Topic=(neuroscience);Refined by: Research Areas=(NEUROSCIENCES
NEUROLOGY) AND Research Areas=(NEUROSCIENCES NEUROLOGY)
AND Document Types=(ARTICLE OR MEETING OR CASE REPORT OR
ABSTRACT OR REFERENCE MATERIAL OR REPORT)

³⁹ UN International Bioethics Committee, "Initial Reflections on the Principle of Nondiscrimination and Nonstigmatization," Unesco.org, August 23, 2012, available at unesdoc.unesco.org/images/0021/002174/217421e.pdf.

in mice have found that memory depends on a wide variety of receptors, enzymes, and proteins.⁴⁰

2.3.2 Possible Military Applications

Possible applications of neuroscience can be divided roughly into two classes—those that help humans to recover normal functionality and those that help humans change normal functionality.

In the first category (recovery of normal functionality), humans sometimes lose neurological functionality through accident or birth defects. For example, boxers and football players are known to suffer neurological damage in playing their sports, as do people who are victims of car accidents. In a military context, traumatic brain injuries (incurred, e.g., as a result of soldiers being exposed to explosions) have been described as the “signature injury” of the wars in Iraq and Afghanistan,⁴¹ and advances in neuroscience may be able to help wounded soldiers recover from such injuries.

In the second category (changing normal functionality), neuroscience could be used to enhance or to diminish normal functionality. For example, through neuroscience-based applications, individuals might be able to operate equipment through a direct brain-machine interface rather than manipulating a joystick or typing commands on a keyboard. Workers in high-stress occupations, such as air traffic control, might be able to process larger amounts of information more quickly. Individuals with needs for the selective enhancement or inhibition of learning and memory might meet those needs with the administration of designer drugs based on neuroscience research. Antisocial tendencies of certain criminals, such as sexual offenders, could be diminished. Psychological traumas might be reduced for victims of abuse, torture, or other horrific events.

Enhancements of the types described in the previous paragraph have obvious military applications for soldiers operating weapons or commanders coordinating battles. Much more controversial from an ELSI standpoint are other proposals suggesting that false human memories can be created and different emotional states induced (e.g., reduced or increased fear, feelings of anger or calm) and that degrading the performance of adversaries in military contexts may be possible—applications that are generally not associated with civilian use.

⁴⁰ For example, Ramirez et al. have demonstrated the insertion of false memories into mice. See Steve Ramirez et al., “Creating a False Memory in the Hippocampus,” *Science* 341(6144):387-391, 2013, available at <http://www.sciencemag.org/content/341/6144/387>.

⁴¹ See http://www.defense.gov/home/features/2012/0312_tbi/.

Cognitive Enhancement

Enhancement may be defined as performance that exceeds a physiological or statistical norm in healthy persons. For example, transcranial magnetic stimulation (TMS) may suppress the effects of sleep deprivation and enable individuals to perform above their baseline capability at specialized tasks, both of which would have obvious advantages for warfighters. Repetitive TMS (rTMS) might also serve to improve learning and working memory, for example, increasing the ability of an operative to speak a native dialect or to recall complicated instructions. Some believe that near-infrared spectroscopy could detect deficiencies in a warfighter's neurological processes and feed that information into a device utilizing in-helmet or in-vehicle TMS to suppress or enhance individual brain functions, such as mood and social cognition. A 2009 National Research Council report titled *Opportunities in Neuroscience for Future Army Applications* recommended that the Army increase its investment in TMS research.⁴² That committee estimated the development timeframe for using TMS to enhance attention at 5 to 10 years, and for in-vehicle deployment at 10 to 20 years.

A different form of cognitive enhancement comes in the form of mitigating the effects of sleep deprivation, which is the source of so much error in civilian as well as in military life. Historically, fatigue has been mitigated through such measures as cocaine, nicotine, and caffeine. More recently amphetamines ("speed") have acquired popularity and have, again, been used by both students and warfighters, especially air force pilots it seems, in the form of "go pills." Modern pharmaceutical technologies may be entering new and somewhat more efficacious territory with evidence that modafinil (originally approved for the treatment of narcolepsy) may reduce fatigue-related cognitive decline, or even outperform methylphenidate (Ritalin) in healthy persons. Short-term memory enhancement may also be achieved through nasally delivered orexin-A, as shown by a DARPA-sponsored study of sleep-deprived monkeys.⁴³

Neurological processes may be modified without the open-skull experiments incident to neurosurgery that have been so important in the history of neuroscience. For example, TMS uses electromagnetic induction to penetrate the skull and modulate the electrical activity of the cerebral cortex. Another method, transcranial direct current stimulation (tDCS), may be safer, but used less often, than TMS. To perform TMS, a techni-

⁴² National Research Council, *Opportunities in Neuroscience for Future Army Applications*, The National Academies Press, Washington D.C., 2009.

⁴³ S.A. Deadwyler et al., "Systemic and Nasal Delivery of Orexin-A (Hypocretin-1) Reduces the Effects of Sleep Deprivation on Cognitive Performance in Nonhuman Primates," *Journal of Neuroscience* 27(52):14239-14247, 2007.

cian holds an iron-core insulated coil on one side of a patient's head while a large, brief current is passed through the coil. The current generates a magnetic pulse that painlessly penetrates the layers of skin, muscle, and bone covering the brain and induces weak, localized electrical currents in the cerebral cortex. It is believed that the induced electrical field triggers the flow of ions across neuronal membranes and causes the cells to discharge, resulting in a chain reaction of neuronal interactions. TMS offers hope for individuals suffering from major depression, Parkinson's disease, and treatment-resistant migraine headaches, and it is under investigation for the treatment of post-traumatic stress disorder. TMS has also helped to map brain circuitry and connectivity.

Brain-Computer Interfaces

Neuroscience technologies are often "dual use," having both military/counterintelligence and medical/scientific applications. Examples of brain-computer interfaces are prosthetic limbs and communication devices. Thus they may benefit both patients and warfighters or other security personnel. These two examples are also convergent technologies: during the past two decades laboratory experiments have shown that simple movements of both rodents and nonhuman primates may be controlled and that primates can be trained to manipulate robotic arms through neural activity alone.⁴⁴ The same principle of remote control of a robotic prosthesis has been applied to human patients suffering from tetraplegia, by means of an implanted intracortical electrode array.

Technological refinements suggest that, for some purposes at least, brain-computer interfaces need not be invasive. In the past, electroencephalogram-sensitive caps, which help control artificial joints during rehabilitation, were expensive and also required the application of a gel. Recent designs for such caps dispense with the gel and are far less expensive. They are now being produced for commercial application to computer gaming, with the potential for control over environmental conditions like room lighting, door locks, and window shades. DARPA has been interested in using new and noninvasive ways to gather neurological information to help adapt a pilot's brain to inputs from a cockpit array, reducing "noise" and distraction for the operator depending on what information is required for specific circumstances. Similarly the Cognitive Threat Warning System seeks to convert unconscious human neurological responses into usable information, as in a pair of binoculars

⁴⁴ L.M. Dauffenbach, "Simulation of the Primate Motor Cortex and Free Arm Movements in Three-Dimensional Space: A Robot Arm System Controlled by an Artificial Neural Network," *Biomedical Sciences Instrumentation* 35:360-365, 1999.

that cue the viewer to certain portions of the visual field.⁴⁵ In time, a true feedback loop that also helps adjust the computer to the human user may also be practical.

Interventions intended as therapy may in some cases enhance normal function. Brain-computer interfaces that control advanced prostheses that render the user faster or stronger would be one example, although perhaps an exoskeleton would be a nearer-term example of the same phenomenon. Dual-use considerations apply to this technology, just as they would for drugs intended to enhance cognitive performance (such as methylphenidate—marketed as Ritalin—which is often believed to help academic performance).

Deception Detection and Interrogation

Traditional measures of deception have relied on neurological correlates of stress like blood pressure and heart and breathing rates, but these are at best physiological proxies of intentional deception. One system known as the “brain fingerprinter” uses an EEG measure to detect an event-related potential called the P300 wave, which is associated with the recognition of a stimulus, such as a photograph of a certain location of interest. Services based on functional magnetic resonance imaging are being offered by companies such as No Lie MRI and CEPHOS, which market their products to governmental and nongovernmental organizations.

A 2008 NRC report entitled *Emerging Cognitive Neuroscience and Related Technologies* stated that “traditional measures of deception detection technology have proven to be insufficiently accurate,” recommending that research be pursued “on multimodal methodological approaches for detecting and measuring neurophysiological indicators of psychological states and intentions. . . .”⁴⁶ The report cautioned, however, that neurological measurements do not directly reveal psychological states, and so there is a distinct risk of over-interpretation of results, leading to both false negatives and false positives.

Another possible approach to deception detection involves the brain hormone oxytocin, which has been shown to be associated with a wide variety of social impulses. In the laboratory, subjects exposed to oxytocin via the nasal route have behaved in a more trusting and generous manner. The National Research Council’s 2008 report on emerging neuroscience identified oxytocin as a “neuropeptide of interest.”⁴⁷ However, the notion

⁴⁵ See <http://www.wired.com/gadgets/miscellaneous/news/2007/05/binoculars>.

⁴⁶ National Research Council, *Emerging Cognitive Neuroscience and Related Technologies*, The National Academies Press, Washington, D.C., 2008.

⁴⁷ National Research Council, *Emerging Cognitive Neuroscience and Related Technologies*, 2008.

that oxytocin could be useful in interrogation requires extrapolating from laboratory experiments conducted under highly specified conditions with subjects whose background and motivation differed from those of likely interrogation targets.

Performance Degradation

In addition to the potential for advances in neuroscience to enhance the performance of one's own forces, these developments also offer possible opportunities to inhibit or reduce the performance of adversaries. At present, the primary focus for such efforts to support military missions and law enforcement goals—as well as applications in areas such as counterterrorism or counterinsurgency where the lines between the two domains are often blurred—is on so-called incapacitating chemical agents (ICAs). The ethical and societal issues associated with ICAs are discussed in Chapter 3; this section briefly introduces the relevant scientific and technological developments. A number of recent reviews have addressed S&T potentially relevant to ICAs.⁴⁸

As an example of these technical reviews, a 2012 Royal Society report, part of a larger Brain Waves project on the implications of developments in neuroscience for society and public policy,⁴⁹ identifies two particularly prominent areas of relevant research.⁵⁰ These are neuropharmacology, which studies the effects of drugs on the nervous system and the brain, and advances in drug delivery methods. A number of pharmaceutical agents, which are primarily chemicals, have at least the theoretical potential to provide the basis for ICAs. Current research on ICAs tends to focus on agents that offer a combination of rapid-action and short-duration effects and thus on those that “reduce alertness and, as the dose increases,

⁴⁸ International Committee of the Red Cross, “Incapacitating Chemical Agents: Implications for International Law,” Expert meeting, Montreux, Switzerland, March 24-26, 2010, available at <http://www.icrc.org/eng/resources/documents/publication/p4051.htm>; Stefan Mogl, ed., *Technical Workshop on Incapacitating Chemical Agents*, Spiez Laboratory, Federal Department of Defence, Civil Protection and Sports, DDPS, Federal Office for Civil Protection, Spiez, Switzerland, September 8-9, 2011, available at http://www.labor-spiez.ch/de/dok/hi/pdf/web_e_ICA_Konferenzbericht.pdf; Scientific Advisory Board, Organization for the Prohibition of Chemical Weapons, “Report of the Scientific Advisory Board on Developments in Science and Technology for the Third Special Session of the Conference of States Parties to Review the Operation of the Chemical Weapons Convention,” RC-3/DG.1, 2012, available at <http://www.opcw.org/documents-reports/conference-states-parties/third-review-conference/>; Royal Society, “Brain Waves Module 3: Neuroscience, Conflict, and Security,” Royal Society, London, 2012.

⁴⁹ Information about the Brain Waves project is available at <http://royalsociety.org/policy/projects/brain-waves/>.

⁵⁰ Royal Society, “Brain Waves Module 3: Neuroscience, Conflict, and Security,” 2012.

produce sedation, sleep, anaesthesia, and death." Some of the classes of pharmaceutical agents under consideration are opioids, benzodiazepines, alpha2 adrenoreceptor agonists, and neuroleptic anaesthetics.⁵¹

In addition to these chemical agents, bioregulators—biochemical compounds that occur naturally and control vital functions such as temperature, heart rate, and blood pressure—have also been the subject of military research. Advances in the synthesis of bioregulatory peptides appear to offer the promise of overcoming some of the problems that have so far limited therapeutic applications and could also potentially enable national security applications as well.

Advances in medical research are also yielding more effective means of delivering drugs into the central nervous system, including across the blood-brain barrier. With regard to ICAs, advances in aerosol delivery are of particular interest because inhalation seems the most plausible dissemination mode for military and law enforcement purposes. At the same time, nanotechnology is offering significant potential to provide more effective, targeted delivery to the brain. To date, however, with some exceptions for veterinary applications, the two streams of research have focused on delivering doses to individuals.⁵²

A number of recent technical reviews have concluded that, in spite of the advances in several fields, the current state of S&T does not provide the basis for safe delivery of ICAs for law enforcement purposes, given all the challenges of delivering nonlethal doses in a variety of settings to groups that would vary by characteristics such as age, health status, and individual sensitivity to the chosen agent(s).⁵³ In its report on S&T developments in advance of the third review conference of the Chemical Weapons Convention, the Scientific Advisory Board (SAB) of the Organization for the Prohibition of Chemical Weapons commented that "in

⁵¹ Morphine is the primary example of an opioid, but the search for novel agents with fewer side effects continues. Fentanyl, the agent reportedly used as part of the aerosol compound piped into the ventilation system to break the Moscow theater siege in October 2002, is an opioid. Benzodiazepines are used to treat anxiety and also as part of general anesthesia. Alpha2 adrenoreceptor agonists, which reduce alertness and wakefulness and can also increase the effects of local and general anesthesia, have been the subject of U.S. Army research as a potential ICA. Neuroleptic anesthetics are able to induce unconsciousness without significant effects on reflexes or muscle tone.

⁵² National Research Council, *Life Sciences and Related Fields: Trends Relevant to the Biological Weapons Convention*, The National Academies Press, Washington, D.C., 2011.

⁵³ International Committee of the Red Cross, "Incapacitating Chemical Agents: Implications for International Law," Expert meeting, Montreux, Switzerland, March 24-26, 2010, available at <http://www.icrc.org/eng/resources/documents/publication/p4051.htm>; Royal Society, "Brain Waves Module 3: Neuroscience, Conflict, and Security," Royal Society, London, 2012; Michael S. Franklin et al., "Disentangling Decoupling: Comment on Smallwood (2013)," *Psychological Bulletin* 139(3):536-541, 2013.

the view of the SAB, the technical discussion on the potential use of toxic chemicals for law enforcement purposes has been exhaustive.”⁵⁴ The associated ethical and societal issues related to military and law enforcement applications are taken up in Chapter 3.

2.3.3 Ethical, Legal, and Societal Questions and Implications

Informed and Voluntary Consent to Use

The widely accepted moral principle of autonomy prohibits nonvoluntary neurotechnological interventions without informed consent or its moral equivalent. Nonetheless, it is clear that some feel impelled to accept such interventions regardless of the low likelihood that their personal goals would be realized. For example, there is little evidence that drug therapies for conditions like ADHD improve academic performance, although the off-label use of medications like Ritalin by college students surely has much to do with the notion that their performance might be improved.

The very term “human enhancement” could beg the question of the actual net benefits of claimed “enhancements.” Their social implications need to be examined on a case-by-case basis. Exaggerated claims about cognitive enhancement, or even accurate statements about short-term benefits, could lead to an increase in addictions due to competitive pressures. Differences in socioeconomic status related to contingent advantages like opportunities for acquiring new skills could be exacerbated by unequal access to enhancing technologies.

In the military, both competitive and coercive pressures are uniquely pronounced. In general, persons in uniform are required to accept interventions that commanders believe will maintain their fitness for duty or enable them to return to duty. In some circumstances, warfighters might even be required to accept medical interventions otherwise regarded as “experimental,” or at least not validated for a particular purpose, if there is a sound basis for believing that they could be of benefit if forces are threatened. A real-world example is described in Box 2.2.

As useful military technologies proliferate, including those that in some sense enhance normal cognitive functions, veterans may face the prospect of adjusting to civilian life without those advantages. The tragic

⁵⁴ Scientific Advisory Board, Organization for the Prohibition of Chemical Weapons, “Report of the Scientific Advisory Board on Developments in Science and Technology for the Third Special Session of the Conference of States Parties to Review the Operation of the Chemical Weapons Convention,” RC-3/DG.1, 2012, p. 21, available at <http://www.opcw.org/documents-reports/conference-states-parties/third-review-conference/>.

experience of many returning veterans, especially those who have faced the stresses of combat, demonstrates that this adjustment is already difficult enough.

A separate but important issue concerns the proliferation of these technologies—in civilian life and in the likely access that unfriendly persons, groups, organizations, and nations will gain to them. Is the potential for gain in U.S. military capabilities sufficient to overcome these potential negative effects? Or is it likely that civilian access to these technologies will precede their presence in military contexts?

Privacy

Longstanding, ill-defined but persistent worries and rumors about “brain-washing” and “mind control” will surely be reinforced by advances in neuroimaging, which is an excellent example of a technology that has both military and civilian applications. But do they raise valid privacy concerns? Besides issues of harm resulting from false positives and negatives, the extent to which brain imaging raises issues of privacy depends of course on the ultimate accuracy of the technology in revealing psychological states—and how such accuracy is perceived by users of the technology. Exaggerated notions of technological capacity can also have adverse social consequences, such as the premature admission of imaging data into courts of law. Constitutional barriers may also be insurmountable if these data are found to violate guarantees against self-incrimination or unacceptable forms of search and seizure.

Privacy challenges are emerging in many fields, including genetics and information technology, and brain imaging may or may not create unique ethical or policy issues. Even relatively simple technologies currently claimed to improve on traditional “lie detector” results have limited accuracy, require a cooperative subject, and may not be more efficient (or more cost-effective) than a simple interview with a skilled interrogator.

ELSI concerns in this category appear to relate to both civilian and military applications of neuroscience. However, in a military or national security context, it is easy to imagine that such applications raise particular concerns when they are applied to innocent bystanders—as they would inevitably be in any kind of counterintelligence investigation.

Safety

The safety of neuroscience-based interventions, whether drugs or devices, is of course a threshold concern. For example, external neuro-modulatory systems like dTCS and TMS are generally considered to present a low risk, but safety studies have generally been performed on

Box 2.2 Military Use in Combat of Drugs Not Approved by the Food and Drug Administration

The 1991 Gulf war raised a number of ethical and policy questions regarding the use of investigational new drugs (INDs)—drugs that have not yet received Food and Drug Administration (FDA) approval for use in particular applications but that are currently being investigated for such use—to defend troops against the possibility that they might be attacked by chemical and biological warfare agents. As a matter of policy, the Department of Defense (DOD) has complied with all FDA requirements concerning the development and use of new drugs, including the requirement to obtain informed consent before administering INDs to research subjects.

At the time of the Gulf war, two INDs were promising candidates for drugs to defend against certain chemical weapon/biological weapon agents. To comply with FDA regulations, the DOD would have had to obtain informed consent for the use of these drugs from every service member deployed to the Persian Gulf. Allowing deployed troops to refuse drugs intended for their own protection could, however, have jeopardized the combat mission. Accordingly, the DOD requested that the FDA both establish authority to waive informed consent requirements and grant waivers for administration of those particular drugs. The FDA agreed that obtaining informed consent might not be feasible “in certain combat-related situations” and that withholding potentially life-saving INDs in such situations would be “contrary to the best interests of military personnel involved,” and subsequently granted the DOD the waivers it sought.¹

This decision led to controversy, much of it focused on the difference between research (in which case informed consent must be obtained for administering a drug to research subjects) and treatment (in which case no such requirement obtains in a military context). Those opposed to the waivers argued that the use of any IND was, by definition, “research” because the consequences, risks, and benefits of use were unknown, and thus informed consent was required under all circumstances. Those opposing pointed to a long line of ethical guidelines, such as

healthy, normal subjects rather than persons with neurological or major psychiatric illnesses. There is a potential for seizures, although less than with conventional electroconvulsive therapy (ECT). However, the longer-term risks of repeated use of external neuromodulation are not known. The larger the populations exposed, the greater the likelihood of untoward results.

ELSI concerns in this category appear to relate to both civilian and military applications of neuroscience equally.

the guidelines in the Belmont report,² that make no exception for waiving informed consent for research conducted under wartime conditions. They further argued that the mere intent to use an IND to provide medical benefit could not transform an experimental investigation into therapy—otherwise, researchers could simply change their stated intentions and redefine an experimental intervention as treatment, thereby evading informed consent requirements.

Proponents of the waivers argued that the DOD had an ethical responsibility to protect its service members to the greatest extent possible. During the Gulf war, the best protection the DOD could offer its personnel included use of the INDs in question. Proponents further argued that despite their status as “investigational,” the drugs were neither remarkably novel nor experimental in a scientific or medical sense because they had already been subjected to “extensive research”; one drug had also been approved for uses that were similar to those that the DOD proposed. Moreover, prior ethical guidelines had been written with human experimentation in mind, in which the outcome of the research was in doubt and could result in serious harm to the subject. But the guidelines had not anticipated the ethical issues surrounding the use of drugs that would provide the only available means of avoiding death or serious disability under combat situations. Finally, the proponents noted that, under the doctrine of military command authority, the DOD could justifiably have chosen to act on its own, without FDA approval, but sought waivers to avoid even the appearance of impropriety.

¹ Food and Drug Administration, “Informed Consent for Human Drugs and Biologics; Determination That Informed Consent Is Not Feasible; Interim Rule and Opportunity for Public Comment,” 21 CFR Part 50, *Federal Register* 55(246):52814-52817, December 21, 1990, available at <http://archive.hhs.gov/ohrp/documents/19901221.pdf>.

² The Belmont report can be found at <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>.

SOURCE: Adapted in large part from RAND, *Waiving Informed Consent: Military Use of Non-FDA-Approved Drugs in Combat*, 2000, available at http://www.rand.org/pubs/research_briefs/RB7534/index1.html.

Responsibility and Loss of Control

Some of the most challenging societal questions relate to the possibility that techniques or drugs derived from neuroscience may be used to alter trust and moral judgment. For example, as noted above, administration of oxytocin to humans has the effect of increasing trust toward individuals shown to be untrustworthy.⁵⁵ A TMS disruption of the right temporo-parietal junction of individuals was shown to increase the like-

⁵⁵ Thomas Baumgartner et al., “Oxytocin Shapes the Neural Circuitry of Trust and Trust Adaptation in Humans,” *Neuron* 58:639-650, 2008.

likelihood that those individuals would forgive an unsuccessful murder attempt, as compared with a control group,⁵⁶ raising the possibility that such disruptions affect moral judgments. In the absence of such manipulations of trust and moral judgment, individuals are often held accountable for behaving appropriately. What remains of the notion of individual responsibility when individuals are subject to such manipulations?

In a military context, one might imagine the use of such techniques to reduce the qualms and inhibitions of soldiers about morally suspect or questionable activities. How and under what circumstances might neurally manipulated soldiers be accountable for activities that violate the laws of war?

Impact of Classification

As with synthetic biology, issues arise regarding coordination of neuroscience research in a classified environment and how to establish effective oversight in these environments. Staying abreast of developments and the associated benefits and risks can also be difficult because the research, by definition, is shielded from public view. As one example—the draft agenda for a conference titled “Evolving Neuro-Cyber Technologies and Applications and the Threats Within” held at Fort McNair in Washington, D.C., on March 14, 2012, included a panel to discuss the question of the ethics of such technologies and applications, and the session was classified top secret.

⁵⁶ Liane Young et al., “Disruption of the Right Temporoparietal Junction with Transcranial Magnetic Stimulation Reduces the Role of Beliefs in Moral Judgments,” *Proceedings of the National Academy of Sciences* 107(15):6753-7657, 2010, available at <http://www.pnas.org/content/early/2010/03/11/0914826107.full.pdf+html>. (One of the investigators in this study, Marc Hauser, was found to have committed scientific misconduct in the falsification of data associated with a number of other experiments, leading to a number of retractions of published papers involving such data. However, there is no indication that the paper cited in this footnote has been similarly discredited. See <http://www.boston.com/whitecoatnotes/2012/09/05/harvard-professor-who-resigned-fabricated-manipulated-data-says/UvCmT8yCmydpDoEkIRhGP/story.html>.)

3

Application Domains

Application domains are, by definition, associated with operational military problems. Solutions to these problems call for the application of various technologies, both foundational and specialized. Research and development work (applied research) on operational military problems is often classified.

This chapter addresses four application domains: robotics and autonomous systems, prosthetics and human enhancement, cyber weapons, and nonlethal weapons. For each, the relevant section provides a brief overview of the technologies relevant to that domain, identifies a few characteristic military applications within the domain, and addresses some of the most salient ethical, legal, and societal issues for that application domain. As with Chapter 2, the reader is cautioned that ELSI concerns are not handled uniformly from section to section—this lack of uniformity reflects the fact that different kinds of ethical, legal, and societal issues arise with different kinds of military/national security applications.

3.1 ROBOTICS AND AUTONOMOUS SYSTEMS

An autonomous system can be defined loosely as a system that performs its intended function(s) without explicit human guidance. The technology of autonomous systems is sometimes called robotics. Many such systems are in use today, both for civilian and military purposes, and more are expected in the future. And, of course, there are degrees of

autonomy that correspond to different degrees and kinds of direct human involvement in guiding system behavior.

The overarching rationale for deploying such systems is that they might replace humans performing militarily important tasks that are dangerous, tedious, or boring or that require higher reliability or precision than is humanly possible. If such replacement is possible, two consequences that follow are that (1) humans can be better protected and suffer fewer deaths and casualties as these important military tasks are performed, and (2) important military tasks will be performed with higher efficiency and effectiveness than if humans are directly involved.

3.1.1 Robotics—The Technology of Autonomous Systems

Computer systems (without the sensors and actuators) have always had a certain kind of “autonomous” capability—the term “computer” once referred to a person who performed computations. Today, many computer systems perform computational tasks on large amounts of data and generate solutions to problems that would take humans many years to solve.

For purposes of this report, an autonomous system (without further qualification) refers to a standalone computer-based system that interacts directly with the physical world. Sensors and actuators are the enabling devices for such interaction, and they can be regarded as devices for input and output. Instead of a keyboard or a scanner for entering information into a computer for processing, a camera or radar provides the relevant input, and instead of a printer or a screen for providing output, the movement of a servomotor in the appropriate manner represents the result of the computer’s labors.

Autonomous systems are fundamentally dependent on two technologies—information technology and the technology of sensors and actuators. Both of these technologies have developed rapidly. On the hardware side, the costs of processor power and storage have dropped exponentially for a number of decades, with doubling times on the order of 1 to 2 years. Sensors and actuators have also become much less expensive and smaller. On the software side, the technologies of artificial intelligence, statistical learning techniques, and information fusion have advanced a long way as well, although at the cost of decreased transparency of operation in the software that controls the system.

Software that controls the operation of autonomous systems is subject to all of the usual problems regarding software safety and reliability—programming errors and bugs, design flaws, and so on. Flaws can include errors of programming (that is, errors introduced because a correct performance requirement was implemented incorrectly) or errors of design (that is, a performance requirement was formulated incorrectly or stated improperly).

To control an autonomous system, the software is programmed to anticipate various situations. An error of programming might be a mistake made in the programming that controls the response to a particular situation, even when that situation is correctly recognized. An error of design might become apparent when a system encounters a situation that was not anticipated, and as a result either does something entirely unexpected or improperly assesses the situation as one for which it does have a response, which happens to be inappropriate in that instance.

Neuroscience may be an enabling technology for certain kinds of autonomous systems. Some neuroscience analysts believe that neuroscience will change the approach to computer modeling of decision making by disclosing the cognitive processes produced by millions of years of evolution, processes that artificial intelligence has to date been unable to capture fully. Such processes may become the basis for applications such as automatic target recognition. Even today, it is possible for automated processes to differentiate images of tanks from those of trucks, and such processes do not rely on neuroscience. However, neuroscience may contribute to an automated ability to make even finer distinctions, such as the ability to distinguish between friendly and hostile vehicles or even individuals.

In general, the logic according to which any complex system operates—including many autonomous systems—is too complex to be understood by any one individual. This is true for three reasons. First, multiple individuals may be responsible for different parts of the system's programming, and they will not all be equally conversant with all parts of the programming. Second, the programming itself may be large and complex enough to make it very hard to understand all of how it works in detail. Third, the program may combine and process inputs (sometimes unique inputs that depend on the very specific circumstances extant at a given moment in time) in ways that no human or team of humans can reasonably anticipate. System testing is one mechanism that can provide some information about the behavior of the system under various conditions, but it is well understood that testing can only provide evidence of flaws and that it cannot prove that a system is without flaw.¹

It is worth noting that a flaw in the software controlling an autonomous system may be far more damaging than a flaw in software that does

¹ National Research Council, *Software for Dependable Systems: Sufficient Evidence?*, The National Academies Press, Washington, D.C., 2007, available at http://www.nap.edu/catalog.php?record_id=11923. See also National Research Council, *Summary of a Workshop on Software Certification and Dependability*, The National Academies Press, Washington, D.C., 2004, available at http://books.nap.edu/catalog.php?record_id=11133. Real-time programming (the class of programming needed for robotics applications) is especially complicated by unanticipated "interaction" effects that are hard to detect by testing and also do not usually arise in non-real-time programming.

not control physical objects—in the latter case, a display may be in error (or indicate an error), whereas in the former case, the physical part of a system (such as a robotically controlled gun) may kill friendly troops.

3.1.2 Possible Military Applications

Technologies for autonomous systems are the basis for a wide variety of real-world operational systems. Today, robots are available to clean pools and gutters, to vacuum and/or wash floors, and to mow lawns. Robotic dogs serve as personal companions to some children. Robots perform a variety of industrial assembly line tasks, such as precision welding. A number of commercial robots also have obvious military applications as well—robots for security patrolling at home have many of the capabilities that robots for surveillance might need to help guard a military facility, and self-driving automobiles are likely to have many similarities to self-driving military trucks. In a military context, robots also conduct long-range surveillance and reconnaissance operations, disarm bombs, and perform a variety of other functions. In addition, these robots may operate on land, in the air, or on and under the sea.

Perhaps the most controversial application of autonomous systems is equipping such systems with lethal capabilities that operate under human control. Even more controversially, some systems have lethal capabilities that can be directed without human intervention. Some of these systems today include:²

- A South Korean robot that provides either an autonomous lethal or nonlethal response in an automatic mode rendering it capable of making the decision on its own.
- iRobot, which provides Packbots capable of tasing enemy combatants; some are also equipped with the highly lethal MetalStorm grenade-launching system.
- The SWORDS platform in Iraq and Afghanistan, which can carry lethal weaponry (M240 or M249 machine guns, or a .50 caliber rifle). A new Modular Advanced Armed Robotic System (MAARS) version is in development.
- Stationary robotic gun-sensor platforms that Israel has considered deploying along the Gaza border in automated kill zones, with machine guns and armored folding shields.

²Ronald C. Arkin, unpublished briefing to the committee on January 12, 2012, Washington, D.C.; and Ronald C. Arkin, “Governing Lethal Behavior,” *Proceedings of the 3rd International Conference on Human Robot Interaction*, ACM Publishing, New York, 2008.

Are such systems new? In one sense, no. A simple pressure-activated mine fulfills the definition of a fully autonomous lethal system—it explodes without human intervention when it experiences a pressure exceeding some preprogrammed threshold. Other newer, fully autonomous systems are more sophisticated—the radar-cued Phalanx Close-In Weapons System for defense against antiship missiles and its land-based counterpart for countering rocket, artillery, and mortar fire are examples. In these latter systems, the fully autonomous mode is enabled when there is insufficient time for a human operator to take action in countering incoming fire.³

Other systems, such as the Mark 48 torpedo, are mobile and capable of moving freely (within a limited domain) and searching for and identifying targets. A torpedo is lethal, but today it requires human intervention to initiate weapons release. Much of the debate about the future of autonomous systems relates to the possibility that a system will deliberately initiate weapons release without a human explicitly making the decision to do so.

Seeking to anticipate future ethical, legal, and societal issues associated with autonomous weapons systems, the Department of Defense promulgated a policy on such weapons in November 2012. This policy is described in Box 3.1.

3.1.3 Ethical, Legal, and Societal Questions and Implications

In some scenarios, the use of armed autonomous systems not only might reduce the likelihood of friendly casualties but also might improve mission performance over possible or typical human performance. For example, autonomous systems can loiter without risk near a target for much longer than is humanly possible, enabling them to collect more information about the target. With more information, the remote weapons operator can do a better job of ascertaining the nature and extent of the likely collateral damage should s/he decide to attack as compared with a pilot flying an armed aircraft in the vicinity of the target; with such information, an attack can be executed in a way that does minimal collateral damage. A remote human operator—operating a ground vehicle on the battlefield from a safe location—will not be driven by fear for his or her own safety in deciding whether or not to attack any given target, and thus is more likely in this respect to behave in a manner consistent with the law of armed conflict than would a soldier in immediate harm's way.

³ Clive Blount, "War at a Distance?—Some Thoughts for Airpower Practitioners," *Air Power Review* 14(2):31-39, 2011, available at <http://www.airpowerstudies.co.uk/APR%20Vol%2014%20No%202.pdf>.

Box 3.1 Department of Defense Policy on Autonomy in Weapon Systems

Department of Defense Directive 3000.09, dated November 21, 2012, on the subject of “Autonomy in Weapon Systems” establishes DOD policy regarding autonomous and semi-autonomous weapon systems.

An autonomous weapon system is a weapon system that, once activated, can select and engage targets without further intervention by a human operator. A subset of autonomous weapon systems are human-supervised autonomous weapon systems that are designed to select and engage targets without further human input after activation but nevertheless allow human operators to override operation of the weapon system and to terminate engagements before unacceptable levels of damage occur.

A semiautonomous weapon system is a weapon system that, once activated, is intended to engage only individual targets or specific target groups that have been selected by a human operator. In semiautonomous weapon systems, autonomy can be provided for engagement-related functions including, but not limited to, acquiring, tracking, and identifying potential targets; cueing potential targets to human operators; prioritizing selected targets; timing of when to fire; or providing terminal guidance to home in on selected targets. Semiautonomous systems also include fire-and-forget or lock-on-after-launch homing munitions that rely on tactics, techniques, and procedures to maximize the probability that only the individual targets or specific target groups explicitly selected by a human operator will be attacked. This provision allows weapons such as the United States Air Force Low Cost Autonomous Attack System loitering missile system to operate within a designated area in which only enemy targets are expected to be found.

Not covered by the policy are autonomous or semiautonomous cyber weapons, unguided munitions, munitions manually guided by operators, or mines.

The policy states that those who authorize the use of, direct the use of, or operate autonomous and semiautonomous weapon systems must do so in accordance with the laws of war, applicable treaties, weapon system safety rules, and the applicable rules of engagement (ROE). In addition, it directs that autonomous and semiautonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force. Autonomous and semiautonomous weapon systems should do the following:

This list of advantages, including ethical ones, provides a strong incentive to develop and deploy autonomous systems. Despite such advantages, a variety of ELSI concerns have been raised about autonomous systems and are discussed below.⁴

⁴ The concerns described below are drawn from a number of sources, including Patrick Lin, “Ethical Blowback from Emerging Technologies,” *Journal of Military Ethics* 9(4):313-331, 2010.

- Function as anticipated in realistic operational environments against adaptive adversaries;
- Complete engagements in a timeframe consistent with commander and operator intentions and, if unable to do so, terminate engagements or seek additional human operator input before continuing the engagement; and
- Be sufficiently robust to minimize failures that could lead to unintended engagements or to loss of control of the system to unauthorized parties.

The policy permits use of semiautonomous weapons systems to deliver kinetic or nonkinetic, lethal or nonlethal force in most combat situations, subject to the requirements described above regarding the laws of war and so on. The policy also permits the use of human-supervised autonomous weapon systems in local defense scenarios to select and engage (nonhuman) targets to respond to time-critical or saturation attacks against manned installations and onboard defense of manned platforms. (This provision allows systems such as the Phalanx Close-in Weapons System (CIWS) to operate in its fully autonomous mode.) Last, it permits the use of autonomous weapon systems in the context of applying nonlethal, nonkinetic force, such as some forms of electronic attack, against materiel targets.

The DOD does not currently possess autonomous weapons systems designed for use in scenarios other than those described in the previous paragraph. But in the future, the acquisition of such weapons systems (that is, autonomous weapons systems designed for use in other scenarios) will be subject to two special additional reviews involving the Undersecretaries of Defense for Policy and for Acquisition, Technology and Logistics, and the Chairman of the Joint Chiefs of Staff. Before a decision to enter into formal development, a review will ensure that the development plan meets the requirements of the policy described above. Before a decision to field such a weapons system, a review will ensure that the weapon to be fielded does meet the requirements of the policy described above and, further, that relevant training, doctrine, techniques, tactics, and procedures are adequate to support its use.

Finally, in an acknowledgment that technology will inevitably evolve, the directive states that the policy will expire in 10 years (on November 22, 2022) if it has not been reissued, canceled, or certified current by November 22, 2017.

International Law

Autonomous systems—especially lethal autonomous systems—complicate today’s international law of armed conflict (LOAC) and domestic law as well. Some relevant complications include the following:

- Individual responsibility is one of the most important mechanisms for accountability under LOAC. However, an autonomous system taking an action that would be a LOAC violation if taken by a human being

cannot be punished and is not “accountable” in any meaningful sense of the term. Behind the actions of that system are other actions of a number of human beings, who may include the system operator, those higher in the chain of command who directed that the system be used, the system developer/designer/programmer, and so on. How and to what extent, if any, are any of these individuals “responsible” for an action of the system?⁵

- How and to what extent can lethal autonomous systems distinguish between legitimate and illegitimate targets (such as civilian bystanders)? How and to what extent can such a system exercise valid judgment that “pulling the trigger” does not result in “excessive” collateral damage?

- How might autonomous systems contribute to a lowering of the threshold for engaging in armed conflict? Some analysts argue that the use of remotely operated lethal autonomous systems in particular emboldens political leaders controlling the use of such weapons to engage in armed conflict.⁶ The argument, in essence, is that nation X will be more likely to wage war against nation Y to the extent that nation X’s troops are not in harm’s way, as would be the case with weapons system operators doing their work from a sanctuary (e.g., nation X’s homeland) rather than in the field (that is, on the battlefield with nation Y’s troops). Under such a scenario, the use of force (that is, the use of such systems) is less likely to be a true act of last resort, and thus violates the “last resort” principle underlying jus ad bellum.

Impact on Users

The armed forces of the world have a great deal of experience with traditional combat, and still the full range of psychological and emotional

⁵ A military organization provides a chain of command in which some specific party is responsible for deciding whether a system or weapon is used, and if untoward things happen as the result of such use, the presumption is that this individual specific party is still responsible for the bad outcome. This presumption can be rebutted by various mitigating circumstances (e.g., if further investigation reveals that the weapon itself was flawed in a way that led directly to the bad outcome and that the responsible party had no way of knowing this fact).

⁶ See, for example, Peter Asaro, “Robots and Responsibility from a Legal Perspective,” *Proceedings of the IEEE 2007 International Conference on Robotics and Automation, Workshop on RoboEthics*, April 14, 2007, Rome, Italy, available at <http://www.peterasaro.org/writing/ASARO%20Legal%20Perspective.pdf>; Rob Sparrow, “Killer Robots,” *Journal of Applied Philosophy* 24(1):62-77, 2007; and Noel Sharkey, “Robot Wars Are a Reality,” *The Guardian* (UK), August 18, 2007, p. 29, available at <http://www.guardian.co.uk/commentisfree/2007/aug/18/comment.military>. Also cited in Patrick Lin, George Bekey, and Keith Abney, *Autonomous Military Robotics: Risk, Ethics, and Design*, California Polytechnic State University, San Luis Obispo, Calif., 2008.

effects of combat on soldiers is not well understood. Thus, there may well be some poorly understood psychological effects on soldiers who engage in combat far removed from the battlefield.

For example, a 2011 report from the United States Air Force School of Aerospace Medicine, Department of Neuropsychiatry, on the psychological health of operators of remotely piloted aircraft and supporting units identified three groups of psychological stressors on these operators:⁷

- Operational stressors (those related to sustaining operations) include issues such as restricted working environments (e.g., ground control stations with limited freedom for mobility) and poor workstation ergonomics.
- Combat stressors (those that involve missions undertaken in direct support of combat operations) include stresses induced in operators of remotely piloted vehicles who must manage their on-duty warrior role contemporaneously with their role as one with domestic responsibilities arising from being stationed at home.
- Career stressors (those arising from the placement of individuals into positions requiring the flying of remotely piloted vehicles) include poorly defined career fields with uncertain career progression, especially for those who have previously qualified for piloting manned aircraft. What is the psychological impact on a Navy pilot when a remotely piloted vehicle can land with ease on an aircraft carrier at night in a storm, or on a specialist in explosive ordnance disposal when a bomb disposal robot can disarm an improvised explosive device without placing the specialist at risk?⁸ How will such individuals demonstrate courage and skill to their superiors and colleagues when such technologies are available?

Humanity of Operators

In the context of armed remotely piloted vehicles (RPVs), concerns have been raised about psychological distancing of RPV operators from

⁷ Wayne Chappelle et al., *Psychological Health Screening of Remotely Piloted Aircraft (RPA) Operators and Supporting Units*, RTO-MP-HFM-205, USAF School of Aerospace Medicine, Department of Neuropsychiatry, Wright-Patterson Air Force Base, Ohio, 2011.

⁸ Peter Singer describes individuals from the Foster Miller Company in Waltham, Massachusetts, talking about the moment at which they decided to use robots for explosive ordnance disposal (EOD). Teams had received robots for EOD but were not using them. But an incident occurred in which two EOD technicians were killed in Iraq, and the prevailing sentiment shifted quickly from "We leave the robots in the back of the truck" and "We don't use them because we're brave" to "You know what? We really do have to start using them." See Robert Charette, "The Rise of Robot Warriors," *IEEE Spectrum*, June 2009, available at <http://spectrum.ieee.org/robotics/military-robots/the-rise-of-robot-warriors>.

their targets. Quoting from a report of the UN Human Rights Council,⁹ “[B]ecause operators are based thousands of miles away from the battlefield, and undertake operations entirely through computer screens and remote audiofeed, there is a risk of developing a ‘Playstation’ mentality to killing.”

Others counter such notions by pointing out that killing at ever-larger distances from one’s target characterizes much of the history of warfare. Increasing the distance between weapons operator and target generally decreases the likelihood that the operator will be injured, and indeed there is no legal requirement that operator and target must be equally vulnerable.

Organizational Impacts

New technology often changes relationships within an organization. For example, the scope and nature of command relationships for the use of that technology are not arbitrary. Someone (or some group of individuals) specifies these relationships. Under what circumstances, if any, is an individual allowed to make his or her own decision regarding placement of a system into a lethal autonomous mode? Who decides on the rules of engagement, and how detailed must they be?

A second example of organizational impact is that autonomous systems reduce the need for personnel—in such an environment, what becomes of promotion opportunities, which traditionally depend in part on the number of personnel that one can command effectively? How do personnel needs affect the scale of financial resources required by an organization?

A third example is that a military organization built around the use of autonomous systems may be regarded differently from one organized traditionally. For example, it is worth considering the controversy over a proposal to introduce a new medal to recognize combat efforts of drone and cyber operators (Box 3.2). The proposal was intended to elevate the status of the operators, recognizing their increasing importance to modern combat. But the public reaction to the proposal reflected skepticism of the idea that a soldier who operates a drone or engages in cyber operations should be recognized and decorated in the same way as the soldier who risks his or her life in the actual theater of battle.

A final example of organizational impact is that autonomous systems

⁹ Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Study on Targeted Killings, Human Rights Council, ¶ 84, UN Doc. A/HRC/14/24/Add.6, May 28, 2010, available at <http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf>.

Box 3.2 The Distinguished Warfare Medal

In February 2013, then-Defense Secretary Leon Panetta proposed the “Distinguished Warfare Medal” to recognize drone operators and cyber warriors whose actions “contribute to the success of combat operations, particularly when they remove the enemy from the field of battle, even if those actions are physically removed from the fight.”¹ While most agreed that electronic warriors deserve recognition for their contributions to war efforts, many were upset at the proposal that this medal would rank above the Bronze Star (awarded for heroic or meritorious acts of bravery on the battlefield) and the Purple Heart (awarded to soldiers who have been injured in battle). In addition, military decorations and recognition are important for promotions. The designation of the Distinguished Warfare Medal as higher than other medals awarded for physical valor in the theater of battle left many veterans feeling insulted and created a great deal of backlash from the Pentagon, veterans groups, and many members of Congress.

Shortly after taking office, Defense Secretary Chuck Hagel ordered a review of the new medal, resulting in a decision to replace the medal with a “distinguishing device” that would be placed on an existing medal to honor the combat achievements of drone and cyber operators. Such a distinguishing device would be similar to the “V” placed on the Bronze Star to indicate valor.

¹ Lolita Baldor, “Pentagon Creates New Medal for Cyber, Drone Wars,” Associated Press, February 11, 2013, available at <http://bigstory.ap.org/article/pentagon-creates-new-medal-cyber-drone-wars>.

raise questions regarding accountability. If an autonomous system causes inadvertent damage or death, who is accountable? What party or parties, for example, are responsible for paying punitive or compensatory damages? The party ordering the system into operation? The programmers who developed the controlling software? The system’s vendor? Is it possible for no one to be responsible? If so, why? What counts as sufficient justification?

Technological Imperfections

Autonomous systems have been known to “go haywire” and harm innocents around them. Such problems obviously present safety issues. Moreover, how and to what extent are operators in the vicinity of an autonomous system entitled to know about possible risks? A pilot in an airplane that is partially out of control may be able to steer the airplane away from populated areas—what of the operator of a remotely piloted

aircraft that is partially out of control? What are the responsibilities of programmers of an RPV to prevent it from landing in a populated area?

Cybersecurity issues are also often overlooked in the rush to deployment of first-generation technologies. In one instance, video feeds from RPV to operator were not encrypted and adversaries could easily intercept the signals.¹⁰ In another instance, a group of university researchers took control of an unmanned aerial vehicle owned by the college after the U.S. Department of Homeland Security asked them to demonstrate such a capability.¹¹

Yet another issue is the ethical standard to which autonomous systems should be held. In particular, for any given dimension of performance, is it sufficient that they do better (on average) than humans can do? Or should they be held to a much higher standard, perhaps a standard of near-perfection? Although the first (weaker) standard is an instance of technology enabling a greater degree of ethical behavior on the battlefield, it is also true that an ethically questionable action of an autonomous system will result in criticism of the system's autonomy as being flawed and ethically improper. And this will still be true even if the system has built up a long record of ethically appropriate performance.

Adversary Perceptions and Use

To the extent that new technologies bring overwhelming advantages against an adversary, the adversary may well respond with behavior that we might regard as improper or unethical; for example, the adversary may use tactics (such as the use of civilians as human shields for military targets) that violate the laws of war. (Indeed, adversaries may use such tactics even without U.S. use of new technologies—but at the very least the new technologies may provide a post hoc justification for unethical tactics.)

In the case of armed remotely piloted vehicles, concerns have been raised that such use enables the insurgent adversary to cast itself in the role of underdog and the West as a cowardly bully that is unwilling to risk its own troops but is happy to kill remotely.¹² Furthermore and regardless of their perceptions of the United States, adversaries may also want to

¹⁰ Siobhan Gorman, Yochi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones," *Wall Street Journal Online*, December 17, 2009, available at <http://online.wsj.com/article/SB126102247889095011.html>.

¹¹ "Texas College Hacks Drone in Front of DHS," RT.com, June 28, 2012, available at <http://rt.com/usa/news/texas-1000-us-government-906/>.

¹² See paragraph 519 in Ministry of Defence, 2011, *Joint Doctrine Note 2/11: The UK Approach to Unmanned Aircraft Systems*, available at <http://dronewarsuk.files.wordpress.com/2011/04/uk-approach-to-uav.pdf/>.

acquire and use such vehicles as well. For example, terrorists could use small drones for assassination purposes, and they could easily be used on U.S. soil.

Civilian Uses

Autonomous systems have a number of civilian applications. Law enforcement authorities can make and have made use of RPVs for surveillance and of bomb disposal robots. Truck and car driving can now be automated under many circumstances,^{13,14} although such driving is not common today. Unpiloted airplanes may soon be used for transporting cargo. And criminals have used remotely piloted vehicles as transport mechanisms for removing stolen property from the site of the crime.¹⁵

Law enforcement authorities act domestically, and within the continental United States a variety of legal protections operate that do not apply overseas. Using technologies originally developed for military application (and in particular for use against non-U.S. citizens outside the borders of the United States) within the United States (e.g., for border surveillance, location of fleeing fugitives) raises a host of potential issues related to civil liberties. The issue is not so much whether these military systems can be usefully and practically employed to assist domestic law enforcement authorities (they do have potential value for certain applications), as it is questions concerning the scope, nature, extent, and conditions of such use. Put differently, the use of military systems in a domestic context raises ethical, societal, and policy questions that are largely open at the time of this writing.

The law enforcement issues are only one policy element of domestic use. For example, liability issues concerning autonomous trucks and cars (technology for which was developed in part by DARPA) have yet to be worked out in any systematic way, at least in part because the authors of today's laws did not contemplate such vehicles. Various regulatory issues related to safe operation of autonomous vehicles (specifically, RPVs) are in

¹³ "Preparing for DARPA's Urban Road Challenge," Cnet.com, January 26, 2007, available at http://news.cnet.com/Preparing-for-DARPAs-urban-road-challenge/2100-11394_3-6153932.html.

¹⁴ "Google Driverless Cars: Genius or Frightening Folly," Electricpig.co.uk, October 11, 2010, available at <http://www.electricpig.co.uk/2010/10/11/google-driverless-cars-genius-or-frightening-folly/>.

¹⁵ Singer reports on a Taiwanese gang that used tiny helicopters with pinhole cameras to carry out a jewelry heist and got away with \$4 million in jewels. See "More Countries, Organizations Seeking to Use Aerial Drones for Peaceful, Nefarious Purposes," October 26, 2011, available at <http://www.pri.org/stories/science/technology/more-countries-organizations-seeking-to-use-aerial-drones-for-peaceful-nefarious-purposes-6639.html>.

the process of being addressed at the time of this writing.¹⁶ Finally, what of the use of such technologies by private citizens to spy on each other or to perform independent environmental monitoring?¹⁷

3.2 PROSTHETICS AND HUMAN ENHANCEMENT

Today, prostheses have been developed for replacement of lost bodily function, but in principle, prostheses could be developed to enhance human functions—physical functions such as lifting strength and running speed and sensory functions such as night vision and enhanced smell.

3.2.1 The Science and Technology of Prosthetics and Human Enhancement

Prostheses are devices that are intended to replace missing human body parts. The discussion below focuses on prostheses that replace body parts that serve physical functions, such as vision or locomotion. Neural prostheses are addressed in the Chapter 2 section on neuroscience.

All prostheses have two components—an assembly (which may be biological and/or electromechanical in nature) and an interface to the human body to which the prosthesis is attached. The assembly replaces the missing part's function and usually has several components:

- Sensors that provide information to the body about the assembly's behavior, configuration, and state.
- Receivers that accept information from the body and thus provide guidance to the assembly about the body's intention for the assembly.
- Actuators that produce the output of that assembly—forms of output are sometimes electrical (as in the case of a prosthesis for a sensory organ) or mechanical (as in the case of a prosthesis for a limb).
- A processing unit that controls the assembly's operation.

The interface transmits information from the assembly's sensors to the body's nervous system and from the nervous system to the assembly. But information flows in the human body are not encoded in forms that are well understood with today's science. Today, a key factor limiting the development of prostheses—at least prostheses that are integrated

¹⁶ For example, the FAA Modernization and Reform Act of 2012 calls on the FAA to fully integrate unmanned systems, including for commercial use, into the national airspace by September 2015.

¹⁷ Siobhan Gorman, "Drones Get Ready to Fly, Unseen, into Everyday Life," *Wall Street Journal*, November 3, 2010, available at <http://online.wsj.com/article/SB10001424052748703631704575551954273159086.html>.

into the human body to be used in a highly natural way—is likely to be understanding information flows in a useful way, and how to interpret the signals from the nervous system that indicate intentionality and how to translate sensor information into forms that the human nervous system can usefully process.¹⁸

As a general rule, today’s state of the art does not result in prosthetic devices that can function nearly as effectively as the human parts they replace. For example, one state-of-the-art visual prosthesis enables a large number of its users to read large-font type and sometimes to recognize words.¹⁹ Considering that these individuals were previously unable to read at all, such a prosthesis is remarkable, but no one would argue that it has come close to being a serious replacement for a lost human eye.

3.2.2 Possible Military Applications

To date, prosthetic devices are under development only for the replacement of lost human function (e.g., a prosthetic limb), and as noted above, they are far from achieving such functionality. But there is no reason in principle that they cannot be designed to exceed human capabilities. Visual prostheses could be designed to see infrared light or to provide telescopic vision. Aural prostheses could be designed to provide better-than-normal hearing. A powered arm or leg prosthesis could be designed to have significantly greater strength than a human arm or leg. Some DARPA efforts have focused explicitly on human enhancement (e.g., increased strength,²⁰ improved cognition,²¹ lowered sleep requirements²²).

If the constraint on integration into the human body is relaxed, devices that replace and even augment human function—devices that have already been designed and tested although they are not available for widespread use today—could come into use. For example, exoskeletons have been developed that can help disabled wheelchair-bound individuals to leave their wheelchairs behind. Other exoskeletons have been

¹⁸ A second limiting factor is the energy storage capacity of reasonably sized batteries.

¹⁹ Lyndon da Cruz et al., “The Argus II Epiretinal Prosthesis System Allows Letter and Word Reading and Long-Term Function in Patients with Profound Vision Loss,” *British Journal of Ophthalmology* 97(5):632-636, 2013, available at <http://bj.o.bmj.com/content/early/2013/02/19/bjophthalmol-2012-301525.full>.

²⁰ See http://www.darpa.mil/Our_Work/DSO/Programs/Warrior_Web.aspx.

²¹ Mark St. John et al., “Overview of the DARPA Augmented Cognition Technical Integration Experiment,” 2007, available at www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA475406.

²² Sam A. Deadwyler et al., “Systemic and Nasal Delivery of Orexin-A (Hypocretin-1) Reduces the Effects of Sleep Deprivation on Cognitive Performance in Nonhuman Primates,” *Journal of Neuroscience* 27(52):14239-14247, 2007, available at <http://www.jneurosci.org/content/27/52/14239.abstract>.

developed to enable individuals to lift much heavier loads than would be possible for unassisted individuals. These latter devices have not been designed for use in direct combat—rather, they enable soldiers in the field to move and handle heavy logistic burdens more easily.

3.2.3 Ethical, Legal, and Societal Questions and Implications

In a nonmilitary context, ethical, legal, and societal issues regarding prosthetics and human enhancement technology span a wide range, and some if not most of these issues spill over into the military context. Such issues include (but are not limited to):

- Exacerbation of economic inequalities due to the high cost of prostheses.
- Damage to solidarities and/or culture based on a group's common experience with lost human function (as is the concern of many in the deaf community).
- Reducing the importance and value of human effort in improving human function (a particularly important point when considering enhancements). If anyone can become very fast, or very strong, or very smart simply by using a prosthetic device, how should we regard an individual who has expended a great deal of personal effort to become faster, stronger, or smarter?

The remainder of this section addresses a number of ethical, legal, and societal issues related to prosthetics and human enhancement that emerge in the military context.²³

International Law

The Martens clause contained in the 1977 Additional Protocol to the Geneva Conventions in essence prohibits weapons whose use would violate the laws of humanity and the requirements of the public conscience. Established as a way to ensure that the use of weapons not explicitly covered by the conventions was not necessarily permitted by them, the Martens clause is broadly recognized as having no accepted interpretation. Nevertheless, some analysts argue that the existence of the Martens clause

²³ Patrick Lin, "More Than Human? The Ethics of Biologically Enhancing Soldiers," *The Atlantic*, February 16, 2012, available at <http://www.theatlantic.com/technology/archive/2012/02/more-than-human-the-ethics-of-biologically-enhancing-soldiers/253217/>.

raises the issue of whether a highly enhanced human soldier engaging in combat might himself be such a weapon.²⁴

Safety and Other Effects on the Recipients of Enhancements

Traditional biomedical ethics come into play any time a foreign object or substance is introduced into the human body, and safety is one of its primary concerns. But when the human body is that of a soldier, especially one who may go into combat, and the soldier functions within a military chain of command, how and to what extent, if any, should concerns about personal safety be weighed against battlefield advantages that an enhancement may afford the user? And what happens if the enhancement is still in its early developmental stages, when the safety risks may be understood only very poorly?

Safety risks may be compounded by exposure to cyber security threats. To the extent that these devices depend on information technology, they may be subject to cyber attacks that could alter their function in dangerous ways or cause them to malfunction. Privacy, too, is an issue—how and to what extent are data associated with the use of these devices sensitive? Does it constitute personal health information that requires special protections?

Reversibility is an ELSI concern as well. Can any deleterious effects of an enhancement on the human body be reversed by removing the prosthesis from the body? Should an enhancement be removed when a soldier leaves military service?

Last, what are the psychological effects of human enhancements that are integrated into the human body? How and to what extent, if any, do they change an individual's conception of himself or herself? How long-lasting are such changes? What is the significance of such changes? Might enhanced soldiers take more personal risks? And how will unenhanced soldiers react to the availability of enhancements for others? For example, will unenhanced soldiers demand them for their own use?

Organizational Issues

How and to what extent, if at all, should a military organization regard enhanced soldiers differently from unenhanced soldiers? For example, what of:

²⁴ See Patrick Lin, Maxwell J. Mehlman, and Keith Abney, *Enhanced Warfighters: Risk, Ethics, and Policy (Greenwall Report)*, California Polytechnic State University, San Luis Obispo, Calif., 2013, pp. 34-35, available at http://ethics.calpoly.edu/Greenwall_report.pdf.

- Expectations for combat behavior,
- Rates of promotion and decoration,
- Integration into existing military units,
- Needs for rest and recuperation, and
- Terms of service in the armed forces.

Civilian Use

Use of prosthetic and enhancement technologies in the civilian sector raises a number of ethical, legal, and societal issues.

For individuals transitioning from military to civilian life, policy makers must ask whether prosthetic and enhancement technologies acquired in the military will remain with the individual. In some cases (e.g., prosthetic limbs that replace lost human function), there may be a social contract that allows these individuals to retain these devices. But should retiring soldiers be allowed to keep devices that enhance their performance? How well will such individuals integrate with civilian society?

Prosthetic and enhancement technologies also move the traditional boundaries separating disability from normal function and normal function from enhanced function—and sometimes certain legal categories are based on traditional boundaries. For example, being a member of a certain legal class (e.g., those individuals regarded as blind or deaf) may be an entitlement gateway for certain benefits; how, if at all, should prosthetic technology change an individual's eligibility for those benefits?

Implanted devices retained by individuals may also subject them to certain restrictions, ranging from increased screening at airports to restricted travel to countries that may be on some “no-export” list. And do individuals actually own their prosthetic devices, in the sense of being allowed to control all uses of such a device? (For example, could they themselves modify it?)

Unanticipated Effects

In his presentation to the committee, Nick Agar of the Victoria University of Wellington introduced the notion that human enhancement technologies might have priming effects on their users. He illustrated the point by describing research on implicit memory effects—subtle and unconscious effects of prior stimuli on human behavior—citing the example of people reading lists of adjectives describing stereotypical attributes of the elderly and then displaying behaviors of the elderly such as stooped

walking.²⁵ In the case of enhancement technologies, Agar speculated that the priming effect might be driven by the stimuli of the technology's function. For example, a prosthetic limb designed in part to serve as a weapon might have a subtle, ongoing priming effect on its bearer that would make him or her more aggressive.

3.3 CYBER WEAPONS

Cyber weaponry opens up a new dimension of warfare that may target critical infrastructures on which society will increasingly depend, generating vast increases in cost to defend and to generate countervailing attack technologies.

3.3.1 The Technology of Cyber Weapons

Cyber weapons are configurations of information technology (either hardware or software) that can be used to affect an adversary's information technology systems and/or networks. Because such weapons are fundamentally based on today's information technology, experts in the field understand the basic technological building blocks of cyber weapons well. That is, there are no "new" technologies that contribute uniquely to cyber weaponry, although new ways of using more mature technologies can certainly emerge. Furthermore, nonstate actors (e.g., terrorists, criminals, random hackers) can develop and/or use certain cyber weapons.

Cyber weapons gain their power and sophistication from two facts. First, the basic technological building blocks can be arranged in many different ways, and those arrangements are limited only by human creativity and ingenuity. Second, cyber weapons are generally designed to target systems that are complex and thus have many failure modes.

These two facts mean that cyber weapons can operate through mechanisms that are quite surprising and difficult to understand, and can thus appear to involve entirely novel capabilities (sometimes looking like "magic" to an uninitiated observer). In practice, these mechanisms will almost always take advantage of sometimes obscure or subtle weak points (that is, vulnerabilities) in a system or the socio-technical organization in which the system is embedded.

In addition, cyber weapons can be designed to be highly discriminating or highly indiscriminate in their targeting. As a general rule, highly discriminating cyber weapons (that is, weapons that affect only their spec-

²⁵ John A. Bargh, Mark Chen, and Lara Burrows, "Automaticity of Social Behavior: Direct Effects of Trait Construct and Stereotype-Activation on Action," *Journal of Personality and Social Psychology* 71(2):230-244, 1996.

ified targets and nothing else) are more difficult to design and implement than are weapons that are more indiscriminate. Highly discriminating weapons also require a great deal of intelligence support for their use—and in the absence of adequate intelligence, the effects of using even a highly discriminating cyber weapon may cascade if previously unknown elements are connected (directly or indirectly) to the targeted system.

3.3.2 Possible Military Applications

Cyber weapons can be used to compromise the confidentiality of information, the integrity of information or software/programming, or the availability of IT-based services:²⁶ to the user and also to forge authenticity:²⁶

- *Breaching the confidentiality of information* refers to the ability to obtain from the targeted IT system information that the rightful owner or operator of that system would prefer to keep confidential. For example, an adversary listens to a Wi-Fi connection between a computer and a base station and is able to capture the data stream between them.

- *Compromising the integrity of computer-represented data* refers to changing or destroying information that its rightful owner wishes to keep intact. That data may be input to computer programs or machine-readable programs themselves. For example, a computer virus can erase all of the files on a user's hard drive.

- *Denying the availability of IT-based services to users* refers to preventing a user from obtaining the full value of his or her interactions with the computer. If the user finds the computer too slow to respond, or that it does not respond at all, availability has been denied. For example, a denial-of-service attack on an important Web site keeps legitimate and authorized users from accessing the services it provides.

- *Forging authenticity.* An authentic message or transaction is one known to have originated from the party claiming to have originated it. Forgery leads the receiver of the message or the other party in a transaction into believing that the sender or first party in a transaction is who he claims to be, even if that is not true.

Cybersecurity analysts distinguish between cyber exploitation and cyber attack. Cyber exploitation refers to activities involving the first bulleted item above (breaching confidentiality), cyber attack to activities involving the second, third, and fourth items above (compromising integ-

²⁶ This discussion of cyber weapons borrows liberally from National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, The National Academies Press, Washington, D.C., 2009.

rity, denying availability, forging authenticity). Many policy makers today believe that cyber exploitations conducted against the United States are a major threat to its economic security, and perhaps even more significant than traditional military threats.

Cyber weapons can cause temporary damage or permanent damage. Some examples of temporary damage include denial-of-service attacks; operations that take advantage of bugs in a target system, causing a machine to crash and reboot at critical times (but leaving it otherwise unharmed); attacks that change the configuration of a system (e.g., to give false credentials that allow an intruder to gain access), and so on.

Examples of permanent damage include injection of commands into database queries to delete or alter data in the database, modification of programs to cause subtle and slow changes in databases such that all of the user's backup files are corrupted and hence the entire database becomes unrecoverable for all practical purposes, and programs that destroy hardware (e.g., by repeatedly writing flash memories in a way that uses up their limited write cycles).

Another class of attacks targets not the computers per se but the physical devices that may be controlled by those computers. Computers often control equipment such as ultracentrifuges or refrigerators or diesel generators, and by introducing faulty programming into the computer controllers of the targeted equipment, it is possible to destroy or damage such equipment.²⁷ Furthermore, it is sometimes possible to compromise the controlling computers in such a way that reinstallation of all of the original software does not restore the computer to its original state—that is, only a replacement of the corrupted computer would suffice to restore the controller to its original state.

A different class of attacks is designed not so much to reduce the actual functionality of the targeted IT systems or networks as to reduce the user's confidence or ability in using them. For example, a user can lose confidence in a system even if the actual damage to the system is relatively minor. (A calculator may provide an accurate answer to a given addition 99.9 percent of the time, but if the user does not know the precise circumstances under which it provides an inaccurate answer, he may well refrain from using it for any calculation at all.) Or an attack on an adversary's primary IT system may force him to use a backup system, which may well have less functionality or which the adversary may use less effectively.

A cyber weapon of special power and significance is the botnet. Bot-

²⁷ For example, the Stuxnet computer worm, first discovered in June 2010, was aimed at disrupting the operation of Iran's uranium enrichment facilities. See http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html.

nets are arrays of compromised computers connected to the Internet that are remotely controlled by the attacker. The attack value of a botnet arises from the sheer number of computers that an attacker can control—often tens or hundreds of thousands and perhaps as many as a million. Since all of these computers are under one party’s control, the botnet can act as a powerful amplifier of an attacker’s actions. Although botnets are known to be well suited to certain denial-of-service attacks, their full range of possible utility has not yet been examined.

3.3.3 Ethical, Legal, and Societal Questions and Implications²⁸

The use of cyber weapons in conflict as a deliberate instrument of national policy raises a variety of ethical, legal, and societal issues.

International Law

Although the United States has stated its view that the law of armed conflict applies to cyberspace,²⁹ this view has not been explicitly endorsed by all of the signers of the Geneva and Hague Conventions or the UN Charter. In addition, cyber warfare raises a variety of questions about how to interpret LOAC in any given scenario involving the use of cyber weapons.³⁰ Moreover, even if LOAC does not apply in any given scenario, the principles underlying LOAC may still be relevant to the ethics of using cyber weapons in that scenario.

For example, the laws of war address the circumstances under which the use of force can be legally justified (also known as *jus ad bellum* and further discussed in Chapter 4). Some of the underlying principles include the following:

- *Assignment of responsibility for a hostile act to the appropriate nation.* In a cyber context, it may be difficult to ascertain the identity of the responsible nation. In some (perhaps many) cases, a hostile cyber operation

²⁸ See, for example, Patrick Lin, “Robots, Ethics, & War,” Center for Internet Society at Stanford Law School, December 15, 2012, available at <http://cyberlaw.stanford.edu/blog/2010/12/robots-ethics-war>.

²⁹ “International Law in Cyberspace,” remarks of Harold Hongju Koh, legal advisor of the U.S. Department of State, to the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Md., September 18, 2012, available at <http://www.state.gov/s/1/releases/remarks/197924.htm>.

³⁰ The most comprehensive source on this topic is Michael Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, available at <http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft.pdf>.

may have been perpetrated by a subnational group, and the responsible party may not be a nation at all. This point suggests that it may be very hard to know the party against which a response should be targeted, or if international law per se is even applicable.

- *The fuzziness of the lines between cyber crime and cyber war*, the former being a law enforcement matter and the latter being a matter of national security. Moreover, because the damage from an individual cyber attack can be very small, the precise point at which a set of many cyber attacks becomes a national security issue may be unclear.

The laws of war also address how opposing forces must behave in the conduct of conflict (known as *jus in bello* and further discussed in Chapter 4). Some of the principles include the following:³¹

- *Differentiation between military and civilian targets*. In general, ethical considerations suggest that only military entities should be targeted. A party aiming kinetic weapons often (indeed, usually) has reasonably direct confirmation that a given target is indeed military. But how does a cyber targeter know that a given computer is indeed a military computer? Any computer could be located at a specific Internet Protocol (IP) address, and IP addresses for a given computer are not necessarily static. In the absence of a machine-readable indication that any given computer is in fact a military computer, an intelligence collection effort must be undertaken to determine the extent to which the computer has military purposes. What evidence and what degree of certainty in the intelligence information are sufficient to make a determination that a given computer is a valid military target?

- *Avoidance of collateral damage*. A second principle is that in attacking military targets, targeters should seek to avoid accidental, inadvertent, or undesired harm to civilians and their property. But a cyber attack may inflict damage on some civilian computers. What consideration should such damage receive in attack planning, especially if it does not result in death or physical destruction? Moreover, given that the success of many cyber attacks depends on good intelligence about their targets, how should commanders estimate likely collateral damage when good intelligence about newly discovered cyber targets is sparse?

- *Cease-fire and conflict termination*. What constitutes a cease-fire in cyberspace between two adversaries? How can the two sides in a cyber-

³¹ For further discussion, see Chapter 7 of National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, The National Academies Press, Washington, D.C., 2009.

conflict negotiation meaningfully demonstrate their commitment to a cease-fire?

Outside the existing law of armed conflict, cyber weapons introduce the possibility that international law could or should evolve to manage new kinds of harm that might be caused through the use of such weapons. Neither LOAC nor any other international law prohibits the conduct of espionage. But this legal tradition evolved before deployments of information technology made it possible to find and exfiltrate much larger volumes of information, and in an era when information is a key coin of the realm, the large-scale exfiltration of important information from a nation surely raises a number of ethical, legal, and societal issues. Should exfiltration of information continue to be legal? If not, what kinds of and how much information exfiltration should be allowed under what circumstances? How might exfiltration be regulated or rules regarding exfiltration be enforced?

Domestic Law

The United States Code includes Title 10, which relates to military matters; Title 50, which relates to intelligence matters; and Title 18, which relates to law enforcement and criminal matters. But the nature of cyber weaponry is that military forces, intelligence agencies, and law enforcement agencies can all find value in the use of cyber weapons under certain circumstances, and the separate legal frameworks of Title 10, Title 50, and Title 18 inevitably leave gaps or result in a lack of clarity about which agencies of the U.S. government should take the lead regarding the use of cyber weapons in any given situation.

As one example of gaps in current domestic law, private-sector entities are prohibited by Title 18 from engaging in offensive operations in cyberspace to protect themselves. Whether or not this policy is wise and appropriate for the nation is subject to debate—but it is manifestly clear that current law forbidding private parties to engage in self-help in cyberspace was formulated many years before the issue attained its current significance.

Civilian Uses

Civilian users have plausible and legitimate uses for cyber weapons. The most common purpose is for developing and testing cyber defenses. Penetration testing—a legitimate activity of civilian enterprises that tests their cyber defenses for their resistance to cyber attack—demands the use of cyber weapons that are comparable to those that might be used in a real

attack. And the development of defenses against particular cyber attacks requires having the appropriate cyber weapons available for use in the development environment.

Organizational Impacts

The use of cyber weapons as an instrument of government policy has many organizational implications. For example, organizations established to use cyber weapons must consider matters such as training, liability for any use of such weapons that harms innocent parties, recruitment (how to obtain personnel skilled in the use of such weapons who can be trusted to use them in the service of legitimate government goals), command and control and rules of engagement (how and under what circumstances cyber “shooters” receive orders to use their weapons, whose authority is needed to issue such orders), and identification friend-or-foe, the process by which legitimate cyber targets are identified.

Adversary Perceptions

The alleged U.S. use of cyber weapons (alleged because such use has not been publicly acknowledged by the U.S. government) against Iran (the Stuxnet worm, as described in Footnote 27) has spawned concerns that cyber weapons released “into the wild” and then used against adversary targets will rebound against U.S. interests in several ways. The first concern is that the use of such weapons by the United States legitimates them as an instrument of international conflict, and increases the likelihood that other nation-states will use them against the United States in a future conflict or disagreement. A second concern is that such use flies in the face of long-standing U.S. policy pronouncements about the value of a secure Internet environment for the entire world. Last, there is a concern that the code—the actual programming—can be reverse-engineered and then used by adversaries to develop cyber weapons of their own.

3.4 NONLETHAL WEAPONS

The U.S. Department of Defense defines “nonlethal weapons” as “weapons . . . designed and primarily employed to incapacitate targeted personnel or materiel immediately, while minimizing fatalities, permanent injury to personnel, and undesired damage to property in the targeted areas or environment. Non-lethal weapons are intended to have reversible effects on personnel or materiel.” Other terms used to refer to similar weapons include “less lethal,” “less than lethal,” “prelethal,” and “potentially lethal.”

3.4.1 The Technology of Nonlethal Weapons

The general class of nonlethal weapons includes a wide variety of technologies:

- Kinetic weapons are decidedly low-tech—bean-bag rounds for shotguns and rubber bullets for pistols have been used for a long time.
- Barriers and entanglements can be used to stop land vehicles moving at high speed (such as a car trying to speed through a checkpoint) or to damage propellers of waterborne craft.
- Optical weapons (e.g., dazzling lasers) are used to temporarily blind an individual using bright light—the individual must shut or avert his eyes to avoid pain. Such weapons are often used on individuals operating a vehicle, with the intent of forcing the driver to stop or flee.
- Acoustic weapons project intense sound waves in the direction of a target from long distances, and individuals within effective range feel pain from the loud sound.
- Directed-energy weapons that project millimeter-wave radiation can cause a very painful burning sensation on human skin without actually damaging the skin.³² Such weapons, used to direct energy into a large area, are believed to be useful in causing humans to flee an area to avoid that pain. Other directed-energy weapons direct high-powered microwave radiation to disrupt electronics used by adversaries.
- Electrical weapons (e.g., tasers and stun guns) use high-voltage shocks to affect the nervous system of an individual, causing him or her to lose muscle control temporarily. One foundational science for understanding such effects is neuroscience, as discussed in Chapter 2.
- Biological and chemical agents may be aimed at degrading fuel or metal, or may target neurological functions to incapacitate people, repel them (e.g., with a very obnoxious odor), or alter their emotional state (e.g., to calm an angry mob, to induce temporary depression in people). For the latter types of effects, a foundational science for understanding such effects is neuroscience.
- Cyber weapons are often included in the category of “nonlethal” weapons because they have direct effects only on computer code or hardware.

³² Directed-energy weapons with this effect are sometimes regarded as being weapons based on neuroscience, since they manipulate the central nervous system, even if the mechanisms involved are not chemically based. See, for example, Royal Society, *Neuroscience, Conflict, and Security*, Royal Society, London, UK, February 2012.

3.4.2 Possible Applications

Nonlethal weapons are intended to provide their users with options in addition to lethal force. Proponents of such weapons suggest that they may be useful in a variety of military engagements or situations that are “less than war,” such as in peacekeeping and humanitarian involvements, in situations in which it is hard to separate combatants and noncombatants, or in civilian and military law enforcement contexts such as riot control or the management of violent criminals. In such situations, the use of lethal force is discouraged—and so new nonlethal weapons (such as tasers) have tended to substitute for older nonlethal weapons (such as billy clubs).

A key question concerning nonlethal weapons in combat is their relationship to traditional weapons—are nonlethal weapons intended to be used instead of traditional weapons or in addition to traditional weapons? For example, an acoustic weapon can be used to drive troops or irregular forces from an area or to dissuade a small boat from approaching a ship. But it can also be used to flush adversaries out from under cover, where they could be more easily targeted and killed with conventional weapons. The latter uses are explicitly permitted by NATO doctrine on nonlethal weapons:

Non-lethal weapons may be used in conjunction with lethal weapon systems to enhance the latter’s effectiveness and efficiency across the full spectrum of military operations.³³

So it is clear that in at least some military contexts, military doctrine anticipates that nonlethal weapons can be used along with traditional weapons. But it is also clear that they are not always intended to be used in this way.

Another issue is whether the availability of nonlethal weapons in addition to traditional weapons creates an obligation to use them before one uses traditional weapons that are (by definition) more lethal. On this point, NATO doctrine is also explicit:

Neither the existence, the presence, nor the potential effect of non-lethal weapons shall constitute an obligation to use non-lethal weapons, or impose a higher standard for, or additional restrictions on, the use of lethal force. In all cases NATO forces shall retain the option for immediate use

³³Science and Technology Organization Collaboration and Support Office, Annex B: NATO Policy on Non-Lethal Weapons, available at <http://ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-SAS-040//TR-SAS-040-ANN-B.pdf>.

of lethal weapons consistent with applicable national and international law and approved Rules of Engagement.³⁴

3.4.3 Ethical, Legal, and Societal Questions and Implications

The diversity of nonlethal weapons types and of possible contexts of use complicate ethical analysis.

Controversy over Terminology

As suggested in the introduction to this section, the term “nonlethal weapon” is arguably misleading, because such weapons can indeed be used with lethal effects. The public policy debate over such weapons is thus clouded, because many of the issues that do arise in fact would not emerge were such weapons always capable of operating in a nonlethal manner.

For example, how and to what extent, if any, should the intended targets of such weapons be taken into account in determining whether a weapon is “nonlethal”? The physical characteristics of the intended target must be relevant in some ways, but this requirement cannot mean that a machine gun aimed at an inanimate object should be categorized as a nonlethal weapon.

Are cyber weapons nonlethal? Yes, to the extent that they do not cause damage to artifacts and systems connected to their primary targets. But many cyber weapons are also intended to have effects on systems that they control, and malfunctions in those systems may well affect humans. Are antisatellite weapons nonlethal? Yes, since most satellites are unmanned. But if fired against a crewed military spacecraft, they become lethal weapons. Are chemical incapacitants nonlethal? Yes (for the most part), when they are used in clinically controlled settings. But the Scientific Advisory Board of the Organization for the Prohibition of Chemical Weapons concluded in 2011 that, given the uncontrolled settings in which such agents are actually used, “the term ‘non-lethal’ is inappropriate when referring to chemicals intended for use as incapacitants.”³⁵

³⁴ Science and Technology Organization Collaboration and Support Office, Annex B: NATO Policy on Non-Lethal Weapons, available at <http://ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-SAS-040///TR-SAS-040-ANN-B.pdf>.

³⁵ Scientific Advisory Board, Report of the Scientific Advisory Board on Developments in Science and Technology for the Third Special Session of the Conference of the States Parties to Review the Operation of the Chemical Weapons Convention, October 29, 2012, available at http://www.opcw.org/index.php?eID=dam_frontend_push&docID=15865.

Impact on Existing Arms Control Agreements

Certain nonlethal weapons raise concerns about eroding existing constraints associated with existing arms control agreements. One good example of such nonlethal weapons is that of biological or chemical agents that are intended to affect humans. The Biological and Toxin Weapons Convention forbids signatories from developing, producing, stockpiling, or otherwise acquiring or retaining biological agents or toxins “of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes” and also “weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict.”³⁶

Similarly, the Chemical Weapons Convention (CWC) forbids parties to the treaty from developing, producing, otherwise acquiring, stockpiling, or retaining chemical weapons.³⁷ Chemical weapons are in turn defined as “toxic chemicals and their precursors,” except when they are intended for permissible purposes and acquired in the types and quantities consistent with the permissible purposes. A toxic chemical is one that through its chemical action on life processes can cause death, temporary incapacitation, or permanent harm to humans or animals. (Thus, incapacitating agents are included in the definition of “toxic chemicals” and the use of incapacitating agents is forbidden as a means and method of war.) Permissible purposes include “industrial, agricultural, research, medical, pharmaceutical or other peaceful purposes”; protective purposes (that is, purposes “directly related to protection against toxic chemicals and to protection against chemical weapons”; and law enforcement, including domestic riot control purposes. Signatories also agree not to use riot control agents as a means of warfare, where a riot control agent is an agent that “can produce rapidly in humans sensory irritation or disabling physical effects which disappear within a short time following termination of exposure.”

Many issues regarding arms control turn on the specific meaning of terms such as “temporary incapacitation,” “other harm,” and “sensory irritation or disabling physical effects.” In addition, they depend on determinations of the intended purpose for a given agent (there is no agreed definition of “law enforcement,” for example).

Such definitional concerns have been particularly apparent in contemplating possible chemical weapons based on neuroscience (see the Chapter 2 section on neuroscience) that could create specific temporary effects in humans. Although there is a broad consensus that the CWC

³⁶ See <http://www.un.org/disarmament/WMD/Bio/>.

³⁷ See <http://www.opcw.org/chemical-weapons-convention/>.

prohibitions on using toxic chemicals in conflict extend to the use of incapacitating chemical agents (ICAs) in genuine combat situations, a number of countries, including the United States and Russia, have shown an active interest in ICAs for law enforcement and in situations such as counterterrorism where the lines between combat and law enforcement may blur. For example, even after the signing of the CWC, research has been proposed to develop “calmatives”—chemical agents that, when administered to humans, change their emotional states from angry to calm (as one possibility);³⁸ such agents might be useful in reducing the damage that a rioting crowd might cause or in sapping the will of adversary soldiers to fight on the battlefield.

The first two CWC review conferences were unable to address the issue of ICAs. Although substantial discussion and debate during the third review conference in April 2013 clarified a number of national positions, a Swiss proposal to undertake formal technical discussions was not included in the final document. At the first meeting of the Organization for the Prohibition of Chemical Weapons (OPCW) executive council following the review conference, the U.S. ambassador stated:

. . . we too are disappointed that time ran out before final agreement could be reached on language relating to substances termed “incapacitating chemical agents”. The United States believes that agreement on language is within reach. We will work closely and intensively with the Swiss and other delegations so that this important discussion can continue. In this context, I also wish very clearly and directly to reconfirm that the United States is not developing, producing, stockpiling, or using incapacitating chemical agents.³⁹

Beyond the debates over whether ICAs would be permitted in law enforcement, there is also concern that the use of such agents will undermine the fundamental prohibitions of the treaty. To the extent that some

³⁸ For example, the International and Operational Law Division of the Deputy Assistant Judge Advocate General of the Navy approved in the late 1990s a list of proposed new, advanced, or emerging technologies that may lead developments of interest to the U.S. nonlethal weapons effort, including gastrointestinal convulsives, calmative agents, aqueous foam, malodorous agents, oleoresin capsicum (OC) cayenne pepper spray, smokes and fogs, and riot control agents (orthochlorobenzylidene malononitrile, also known as CS, and chloracetophenone, also known as CN). See, for example, Margaret-Anne Coppernoll, “The Nonlethal Weapons Debate,” *Naval War College Review* 52:112-131, Spring 1999. In 2004, a Defense Science Board study on future strategic strike forces (available at <http://www.fas.org/irp/agency/dod/dsb/fssf.pdf>) noted that calmatives could have value in neutralizing individuals while minimizing undesirable effects.

³⁹ Robert Mikulak, Statement by Ambassador Robert P. Mikulak, United States Delegation to the OPCW at the Seventy-Second Session of the Executive Council, OPCW EC-72/NAT.8, available at http://www.opcw.org/index.php?eID=dam_frontend_push&docID=16511.

ICAs also fall under the provisions of the Biological Weapons Convention (BWC), the same concerns apply.

The pressures placed on the CWC and the BWC by the possibility of developing chemically or biologically based incapacitating agents may point to a broader lesson. Arms control agreements are often signed in a particular technological context. Changes in that context, whether driven by new S&T developments or new concepts of use for existing technologies, mean that in order to remain effective treaties must strive to stay on top of relevant advances. In extreme cases, even changes in the basic language of the treaty or abrogation or creation of new legal mechanisms might become necessary in response.⁴⁰ This lesson suggests that even research on certain new technology developments may have ELSI implications for existing agreements long before such research bears fruit.

International Law

The BWC and the CWC are not the only legal frameworks that affect the potential development and use of nonlethal weapons. The law of armed conflict (specifically, Article 51 of Additional Protocol I to the Geneva Conventions) stipulates that civilians shall not be the subjects of attack. This is a key element of the principle of distinction, which distinguishes between members of a nation's armed forces engaged in conflict and civilians, who are presumed not to participate in hostilities directly and thus should be protected from the dangers of military operations.⁴¹ Although civilians (that is, noncombatants) have always contributed to the general war effort of parties engaged in armed conflicts (e.g., helped produce weapons and munitions), they have usually been at some distance from actual ground combat. Since the end of World War II and the

⁴⁰ Because science and technology are at the core of both treaties, both the CWC and the BWC call for regular review of developments in science and technology that could affect the future of conventions, both during the review conferences held every 5 years and in between (see National Research Council, *Life Sciences and Related Fields: Trends Relevant to the Biological Weapons Convention*, The National Academies Press, Washington, D.C., 2012). In 2012, for example, the Organization for the Prohibition of Chemical Weapons created a temporary working group on convergence to address the increasing overlap between chemistry and biology and how that affects the future of the CWC and the BWC. Members included a member of the staff of the BWC Implementation Support Unit and the chair of a major independent international review of trends in S&T for the seventh BWC review conference (see <http://www.opcw.org/about-opcw/subsidiary-bodies/scientific-advisory-board/documents/reports/>).

⁴¹ Nils Melzer, "Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law," International Committee of the Red Cross, Geneva, Switzerland, 2009, available at <http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf>.

increase in civil wars over traditional interstate conflict and then the rise of nonstate actors, the assumption of separation has been increasingly challenged, and combatants and noncombatants are often intermingled.

The fact of intermingling is one rationale for the development of nonlethal weapons—the use of these weapons when combatants and noncombatants are intermingled is intended to reduce the risk of incurring noncombatant casualties. A common use scenario is one in which a soldier confronting such a situation is unable to distinguish between a combatant and a noncombatant, and uses a nonlethal weapon to subdue an individual. The rationale for nonlethal weapons is thus that if the individual turns out to be a noncombatant, then no harm is done, but if the individual turns out to be a combatant, then he has been subdued.

In this case, the argument turns on the meaning of the term “attack,” which is defined as an act of violence. For “nonlethal” weapons other than those covered by the CWC and BWC, is it an act of violence to use a weapon that causes unconsciousness? And if the answer is not categorical (that is, “it depends”), what are the circumstances on which the answer depends?

A second requirement of the law of armed conflict is a prohibition on weapons that are “calculated to cause unnecessary suffering.”⁴² In the 1980s and 1990s, a question arose over whether a weapon intended to blind but not kill enemy soldiers—by definition, a nonlethal weapon—might be such a weapon.

Box 3.3 recounts briefly some of the history of blinding lasers. At a high level of abstraction, lessons from this history suggest an interplay of ethical and legal issues. No specific international prohibitions against blinding lasers were in place in the early 1980s, and the United States sought to develop such weapons. However, over time, ethical concerns suggesting that blinding as a method of warfare was in fact particularly inhumane were one factor that led the United States to see value in explicitly supporting such a ban, first as a matter of policy and then as a matter of international law and treaty, even if blinding lasers themselves could arguably have been covered under the prohibition of weapons that caused unnecessary suffering.

Another distinct body of law, discussed further in Chapter 4, is international human rights law, which addresses the relationship between a state and its citizens rather than relationships between states in conflict addressed by the law of armed conflict. Many analysts, but by no means all, believe that international human rights law and international

⁴² Annex to Hague Convention IV Respecting the Laws and Customs of War on Land of October 18, 1907 (36 Stat. 2277; TS 539; 1 Bevans 631), article 23(e). Notably, neither the annex nor the convention specifies a definition for “unnecessary suffering.”

humanitarian law (that is, the law of armed conflict) are closely related, however.⁴³ International human rights law is codified in a number of general treaties as well as international agreements focused on particular issues.

Among the provisions of international human rights law that could be relevant to nonlethal weapons are prohibitions on torture or on degrading or inhumane punishments. More general provisions, such as a fundamental right to life or to health, are also potentially relevant. Potential violations of international human rights law have been cited as part of the arguments against the use of incapacitating chemical agents,⁴⁴ as well as against other forms of nonlethal weapons.

Safety

The extent to which a given weapon is nonlethal (or more precisely, less lethal) is often an empirical question. How might such weapons be tested for lower lethality? Animal testing and modeling do provide some insight, but high fidelity is sometimes available only through human testing. Laboratory testing conditions often do not reflect real-world conditions of use. In practice, then, certain information on lethality may be available only from operational experience—a point suggesting that the first uses of a given nonlethal weapon may in fact be more lethal than expected.

In the cases of the nonlethal weapons described above:

- Weapons that provide high-voltage shocks to an individual may cause serious injury or death if the person falls or if the person's heart goes into cardiac arrest.
- Dazzling lasers may cause a driver to lose control of a vehicle by

⁴³ See, for example, Robert Kolb, "The Relationship Between International Humanitarian Law and Human Rights Law: A Brief History of the 1948 Universal Declaration of Human Rights and the 1949 Geneva Conventions," *International Review of the Red Cross*, No. 324, September 30, 1998, available at <http://www.icrc.org/eng/resources/documents/misc/57jpg2.htm>; Marco Sassoli and Laura Olson, "The Relationship Between International Humanitarian and Human Rights Law Where it Matters: Admissible Killing and Internment of Fighters in Non-International Armed Conflicts," *International Review of the Red Cross* 90(871):599-627, September 2008, available at <http://www.icrc.org/eng/assets/files/other/irrc-871-sassoli-olson.pdf>; and United Nations Office of the High Commissioner on Human Rights, "International Humanitarian Law and Human Rights," July 1991, available at <http://www.ohchr.org/Documents/Publications/FactSheet13en.pdf>.

⁴⁴ International Committee of the Red Cross, "Incapacitating Chemical Agents": *Law Enforcement, Human Rights Law, and Policy Perspectives*, report of an expert meeting, Montreux, Switzerland, April 24-26, 2012, available at <http://www.icrc.org/eng/resources/documents/publication/p4121.htm>.

Box 3.3 On the Compliance of Lasers as Antipersonnel Weapons with the Law of Armed Conflict

In 1983, the *New York Times* reported that the U.S. Army was developing a weapon known as C-CLAW (Close Combat Laser Assault Weapon) that used low-power laser beams to blind the human eye at distances of up to one mile.¹ Pentagon officials noted that the beam “would sweep around the battlefield and blind anyone who looked directly into it.”

In September 1988, the DOD Judge Advocate General issued a memorandum of law concerning the legality of the use of lasers as antipersonnel weapons.² This memorandum identified the key law-of-armed-conflict issue as whether the use of a laser to blind an enemy soldier would cause unnecessary suffering and therefore be unlawful. The memorandum noted that blinding a soldier “ancillary to the lawful use of a laser rangefinder or target acquisition lasers against material targets” would be legal. If so, the memorandum argued, consistency requires that it must not be illegal to target soldiers directly with a laser. If it were otherwise, “enemy soldiers riding on the outside of a tank lawfully could be blinded as the tank is lased incidental to its attack by antitank munitions; yet it would be regarded as illegal to utilize a laser against an individual soldier walking ten meters away from the tank.” The memorandum then noted that “no case exists in the law of war whereby a weapon lawfully may injure or kill a combatant, yet be unlawful when used in closely-related circumstances involving other combatants.” The memorandum then concluded that a blinding laser would not cause “unnecessary suffering when compared to other [legal] wounding mechanisms to which a soldier might be exposed on the modern battlefield,” and that thus the use of a laser as an antipersonnel weapon must be lawful.

However, in September 1995, the U.S. Department of Defense promulgated a new policy that prohibited “the use of lasers specifically designed to cause permanent blindness of unenhanced vision and supported negotiations prohibiting the use of such weapons” and continued training and doctrinal efforts to minimize accidental or incidental battlefield eye injuries resulting from using laser systems for nonprohibited purposes. One month later, the first review conference of the 1980 Convention on Certain Conventional Weapons adopted a protocol on blinding laser weapons, which the United States signed. Some of the issues raised in

forcing the driver to shield his or her eyes, leading to injury or death as a result.

- Acoustic weapons can cause permanent hearing losses through repeated exposure.
- Chemical incapacitants can cause serious harm, or death may occur if overdoses occur or as the result of secondary effects (e.g., an incapacitated person who falls and hits his head on a rock).

the lead-up to this conference included the desirability of a protocol to cover this issue; a debate over whether to prohibit blinding weapons per se or blinding as a method of warfare; and the possibility of a ban interfering with other military uses of lasers, such as the designation of targets.

In January 2009, the United States deposited its instrument of ratification for Protocol IV of the Convention on Conventional Weapons, which prohibits the employment of laser weapons “specifically designed, as their sole combat function or as one of their combat functions, to cause permanent blindness to unenhanced vision.”³ The protocol further prohibits the transfer of such weapons to any state or nonstate entity. However, it recognizes the possibility of blinding as “an incidental or collateral effect of the legitimate military employment of laser systems, including laser systems used against optical equipment,” and exempts such blinding from the prohibition of this protocol.

One analyst suggests that a major factor in the adoption of the protocol was the support garnered from a variety of nongovernment organizations, such as medical associations and national Red Cross and Red Crescent organizations.⁴ In addition, in May 1995, the European Parliament called on the Council of Europe to take action on the protocol. In the United States, Human Rights Watch (HRW)—an international nongovernmental organization—issued a report in May 1995 that documented U.S. efforts to develop military laser systems that were intended to damage optical systems and/or eyesight. Whether or not prompted by the HRW report, a number of influential U.S. senators and representatives shortly thereafter asked the administration to adopt a ban on blinding lasers.

¹ See <http://www.nytimes.com/1983/12/18/us/army-works-on-a-blinding-laser.html>.

² “Memorandum of Law: The Use of Lasers as Antipersonnel Weapons,” *The Army Lawyer*, DA PAM 27-50-191, November 1988, available at http://www.loc.gov/rr/frd/Military_Law/pdf/11-1988.pdf.

³ See <http://www.state.gov/r/pa/prs/ps/2009/01/115309.htm>.

⁴ Louise Doswald-Beck, “New Protocol on Blinding Laser Weapons,” *International Review of the Red Cross*, No. 312, June 30, 1996, available at <http://www.icrc.org/eng/resources/documents/misc/57jn4y.htm>. This article also provides some of the other information contained in this box.

Unanticipated Uses

Nonlethal weapons—at least some of them—raise issues that are not generally anticipated in the doctrines of their use. For example, although nonlethal weapons are often presented as a substitute for lethal weapons, they may in practice be a substitute for nonviolent negotiations—that is, they may be used to bypass the time-consuming process of negotiations.

Indeed, there are instances in which nonlethal weapons have been used when no force (rather than lethal force) would have been used.⁴⁵

Building on this possibility, nonlethal weapons could be used as a means for coercion—that is, they might be used to torture an individual or persuade an otherwise unwilling individual to cooperate. The nonlethality of some nonlethal weapons is premised on the ability of an individual to flee the scene of weapons use (as is true for nonlethal area-denial systems)—the weapon causes pain for an individual who is exposed to the weapon's effects, but the individual is free to leave the area in which the weapon causes these effects. But if the individual is *not* free to leave (e.g., by being restrained), an area-denial system could plausibly be used as an instrument of torture.

It is of course true that virtually any instrument can be used as an instrument of torture, which is prohibited under international law. In this context, a possible ELSI concern arises because certain nonlethal weapons technologies might be better suited for torture (if, for example, the use of a particular technology left no physical evidence of the torture).

⁴⁵ In one study performed by the sheriff's office in Orange County, Florida, officers on patrol were equipped with tasers and were trained to use them. One immediate effect was that the number of citizen fatalities due to police action decreased significantly—the intended effect. A second immediate (and unanticipated) effect was a significant increase in the frequency of police use of force overall. That is, without tasers, there were most likely a number of situations in which the police would not have used force at all, but with tasers available, they were more willing to use force (nonlethal force, but force just the same) than before. See Alex Berenson, 2004, "As Police Use of Tasers Soars, Questions Over Safety Emerge," *New York Times*, July 18, 2004.

4

Sources of ELSI Insight

This chapter discusses sources of ELSI insight that might be relevant to considering the ethics of R&D on emerging and readily available (ERA) technologies in a military context. These sources include generalizable lessons arising from consideration of the science and technologies described in Chapters 2 and 3; philosophical ethics and existing disciplinary approaches to ethics; international law; social sciences such as anthropology and psychology; scientific and technological framing; the precautionary principle and cost-benefit analysis; and risk communication. The final section describes how these sources of insight might be used in practice. Also provided in this chapter is some background necessary for understanding the different kinds of ethical, legal, and societal issues that arise in Chapter 5.

A note on terminology: throughout this report, the terms “cost” and “benefit” are used in their broadest senses—all negative and positive impacts, whether financial or not.

4.1 INSIGHTS FROM SYNTHESIZING ACROSS EMERGING AND READILY AVAILABLE TECHNOLOGIES

Applications of most of the technologies described in Chapters 2 and 3 raise ethical, legal, and societal issues. Some of these issues are new; others put pressure on existing ELSI understandings and accommodations that have been reached with respect to more traditional military technologies. As a historical matter, such understandings have generally

been reached through a process in which society has addressed the ELSI implications of a new application or technology because its emergence has forced society to do so. Only rarely have ELSI implications been addressed prior to that point.

Because new technologies provide new capabilities and also allow old activities to be performed in new ways, situations can arise in which existing policy does not provide adequate guidance—giving rise to what Moor has characterized as a policy vacuum.¹ But in practice, the vacuum involves more than policy—such situations also challenge existing laws, ethical understandings, and societal conventions that may have previously guided decision making when “old” technologies were involved. In a military context, it may be the existence of real-world hostilities that pushes policy makers to fill the policy vacuum.

Developing new ELSI understandings and accommodations is a fraught and complex process. For example, the technical implications of a new application may not be entirely clear when it first emerges. The intellectual concepts underpinning existing understandings may have ambiguities that become apparent only when applied to situations involving the new applications. An analogy used to extend previous understandings to the new situation may be incomplete, or even contradict the implications of other analogies that are used for the same purpose. As a practical matter also, new situations provide antagonists with the opportunity to reopen old battles over ethical, legal, and societal issues, thus potentially upending previously reached compromises on controversial issues.

In some cases, an R&D activity may be inherently suspect from an ELSI perspective. For example, advances in genetic engineering may someday enable the development of pharmaceutical agents that can act more effectively on individuals from certain ethnic groups. Although such agents might afford significant therapeutic benefit to members of those ethnic groups, the underlying science might also be used by a rogue state to harm those groups.² Thus, R&D aimed at developing agents that have differential effects on various ethnic groups, whether or not intended for use in conflict, immediately raise a host of ELSI concerns.

In other cases, an application’s concept of operation is a central element in an ELSI analysis of that application. In general, an application of a given technology is accompanied by a concept of operation that articu-

¹ James H. Moor, “Why We Need Better Ethics for Emerging Technologies,” *Ethics and Information Technology* 7:111-119, 2005.

² The possibility that such weapons might be used was introduced in the professional military literature as early as 1970. See Carl Larson, “Ethnic Weapons,” *Military Review* 50(11):3-11, 1970.

lates in general terms how the application is expected to be used, and it may be an application's concept of operation rather than the application itself that raises ethical, legal, and societal issues. A system with lethal capabilities may have "selectable" modes of operation: fully autonomous operation of its lethal capabilities; human-controlled operation of its lethal capabilities; and target identification only. A concept of operations for the fully autonomous mode that does not adequately specify the circumstances under which it may be activated may well be suspect from an ELSI perspective.

An application's practical value helps to shape developing new ELSI understandings and accommodations. If an application turns out to have a great deal of practical or operational value, an ELSI justification may emerge after that value has been established. Similarly, if an application has little operational value, ELSI-based objections will seem more powerful, and may become part of the narrative against that application.

For example, the emergence of new weapons technologies often sparks a predictable ethical debate. Regardless of the actual nature of the weapon, some will argue that a new weapon is ethically and legally abhorrent and should be prohibited by law, whereas others will point to the operational advantages that it confers and the ethical responsibility and obligation to provide U.S. armed forces with every possible advantage on the battlefield. Sometimes this ethical debate ends in a consensus that certain weapons should not be used (e.g., weapons for chemical warfare). In other cases, existing ELSI understandings are eroded, undermined, or ignored (as was the case with the London Naval Treaty of 1930, which outlawed unrestricted submarine warfare but subsequently was abandoned for all practical purposes). But the point is that operational value has often made a difference in the outcome of an ELSI analysis.

The above points are relevant especially in an environment of accumulating incremental change and improvement. Ethical, legal, and societal issues often become prominent when a new technology offers a great deal more operational capability than previous ones. But as a technology is incrementally improved over many years and becomes much more capable than it was originally, the capabilities afforded by the improved technology may render the originally developed ELSI understandings obsolete, moot, or irrelevant.

Perhaps the most important point to be derived from synthesizing across technologies is that technology-related ELSI debates are ongoing. One should expect such debates as technology evolves, as applications evolve, as threat/response tradeoffs change (e.g., nation-state warfare, guerrilla warfare, terrorist warfare, cyber warfare), and as societal perceptions and analysis change. In some cases, new ELSI debates will emerge. In other cases, the ELSI debates will be familiar, even if they are newly

cast in terms of the relevant change at hand. And in still other cases, the ELSI debates will sound familiar right down to the literal words being used, simply because a proponent of a particular ELSI perspective sees an opportunity to (re-)present his or her point of view.

4.2 ETHICS

4.2.1 Philosophical Ethics

Classically, Western moral philosophers have advanced two general kinds of moral theories that have proven useful in analyzing moral problems. One kind of theory, consequentialism (or equivalently, utilitarianism), looks at the consequences of actions and asks, for example, which actions will provide the greatest net good for the greatest number of people when both harms and benefits are taken into account. Thus, an action is judged to be right or wrong given its actual consequences. Consequentialism allows the ranking of different actions depending on the outcomes of performing them.

A second kind of theory, deontological ethics, judges the morality of actions in terms of compliance with duties, rights, and justice. Examples are following the Ten Commandments or obeying the regulations spelled out in a professional code of ethics. The morality of killing or lying would be decided based on the nature of the act and not on its results or on who the actor is. That is, the act of killing an innocent person, for instance, would under some versions of deontological ethics be categorically wrong in every circumstance. Other versions of deontological ethics allow for some ranking of conflicting duties and therefore are less categorical.

In many cases, persons acting on the basis of any of these theories would view the rightness or wrongness of any given action similarly. In other cases, they might well disagree, and philosophers have argued extensively and in many academic treatises about the differences that may arise. In practice, however, few people act for purely deontological or purely utilitarian reasons, and indeed many ethical controversies reflect the tensions among these theories. For example, Party *A* will argue for not doing *X* because *X* is a wrong act that cannot be justified under any circumstances, whereas Party *B* will argue for doing *X* because on balance, doing *X* results in a greater good than not doing *X*.

Sometimes these different approaches work nicely together in generating a more ethical outcome. Consequentialist ethics allow for managing a complex ethical situation to mitigate its negative effects. In some cases, the rapid pace of a program may give rise to concerns that certain stakeholders will not have a fair chance for input into a decision-making process (a deontological ethical concern). Slowing the program or build-

ing in certain checkpoints may address some of these concerns. In such cases, the issue may not be so much whether or not to do something, but rather when it should be done.

A third perspective on philosophical ethics is called virtue ethics—this perspective emphasizes good personal character as most basic to morality. People build character by adopting habits that lead to moral outcomes. Good character includes being trustworthy, helpful, courteous, kind, and so on. Under this theory, a scientist with good character will not fabricate data or exaggerate outcomes in her published research. In a military context, an example of virtue ethics is the set of core values articulated by the U.S. Army for soldiers: loyalty, duty, respect, selfless service, honor, integrity, and personal courage.³ Actions or behavior that compromise one or more of these values are to be avoided.

Perhaps related to virtue ethics is the body of moral beliefs found in specific religions that often prescribe what should count as “good” and what individuals should, or should not, do. Specific notions such as what is humane or evil; what constitutes human nature; compassion; peace; stewardship; and stories of creation are often closely linked to religious worldviews. The discussion of the laws of war below notes that the major religions of the world are not silent on questions related to war and peace, civilian and military involvement in conflict, and so on, and further that there are some commonalities to the philosophical approaches taken by those religions. But answers to questions involving such concepts may well vary according to the specific religions in question, and a serious examination of the ethics involving conflict or technologies to be used in conflict may require a detailed look at those religions. A detailed examination of what various religions say about such matters is beyond the scope of this report, and thus apart from acknowledging that religion plays an important role in the formulation of answers, the role of any specific religion is not addressed in this report.

Some relevant questions derived from philosophical ethics include the following:

- On what basis can the benefits and costs of any given research effort be determined and weighed against each other, taking into account both the research itself and its foreseeable uses?
- What categorical principles might be violated by a research effort, again taking into account both the research itself and its foreseeable uses?
- How and to what extent, if any, might a research effort and its fore-

³ See, for example, http://www.history.army.mil/lc/the%20mission/the_seven_army_values.htm.

seeable uses compromise the character and basic values of researchers or military users?

- How and to what extent, if any, does a research effort implicate shared ethical or moral concerns of major religious traditions?

4.2.2 Disciplinary Approaches to Ethics

Just as specialization in general areas of science and engineering has become necessary and commonplace, the same is true for ethics. The sources of modern-day ethics continue to evolve, and ethical perspectives are dynamic. For example, new theoretical orientations coming from communitarian ethics raise and address issues for which the moral theories described above are not seen to provide sufficient guidance.⁴ New subfields of ethics, specializing in practical and professional ethics, are now commonplace and address the issues and problems relevant to a particular area. Included among these subfields are biomedical ethics, engineering ethics, and information technology ethics, among others.

All of these specializations are concerned with examining and assisting in the particularities of moral analysis and decision making that arise in those domains, and sometimes between domains.

Biomedical Ethics

The field of biomedical ethics (bioethics) has developed over several decades and encompasses medical ethics, research ethics, and concerns over the implications of biomedical research. The field is interdisciplinary, and thus its approach to ethics incorporates work from law, medicine, philosophy, theology, and social science. In addition, the field's boundaries are indistinct and often overlap into medical ethics, research ethics, law, public policy, and philosophy. The field initially focused on the ethics of research with human subjects, but numerous key events in medicine and biomedical research have led to the development of the field's basic principles.

The initial discussion on the ethics of human subjects research resulted in one of the primary standards of bioethics: informed consent. In 1947, the Nuremberg Trial of Nazi doctors spurred legal discussions of consent and examinations of medical codes of ethics. Although this ruling relied on a standard of informed voluntary consent, it had little initial direct

⁴ See <http://plato.stanford.edu/entries/communitarianism/>.

impact on U.S. medical ethics.⁵ The subsequent 1964 Declaration of Helsinki from the World Medical Association brought the issue of achieving informed consent in medical research to the attention of the U.S. medical community, and the declaration was incorporated into the professional codes of U.S. physicians.⁶ The difficulties with achieving and establishing standards for informed consent have been a consistent focus of bioethics. With the discovery of cases of human subjects' abuses throughout the 1960s and 1970s, the field was pushed to hold stricter standards for both informing patients and research subjects and also for ensuring voluntary consent.

Henry Beecher's 1966 article in the *New England Journal of Medicine*,⁷ in which he described numerous ethical abuses of patients by physicians and researchers, drew attention to the physicians' behavior and raised concerns about physician authority. Specific cases, some identified by Beecher, focused attention on the issue of getting informed consent in medical research and also on the conflict of interest between advancing medical knowledge and not harming patients. These cases included the following:

- *The Fernald School experiments.* Mentally disabled children were fed radioactive calcium in their meals to learn about the absorption of calcium.
- *The Jewish Chronic Disease Hospital.* Terminally ill patients were injected with live cancer cells to learn about human ability to reject foreign cells.
- *The Willowbrook State School.* Children in the state school were deliberately given hepatitis in order to learn more about the virus and control the spread of the disease in the hospital.
- *The Tuskegee Syphilis Study.* African American men with syphilis were followed for over 40 years and denied treatment (penicillin) once it was available in order to learn about the disease progression.

⁵ Jay Katz, "The Consent Principle of the Nuremberg Code: Its Significance Then and Now," *The Nazi Doctors and the Nuremberg Code: Human Rights in Human Experimentation*, George J. Annas and Michael A. Grodin, eds., Oxford University Press, New York, 1992.

⁶ Susan E. Lederer, "Research Without Borders: The Origins of the Declaration of Helsinki," pp. 199-217 in *Twentieth Century Ethics of Human Subjects Research: Historical Perspectives on Values, Practices, and Regulations*, Volker Roelcke and Giovanni Maio, eds., Franz Steiner Verlag, Stuttgart, 2004; Jonathan D. Moreno and Susan E. Lederer, "Revising the History of Cold War Research Ethics," *Kennedy Institute of Ethics Journal* 6(3):223-237, 1996.

⁷ H.K. Beecher, "Ethics and Clinical Research," *New England Journal of Medicine* 274(24):1354-1360, June 16, 1966, available at [http://whqlibdoc.who.int/bulletin/2001/issue4/79\(4\)365-372.pdf](http://whqlibdoc.who.int/bulletin/2001/issue4/79(4)365-372.pdf).

These cases all involved issues with the informed consent process, including the lack of information given and how voluntary the consent was.

The field of bioethics also developed principles around medical care, which have their roots in medical ethics and the physician-patient relationship. David J. Rothman has argued that the issues of informed consent and the resulting push for regulation in human experimentation overflowed into medical care during the 1960s.⁸ Whatever the cause, during the 1960s the physician-patient relationship was reconsidered and physician authority in making medical decisions was questioned. The results were calls for patient autonomy and an emphasis on physicians' truthfully informing patients of their condition, rather than paternalistically shielding patients from the realities of their illnesses. These changes in norms emphasized personal autonomy and truth-telling, and were spurred by various developments in medical technology and experimental medical treatments.⁹ Organ transplantation and heart-lung machines raised questions about when death occurred and about patients' rights to request withdrawal of care or deny treatment. Kidney dialysis and organ transplantation raised questions about the just allocation of limited resources, specifically asking if physicians should be the only ones making these decisions and how the decisions should be made.

The field of bioethics includes consideration of the impacts of scientific and technological developments on social morality. During the field's development, research and advances in genetics and in vitro fertilization drove the field to think about the effects they have on society and its norms. A growing number of tests for genetic diseases raised issues of personal autonomy, genetic privacy, and claims of practicing eugenics. The development of in vitro fertilization in the 1970s and 1980s raised questions, for the first time, argued Alta Charo, about what was right and wrong regarding the manipulation of human embryos and about how to define personhood.¹⁰

In 1979, the first federal bioethics commission, the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, formalized the principles of bioethics articulated in the Belmont report (Box 4.1). The commission was charged with focusing on the ethics of research on or involving human subjects; however, the moral principles it outlined have been applied, augmented, and adapted by a number of

⁸ David J. Rothman, *Strangers at the Bedside: A History of How Law and Bioethics Transformed Medical Decision Making*, Basic Books, New York, 1991.

⁹ Alta Charo, "Prior ELSI Efforts—Biomedical/Engineering Ethics," presentation to the committee, August 31, 2011.

¹⁰ Alta Charo, "Prior ELSI Efforts—Biomedical/Engineering Ethics," presentation to the committee, August 31, 2011.

commentators and analysts not just to human subjects research but to all aspects of bioethics, including medical care, and to the impacts of biotechnology and life sciences research on society, and to other domains as well.¹¹

Since the Belmont report, the biomedical ethics field has explored and focused on how these principles apply to specific areas of medicine and research, including end-of-life care, genetics and biotechnology, health systems, global health, nanotechnology, stem cell research, assisted human reproduction, gene therapy, cloning, and health care policy. Notably, in 1988 when James Watson launched the National Institutes of Health's Human Genome Project (HGP), he also announced that 3 percent (later increased to 5 percent) of the funding would go to researching the ethical, legal, and societal issues associated with genetics, which is where the term "ELSI" originated. HGP-supported ELSI research focused the field of bioethics on the issues with genetics. In addition, the support for ELSI research also funded centers for bioethics across the country, which enabled the field to spread and resulted in more scholars and researchers being educated in bioethics or in becoming bioethicists. This NIH-supported genetics ELSI research continues today.

Questions of interest in biomedical ethics include the following:

- How do standards for achieving informed consent change with different populations? Do different stresses on volunteers or patients alter the ability to achieve informed consent?
- What kinds of inducements overwhelm voluntarism? What protections are necessary to maintain a person's voluntary choice in decision making?
- How should public good be weighed against risks to individuals?
- How should research populations be chosen to address issues of social justice while balancing the vulnerability of populations?
- What obligations for truth telling exist in research? Are there justi-

¹¹ See, for example, Amy Gutmann, "The Ethics of Synthetic Biology: Guiding Principles for Emerging Technologies," *The Hastings Center Report* 41(4):17-22, 2011, available at <http://www.upenn.edu/president/meet-president/ethics-synthetic-biology-guiding-principles-emerging-technologies>; David Koepsell, "On Genies and Bottles: Scientists' Moral Responsibility and Dangerous Technology R&D," *Science and Engineering Ethics* 16(1):119-133, 2010, available at <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2832882/>; David Koepsell, *Innovation and Nanotechnology: Converging Technologies and the End of Intellectual Property*, Bloomsbury Academic, New York, 2011; and U.S. Department of Homeland Security, "Applying Ethical Principles to Information and Communication Technology Research: A Companion to the Department of Homeland Security Menlo Report," GPO, January 3, 2012, available at <http://www.cyber.st.dhs.gov/wp-content/uploads/2012/01/MenloPrinciplesCOMPANION-20120103-r731.pdf>.

Box 4.1 Fundamental Principles of Biomedical Ethics

The Belmont report of 1979 articulated three principles to govern the conduct of biomedical research: respect for persons, beneficence, and justice.¹ In the discussion below, which is based on a discussion of biomedical ethics by Thomas L. Beauchamp and James L. Childress, a fourth principle is added: nonmaleficence.² From each of these principles are drawn obligations and rules for how to act.

- *Respect for autonomy.* Autonomy is defined as including two essential conditions: “(1) liberty (independence from controlling influences) and (2) agency (capacity for intentional action).”³ This principle holds that the autonomy of people should not be interfered with. Autonomy should be respected, preserved, and supported. In the case of health care and human subjects research, the principle obliges physicians and researchers to get informed consent, tell the truth, respect privacy, and only when asked help others to make important decisions. Discussions in biomedical ethics around how to abide by this principle often focus on a few areas: evaluating capacity for making autonomous choices, the meanings and justifications of informed consent, disclosing information, ensuring voluntariness, and defining standards for surrogate decision making.

- *Nonmaleficence.* This principle asserts “an obligation not to inflict harm on others.”⁴ It does not require that a specific action be taken, but rather that one intentionally *refrain* from taking action that will either cause harm or impose a risk of harm. The specific rules drawn from this principle include: do not kill, do not cause pain or suffering, do not incapacitate, do not cause offense, and do not deprive others of the goods of life.⁵ When applied to the health care and research experiences, the discussion over the implementation of this principle focuses on distinctions and rules for nontreatment, quality-of-life discussions, and justifications and questions regarding allowing patients to die or arranging deaths. This principle is most closely connected with the physicians’ code of ethics rule that they “do no harm.”

- *Beneficence.* Closely related to the principle of nonmaleficence, this principle is “a moral obligation to *act* for the benefit of others.”⁶ This includes two aspects:

fications for not telling the whole truth or leaving patients or volunteers in the dark?

- What impacts do conflicts of interest have on research results and participants’ involvement? How can conflicts of interest be resolved, or must they be avoided entirely?

- When and how do privacy issues and the collection of data negatively affect autonomy?

- How do cultural perspectives alter bioethics standards? How flexible should bioethics standards be in response to different cultures?

(1) positive beneficence, which requires one to take action to provide benefits, and (2) utility, which requires that one balance benefits and costs to ensure the best result. The more specific rules drawn from this principle include: protect and defend the rights of others, prevent harm from occurring, remove conditions that will cause harm, help persons with disabilities, and rescue persons in danger.⁷ In reference to human experimentation this principle obliges researchers and institutional review boards to weigh the risk to subjects and to ensure that the risk be minimal unless there is a direct benefit to the subject. In the case of medical care this principle obliges physicians to promote patient welfare.

- *Justice*. An obligation to treat people fairly, equitably, and appropriately in light of what is due or owed to them. This principle includes the concept of distributive justice, which refers to the just distribution of materials, social benefits (rights and responsibilities), and/or social burdens.⁸ Determinations of what is a morally justifiable distribution vary based on different philosophical theories; for instance, a utilitarian view emphasizes maximizing public good, whereas an egalitarian view emphasizes equal access to the goods. In the medical context this principle focuses on rules regarding access to decent minimal health care, such as emergency care, the allocation of health resources, and the rationing of and priority setting for resources and treatments. Regarding human experimentation, this principle is often used to ensure that vulnerable populations are not exposed to more risk than other populations.

¹ The Belmont report can be found at <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>.

² Thomas L. Beauchamp and James F. Childress, *Principles of Biomedical Ethics*, 5th Edition, Oxford University Press, New York, 2001.

³ *Ibid.*, p. 58.

⁴ *Ibid.*, p. 113.

⁵ *Ibid.*, p. 117.

⁶ *Ibid.*, p. 166.

⁷ *Ibid.*, p. 167.

⁸ *Ibid.*, p. 226.

Engineering Ethics

The academic field of engineering ethics developed in the United States in the early 1970s with other inquiry concerning issues of practical and professional ethics. Perhaps biomedical ethics was earliest to gain both scholarly and public interest; engineering and research ethics soon followed.

Controversies concerning engineering catastrophes and research misconduct are likely to have fueled public demands and professional response. Work in the field accelerated when ABET, the accrediting body for engineering and technology programs at colleges and universities,

initiated a requirement in 1985 that engineering students demonstrate understanding of ethics for the profession and practice. Current National Science Foundation (NSF) and NIH requirements for ethics mentoring of postdoctoral students and ethics education for graduate and undergraduate students have also stimulated activity.

Initially, research by philosophers, often with engineers as collaborators, focused on ethical problems from the perspective of individual engineers. Ethical theory can provide useful conceptual clarification of the ethical dimensions of possible action. In addition, codes of ethics and other guidance concerning human development and human rights, from professional societies and national and international bodies, provided other resources, as did laws and other regulations.

More recent research includes historians and social and behavioral scientists as well as science and technology studies scholars, and examines issues of complex systems and collective as well as individual responsibility. These issues involve the responsibilities of engineers in organizations and the collective responsibilities of engineering societies and the organizations and networks that employ engineers and that develop, promote, and regulate engineering innovations. They also involve issues of design and implementation and ask whether traditional theories and approaches in ethics must be revised, augmented, or cast aside in light of the difficulties that complexity creates for development and management.

An important resource for the field is case studies, which take numerous forms and have many uses. For example, the case descriptions, commentaries, and findings of the Board of Ethical Review of the National Society of Professional Engineers is a rich source of material for engineers faced with, and scholars wishing to examine, ethical problems. Cases can be hypothetical or historical, provide positive or negative role models, focus on everyday or rare and large-scale events, or emphasize individual or organizational actions. They can take a prospective or retrospective view—that of the agent or the judge. They can describe value conflicts or problems of drawing lines between what is permissible, unacceptable, recommended, or forbidden. The cases can be simplified to illustrate a particular concept (called thin description) or illustrate real-life messiness so as to demonstrate how people may legitimately arrive at different solutions. Finally, cases may illuminate a problem from the perspective of an individual engineer, or they may document and analyze an issue that can be resolved only at an organizational or societal level.

As noted above, the field of engineering has also begun to grapple with the implications of complexity for individual and organizational responsibility. Some scholars believe that the increasing complexities require new ethical theories, concepts, and approaches if they are to be resolved, whereas others hold that further elucidation of already extant

understandings can handle most such problems, while acknowledging that new policies and practices may be required. This is a bifurcation in views that seems common to considerations of ethics in a great many fields of science, engineering, and technology.

Some of the questions of interest in engineering ethics include the following:

- How can the domain of professional engineering responsibility be legitimately circumscribed? Are there ethical commonalities covering all engineering fields, or is different field-specific guidance needed?
- How can engineered systems identify and address issues of social and societal inequities? Who has responsibilities to do this; who shares these responsibilities?
- How should engineers participate in societal determinations about promoting innovation? Who should bear the costs and risk of failure? Are there ethically better and worse ways to distribute benefits? Who should decide?
- Recognizing both that R&D on some military technologies is necessary for the safety of the nation and that engineers have paramount responsibility for health, the environment, and safety, are there engineered systems that are too complex or dangerous to introduce in society?
- How should engineers and the engineering profession contribute to a future that is economically, environmentally, and socially sustainable?
- How, and to what extent if any, do engineering and engineering ethics translate across political, geographical, and generational boundaries?
- What are legitimate social expectations concerning the development and use of engineered systems and services, vis-à-vis feasible control and due care? Should ethical distinctions be made between deliberate and accidental misuse? How should legal, educational, and professional institutions address the limits of “good enough” engineering and problems of unintended uses and users?

Information Technology Ethics

Scholars have advanced a number of views on the nature of information technology ethics.¹² One view is that it is simply the application of traditional ethical theories (e.g., consequentialism, deontology) to problems associated with the use of information technology, some of which have manifestations even without information technology and others of

¹² Much of the discussion in this section is based on Terrell Bynum, “Computer and Information Ethics,” *Stanford Encyclopedia of Philosophy*, 2008, available at <http://plato.stanford.edu/entries/ethics-computer/>.

which come into existence because of information technology. A variant of this view is that the latter category (problems that exist because of information technology) is vanishingly small, and that for the most part what appear to be new ethical problems are really old problems with a different technological underpinning.

Others believe that information technology results in entirely new ethics problems that would not exist in the absence of such technology. For example, Walter Maner noted that ethical analysts are often unable to find a satisfactory noncomputer analogy to a problem arising with information technology—a fact that for Waner testified to the uniqueness of problems in information technology ethics. In this context, “lack of an effective analogy forces us to discover new moral values, formulate new moral principles, develop new policies, and find new ways to think about the issues presented to us.”¹³

Still others argue that information technology ethics is concerned with ethical problems that become apparent or manifest only when unprecedented IT applications emerge. These problems arise because IT provides new capabilities and thus new possibilities for action—and either there are no policies or guidance in place that address the new possibilities or existing policies and guidance are inadequate. (For example, hiding information deep inside a computer system’s file structure is no longer a viable method for protecting it, since search engines can find such information no matter where it is located as long as there is at least one path, however obscure, to it; thus, privacy policies based on hiding information in obscure locations are less viable than they once were.) IT ethics address what constitutes ethical behavior in new cases.

Last, some regard IT ethics as a subset of professional ethics—what are the ethical responsibilities of individual practitioners or researchers in the field of IT? For example, the ACM and IEEE-CS Software Engineering Code of Ethics and Professional Practice calls on software engineers to commit themselves to the health, safety, and welfare of the public through adherence to eight principles¹⁴—acting consistently with the public interest; acting in a manner that is in the best interests of their client and employer consistent with the public interest; ensuring that their products and related modifications meet the highest professional standards possible; maintaining integrity and independence in their professional judgment; subscribing to and promoting an ethical approach to the management of software development and maintenance; advancing the integrity and reputation of the profession consistent with the public interest; being

¹³ Walter Maner, “Unique Ethical Problems in Information Technology,” in Terrell Bynum and S. Rogerson, eds., *Science and Engineering Ethics* 2(2):137-154, 1996.

¹⁴ See <http://www.acm.org/about/se-code>.

fair to and supportive of their colleagues; and participating in lifelong learning regarding the practice of their profession and promoting an ethical approach to the practice of the profession.

Some of the topics considered under the rubric of information technology ethics or computer ethics include the following:¹⁵

- *Computers in the workplace*, e.g., what is an ethical policy for employee use of computers in the workplace?
- *Computer crime*, e.g., how does a crime committed with the use of a computer differ, if at all, from a similar crime that is committed without a computer?
- *Privacy and anonymity*, e.g., what are the consequences (both incremental and cumulative) for privacy and anonymity of any given deployment of information technology?
- *Intellectual property*, e.g., how and to what extent, if any, should intellectual property rights be associated with software?
- *Professional responsibility*, e.g., what are the special ethical responsibilities of IT workers, if any, in the course of their employment?
- *Globalization*, e.g., how and to what extent should disparities in accessibility of information technology between “have” and “have-not” nations be addressed?

Convergence

A common thread among the disciplinary ethics described above is the phenomenon of convergence among the technology disciplines. In this context, convergence means that the disciplines in question are to varying degrees becoming increasingly interdependent. To the extent that this is true, the different ethics of each discipline may—or may not—pose conflicts with each other.

4.3 INTERNATIONAL LAW

Modern international law has its origins in the 1648 Treaty of Westphalia, which is commonly considered the beginning of an international system based on nation-states. At its root, the nation-state arrangement means that international law governs relationships between sovereign states, and that individual states have exclusive jurisdiction over events and matters in their own territories.

¹⁵ See Terrell Ward Bynum, “Computer Ethics: Basic Concepts and Historical Overview,” *Stanford Encyclopedia of Philosophy*, 2001, available at <http://plato.stanford.edu/archives/win2001/entries/ethics-computer/>.

Subsequent treaties and conventions relying on the framework provided by the Treaty of Westphalia (e.g., the various Geneva Conventions addressing armed conflict) share a common goal: to regulate certain armed activities among nations. Over the centuries, international law has sought to adapt to changing patterns of armed conflict while retaining its fundamental principles. The rights accorded by national sovereignty have been increasingly challenged by such changes.

In the 60 years following World War II, the world experienced a remarkable decline in interstate conflict, with internal armed conflict becoming by far the most common form.¹⁶ More recently, terrorism has emerged as a major threat, including the increasing links between terrorists and organized crime in a number of settings. Internal conflict and terrorism/organized crime raise questions about how the international community can respond to threats arising within nations, especially in cases where nations lack the willingness or capacity to respond.

A growing list of international conventions address international security threats that cannot be readily met by national responses alone, such as those against terrorism, piracy, or organized crime. Along with the arms control treaties discussed below in this section, these agreements call on their member states to enact national legislation to implement their provisions. For weapons of mass destruction, UN Security Council Resolution 1540, adopted in 2004, obliges member states to adopt measures to prevent terrorists or organized criminal groups from gaining access to weapons of mass destruction or the means to deliver them. The United States has actively supported many of these measures and has provided assistance to countries to help them adopt appropriate legislation.

The UN treaty process is not the only means through which treaties emerge. In some cases, groups of states come together to craft treaties. The Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction, also known as the Ottawa Treaty, is such an example. In the mid-1990s, widespread use of land mines in violation of traditional military practices¹⁷ prompted humanitarian organizations that could not carry out their missions in postconflict areas because of mine-related hazards to propose a ban on antipersonnel mines. When efforts to change the additional protocol to the Convention on Certain Conventional Weapons (usually acronymized

¹⁶ This shift has occurred despite the fact that the number of nations belonging to the United Nations has almost quadrupled since its creation. Trends in various forms of armed conflict may be found on the Uppsala Conflict Data Program Web site at <http://www.pcr.uu.se/research/UCDP/>.

¹⁷ Traditional military practice calls for the marking of minefields and the subsequent clearing of those minefields by those who lay them. But in the 1990s, a number of military forces, both national and insurgent, were using mines more or less indiscriminately.

as CCW) covering antipersonnel land mines to create a ban on land-mine use failed, a treaty was negotiated outside the UN framework—namely, the Ottawa Treaty. The treaty has 160 members, but a number of major nations and land-mine producers—the United States, Israel, India, Pakistan, Russia, and China—are not parties to the treaty. However, the UN treaty process did amend Protocol II to the CCW, for example to include internal as well as interstate conflict, and the United States, Israel, India, Pakistan, Russia, and China are parties to this protocol.¹⁸

In addition, nations can and do come to international agreements outside of any treaty process. For example, the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction is not a formal treaty;¹⁹ rather, it is a multilateral nonproliferation initiative created by the G-8 countries (Canada, France, Germany, Italy, Japan, the United Kingdom, the United States, and Russia) in 2002 to support the implementation of arms control treaties and customary international law. The members of the partnership (now 25 nations) fund and implement projects to prevent terrorists and other proliferators from acquiring weapons of mass destruction.

The challenges in the new international security context for the application of the modern law of armed conflict to deal with nonstate actors are particularly vexing. In an era of international terrorism, the distinction between “inside a state” and “state-to-state” has been blurred, and legal systems (such as that of the United States) that draw a sharp distinction between law enforcement authorities that operate domestically and military forces that operate internationally have come under considerable pressure. To the extent that new emerging and readily available (ERA) technologies for military purposes are relevant to this new environment (e.g., when they are used by terrorists or to combat terrorists), the development and use of such technologies will challenge existing understandings about when and under what circumstances the use of lethal force is appropriate from legal and ethical standpoints.

The U.S. struggle against terrorism is beset by questions and uncer-

¹⁸ More specifically, Protocol II of the convention had prohibited the indiscriminate use of mines and their intentional use against civilians. It also requires that remotely delivered land mines have effective self-destructing and self-deactivating mechanisms. An amendment to Additional Protocol II, agreed to in 1996, extends the original Protocol II to apply to non-international armed conflicts as well as conflicts between states and to prohibit the use of antipersonnel mines that do not contain enough iron to be detected with standard demining equipment; it also regulates the transfer of land mines. See <http://www.gichd.org/international-conventions/convention-on-certain-conventional-weapons-ccw/amended-protocol-ii/>.

¹⁹ See <http://www.nti.org/treaties-and-regimes/global-partnership-against-spread-weapons-and-materials-mass-destruction-10-plus-10-over-10-program/>.

tainties about whether this struggle should be governed by the laws of war or by the laws governing law enforcement. Domestic law enforcement authorities in the United States operate on the assumption that lethal force is an option of last resort to protect citizens from imminent harm, whereas military forces engaged in hostilities do not operate with such an assumption. In addition, this struggle is conducted against adversaries for whom national borders are irrelevant; how and to what extent are matters of national sovereignty relevant in such a struggle?

Thus, the post-9/11 security context adds another layer of stress on the traditional nation-state system. In addition, more states are seen as inconsistently willing, or even able, to protect the rights of their citizens, and indeed, may be seen as oppressors of their citizens. As a result, the conduct of such states has increasingly prompted international intervention in the internal affairs of individual nation-states, as in the recent cases of Iraq and Libya. Similarly, states increasingly lack the ability to restrain their citizens if they reach out to attack others, even if the targets of these attacks are nations and even if they may strike with force of existential proportion.

4.3.1 The Laws of War²⁰

At the highest level of abstraction, the ethics of war and peace can be divided into three major schools of thought—realism, pacifism, and just-war theory. Realists argue that nations, governments, and even individuals resort to war (or armed conflict) when such actions serve their interests, and by extension, that actions taken to serve vital state interests should not be constrained by ethical considerations. Pacifists argue that as a matter of ethics, war and armed conflict are never appropriate. Because neither of these positions are associated with stated U.S. policy, they are not discussed further in this report.

Just-war theory has existed in some form for many centuries. Just-war theorists—the first of whom came from religious and philosophical traditions rather than legal traditions—argue that war or armed conflict can be justified under some circumstances. That is, a state that uses force or violence against another state must have “god” reasons for doing so. The principle is relevant because it assumes that not using force or violence is the normative and preferred state of affairs, and that the use of force or violence is an unusual act that requires some justification. The set of ethical principles regarding justifications for using force or violence is known

²⁰ The discussion of the law of armed conflict and of related material in this section is based largely on Brian Orend, “War,” *Stanford Encyclopedia of Philosophy: Fall 2008 Edition*, Edward N. Zalta, ed., available at <http://plato.stanford.edu/entries/war>.

as *jus ad bellum*, and it answers the question, When is it permissible for a nation to use force against another nation? Another set of ethics known as *jus in bello* speaks to the question of what behavior is permissible for parties engaged in armed conflict.

The distinction between *jus ad bellum* and *jus in bello* is accepted in many ethical systems, although what specifically is permissible does vary. For example, in his presentation to the committee, Steven Lee noted that the major religions do accept this distinction. Further, they generally acknowledge two other important points. First, going to war should be an enterprise or an activity that does not do more harm than good, however “good” and “harm” are measured. Second, certain people (e.g., civilians) who might get caught up in armed conflict should be exempt from harm if possible. Neither of these points is absolute, and religions may differ in the weight or prioritization they give to these points under different circumstances. The cultural milieu in which a religion is embedded (e.g., an Islamic culture in East Asia as compared with an Islamic culture in Africa) is particularly important in this regard.

Within the Western tradition of *jus ad bellum* and *jus in bello*, there are a number of ethical principles underlying how the international law of armed conflict has been formulated. (The term “law of armed conflict” (LOAC) is used interchangeably with “laws of war.”)

Jus ad Bellum

Decisions about using force have ethical impact. In the formulation of Brian Orend,²¹ the Western tradition of *jus ad bellum* identifies six principles (just cause, right authority, right intention, reasonable hope, last resort, proportionality) that must be satisfied for war to be ethically justified. Four of these principles appear to have relevance for the development of technology for military purposes:

- *Just cause* addresses the reason for engaging in conflict. Some of the reasons offered include self-defense from external attack, defense of others from external attack, and protection of innocents from aggression. In a technology development context, the principle suggests that a distinction might be made between defensive and offensive technologies or applications. In practice, it rarely if ever happens that a particular technology application cannot be used for offensive purposes. (For example, any “defensive” technology might be used to blunt an adversary’s response, leaving the adversary in a weaker position.) Also, “self-defense” is some-

²¹ Orend, “War,” 2008.

times interpreted to allow preemptive or anticipatory offensive action for defensive purposes.

- *Right authority* addresses legitimacy and political accountability. According to the just-war theorists, individuals and other nonstate actors are not permitted to initiate war or armed conflict; only legitimate government authorities, acting in accordance with specified processes, can do so. In a technology development context, the principle might inhibit technology or applications that would facilitate nonstate initiation of armed conflict. Of course, the very premise of this report is that limiting access of nonstate actors to many emerging technologies of military importance will be increasingly difficult if not impossible.

- *Last resort* requires that a state may resort to war only if all less violent alternatives (e.g., negotiations and other nonviolent measures such as economic pressure) to resolving a conflict have proven fruitless. In a technology development context, the principle might suggest the desirability of developing nonviolent but coercive applications that could be used before violent force is used, and other nonviolent applications might be developed to reduce the likelihood of using force. It might also suggest the possible undesirability of technologies that increase the likelihood of a policy maker deciding to use force.

For example, nonlethal weapons are not explicitly designed for causing death and destruction, a fact that may lead policy makers and/or users to favor their use before exhausting other nonforceful options, such as negotiation. Remotely operated systems enable the projection of lethal military force without putting friendly forces at risk, a fact that may lead policy makers to have fewer qualms about the use of force. The use of cyber weapons is inherently deniable, from a technical standpoint, with high-quality tradecraft, a fact that may lead policy makers to use such weapons when deniability is politically advantageous. Such factors, if operative, may lower the thresholds for the use of force by national leaders and/or by troops on the ground.

- *Proportionality* requires that the degree of violence expected by initiating armed conflict should be commensurate with the harm suffered. Moreover, the overall good (such as restoration of the status quo ante) must be worth the costs that will be incurred if armed conflict is begun. In a technology development context, the principle suggests that new and different kinds of harm caused by new weapons might have to be considered. Furthermore, the principle suggests that harm to all parties (including civilians) would reasonably be within the scope of consideration.

From an international legal standpoint, *jus ad bellum* is embodied today in the UN Charter, which generally prohibits “the use or threat of force” by nations (Article 2(4)) except under two circumstances. First,

Articles 39 and 42 of the charter permit the Security Council to authorize uses of force in response to “any threat to the peace, breach of the peace, or act of aggression” in order “to maintain or restore international peace and security.” Second, Article 51 provides: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.”²²

What actions might constitute the use of force, the threat of force, or an armed attack, especially when weapons based on new technologies might be involved? Traditionally, an armed attack was the use of kinetic weaponry to cause a significant degree of death and destruction.

But cyber attack raises the possibility that a nation might be attacked economically (e.g., might be bankrupted) through cyber means without significant death or destruction. Mood-changing chemical agents that do no lasting harm to individuals raise the possibility that their use might not be considered a use of force (although it might be regarded as a violation of the Chemical Warfare Convention). Loss of privacy or loss of computer functionality for civilians is arguably collateral damage when cyber weapons are used, even if today’s interpretations of LOAC do not allow for that possibility. Given that there is no legal consensus on these terms even when traditional kinetic weapons are involved (there are only precedents whose applicability to new situations is often unclear), it should not be surprising that consensus may be lacking when new technologies are involved.

Considering *jus ad bellum* from an ethical standpoint raises additional issues by implicating actions that fall below the level of a use of force or an armed attack. That is, even if an unfriendly or hostile action may not rise to such levels, that action would still be subject to scrutiny with respect to the principles described above.

Jus in Bello

A premise of the law of armed conflict is that unnecessary human suffering during the course of conflict should be minimized even if violent conflict is inevitable from time to time. Again following Orend,²³ *jus in bello* is also based on six principles: adherence to international law on the use (or nonuse) of certain weapons; discrimination between combatants and noncombatants (and immunity for the latter); proportionality;

²² Article 51 is silent on whether actions taken in self-defense are permissible under other circumstances.

²³ Orend, “War,” 2008.

humane treatment for prisoners of war; nonuse of weapons or methods that are “evil in themselves”; and prohibition on reprisals. (Legal analysts also traditionally add military necessity to this list.) Several of these principles appear to have relevance for the development of technology for military purposes.

- *Discrimination between combatants and noncombatants (and immunity for the latter)*. Under this principle, weapons that kill or destroy or cause damage indiscriminately (in a way that cannot distinguish between protected civilian entities and legitimate military targets) may not be used. In a technology development context, the principle would forbid applications that cannot be discriminating in their application, and might impose requirements (or at least preferences) for capabilities that enable users to avoid harm to noncombatants. Chemical agents, certain nonlethal weapons (such as area denial systems), and certain cyber weapons may be regarded under some scenarios for use as indiscriminate in their targeting.
- *Proportionality*. The degree of violence used should be proportional, and not excessive, to the sought military objective. In a technology development context, this principle might require that a weapon be capable of selectivity in the destruction it can cause.
- *Humane treatment for prisoners of war*. In a technology development context, this requirement might inhibit the development of tools for interrogation that might be regarded as inhumane.
- *Prohibition of the use of weapons or methods that are “evil in themselves.”* Arms control treaties (discussed below) that prohibit the use of certain kinds of weapons arguably address this category of weapons.

In addition, LOAC presumes that combatants are subject to a military chain of command. Responsibility for actions taken in war is assumed by military commanders and soldiers in a chain of command. Weapons that operate without explicit human direction raise questions about the ability of a military chain of command to maintain affirmative control over the actions of such weapons. In a technology development context, this principle might inhibit applications that call into question that chain of command.

LOAC is extensively, although not comprehensively, codified in the Hague Conventions, the 1977 Geneva Protocols, and a number of other conventions dealing with particular weapons (such as antipersonnel land mines and blinding lasers) and particular targets (such as cultural objects). Much of LOAC is still found in customary international law. Some LOAC violations are criminalized by the Rome Statute of the International Criminal Court.

The United States is a party to a number of these conventions. Some

are regarded as reflecting, in whole or in part, customary international law, which until recently was almost universally regarded as incorporated into U.S. law and enforceable in U.S. courts. In addition, some LOAC violations are punishable as crimes under U.S. domestic law. The War Crimes Act of 1996, for example, sets forth criminal sanctions for grave breaches of the Geneva Conventions. Other actions are proscribed by U.S. criminal law but are not expressly described as violations of international law. All U.S. military personnel receive training in how to observe LOAC.

The discussion above relates to international armed conflict—armed conflict between nations. But international law also governs non-international armed conflict, which includes but is not limited to civil war.²⁴ The distinction between international and non-international conflicts has always been troublesome. Common Article 3 and Protocol II to the Geneva Conventions are the only general measures addressing non-international conflicts. They contain many of the same protections for noncombatants as the rest of LOAC. In practice, states may treat both kinds of conflicts as the same, and some prominent legal scholars argue that LOAC norms for the international and non-international conflicts “have become nearly indistinguishable.”²⁵

Application of these rules to conflicts between state and nonstate belligerents has also been troublesome. In the aftermath of 9/11, a number of analysts argued that the laws of war did not apply to the Taliban or members of Al-Qaeda,²⁶ but they did not say what law, if any, would provide them with humanitarian protections. The search for protective principles continues today, as nations like the United States struggle, for example, to justify targeted killings based on the certain identification of individuals targeted and the imminence of the threat they pose.

In the struggle against international terrorism, nations continue to be bound by the transcendent principles of necessity, distinction, and proportionality, even if the effect of their application in a given case may be exceedingly difficult to predict. These same principles apply to the deployment and use of all kinds of weaponry. Sanctions for violations of these principles may be found in domestic criminal laws, including

²⁴ More formally, non-international armed conflict is “armed confrontation occurring within the territory of a single State and in which the armed forces of no other State are engaged against the central government.” See Michael Schmitt, “The Manual on the Law of Non-International Armed Conflict With Commentary,” International Institute of Humanitarian Law, 2006, available at <http://www.iihl.org/iihl/Documents/The%20Manual%20on%20the%20Law%20of%20NIAC.pdf>.

²⁵ Michael N. Schmitt, “Targeting and International Humanitarian Law in Afghanistan,” *Naval War College International Law Studies* 85:307, 308, 312, 323, 2009.

²⁶ See, for example, John C. Yoo and James C. Ho, “The Status of Terrorists,” *Virginia Journal of International Law* 44:207, 2003.

the Uniform Code of Military Justice. Punishment may be imposed by ad hoc international tribunals, military commissions, courts martial, or domestic courts.

A relevant ethical question derived from considering the law of armed conflict is the following:

- How and to what extent, if any, does the research effort and foreseeable uses of its results implicate the ethical principles underlying the law of armed conflict? For example:

- What is its impact on policy makers regarding their willingness to resort to the use of force?

- How and to what extent, if any, should the effects of an application be regarded as “harm” that implicates the law of armed conflict?

- How does it affect discrimination?

- How might it affect command responsibilities and authority?

4.3.2 International Human Rights Law

Human rights are restraints on the actions of governments with respect to the people under their jurisdiction. These rights may originate nationally (e.g., the civil and political rights granted under the U.S. Constitution), through international human rights treaties (e.g., the International Covenant on Civil and Political Rights), or through customary international law.

The Universal Declaration of Human Rights (UDHR) is a UN General Assembly declaration adopted in 1948. It is not a treaty, and therefore it is not binding on nations, although some provisions have become a part of customary international law (e.g., prohibitions against torture). However, the UDHR is sometimes cited as one basis for the existence of customary international law regarding human rights.

The UDHR covers such areas as prohibitions on torture and cruel, inhuman, or degrading treatment; freedom to freely seek, receive, and impart information and ideas; freedom to assemble peaceably; and freedom to move and reside freely within the borders of one’s state. In a technology development context, the UDHR might suggest special examination for technologies that governments could use to suppress or curtail the human rights of their citizens.

For example, Article 19 of the UDHR speaks to freedom of opinion and expression and explicitly includes the right to seek, receive, and impart information and ideas through any media and regardless of national borders. Thus, development of information technologies that

could interfere with this right (e.g., technologies that could be used for censorship) potentially raises ethical issues. Article 13 recognizes freedom of movement, thus potentially raising ethical issues with respect to the development of technologies that can enable or facilitate tracking of individual movements.

The UDHR is not a treaty, but over time it has led to the creation of a wide range of legal instruments and customary international law. In 1966, the UN Commission on Human Rights produced the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights. The two treaties contain most of the rights laid out in the UDHR and make them binding on those that have ratified the agreements. Taken together, the three documents are said to constitute the International Bill of Human Rights. The commitments embodied in the UDHR have “inspired more than 80 international human rights treaties and declarations, a great number of regional human rights conventions, domestic human rights bills, and constitutional provisions.”²⁷

International human rights law shares many principles with LOAC. Many states regard human rights law, which in some respects is more protective than LOAC, as applicable in peacetime and in armed conflicts alike.²⁸ However, the United States takes the position that during armed conflicts human rights law gives way to LOAC. If human rights law is intended to codify ethical issues related to human rights—and the discussion of the UDHR above and that of nonlethal weapons in Chapter 3 suggest that a number of the technologies considered in this report have implications for human rights—then assessments of ethical issues may do well to consider human rights as a source of insights.

A relevant ethical question derived from considering international human rights law is the following:

- How and to what extent, if any, do the research effort and the

²⁷ See, for example, United Nations, *The Universal Declaration of Human Rights*, available at http://www.un.org/en/documents/udhr/hr_law.shtml.

²⁸ For a comparison between human rights law and the law of armed conflict, see International Committee on the Red Cross, “International Humanitarian Law and International Human Rights Law: Similarities and Differences,” 2003, available at http://www.ehl.icrc.org/images/resources/pdf/ihl_and_ihrl.pdf and “What Is the Difference Between Humanitarian Law and Human Rights Law?,” 2004, available at <http://www.icrc.org/eng/resources/documents/misc/5kzmuy.htm>. For arguments in favor of the simultaneous applicability of human rights law and the law of armed conflict, see United Nations, “International Legal Protection of Human Rights in Armed Conflict,” 2011, HR/PUB/11/01, available at <http://www.unhcr.org/refworld/docid/4ee9f8782.html>; and Kenneth Watkin, “Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict,” *American Journal of International Law* 98(1):1-34, 2004.

foreseeable uses of its results implicate the ethical principles underlying international human rights law and/or the UN Universal Declaration of Human Rights?

4.3.3 Arms Control Treaties

The theory underlying arms control agreements is that such agreements could serve three broad purposes in principle:²⁹

- *Reducing the likelihood that conflict will occur.* Confidence-building measures—arrangements in which the involved parties agree to refrain from conducting certain activities that might be viewed as hostile or escalatory, to notify other signatories prior to conducting such activities, or to communicate directly with each other during times of tension or crisis—are supposed to reduce the likelihood of conflict due to accident or misunderstanding.
- *Reducing the destructiveness of any conflict that does occur.* Limitations or bans on the use of certain weapons, or on the types of entities that may be targeted, could have such effects, thereby reducing the likelihood of conflict escalation or facilitating more rapid cessation of hostilities. One important aspect of reducing destructiveness is reducing unnecessary destructiveness—a point related to the principle that weapons should not cause superfluous injury or unnecessary suffering.
- *Reducing financial costs.* Limitations on acquisition of weapons may reduce expenditures on those weapons.

All of these rationales arguably reflect ELSI concerns.

Treaties that ban or restrict the use of certain weapons tend to inhibit technology or applications that might resemble, be confused with, or be associated with any prohibited weapon. In addition, the possibility of developing any given technology or application with military value raises the issue of whether U.S. interests are better served by its unrestricted development (and use) or in a world in which its development and use are restricted by mutual agreement with other nations that might also develop and/or use that technology or application. Some of the considerations in addressing such an issue may include the following:

- The technological capabilities of other parties to exploit the technology or application in question, taking into account the time scale on which these other parties will be able to do so.

²⁹ These three purposes can be found in Thomas C. Schelling and Morton H. Halperin, *Strategy and Arms Control*, Pergamon Brassey's, Washington, D.C., 1985.

- The value of unilateral U.S. advantages afforded by the technology or application, taking into account the time scale on which the United States will have such advantages.
- The efficacy with which U.S. advantages can be countered.
- The value of setting an example of restraint in a global environment in which leading states set precedents for the legitimacy of other states to follow in the footsteps of those leading states. (That is, once the United States claims the right to develop and potentially use a given technology or application for military purposes, other states are likely to have fewer inhibitions against making similar claims.)
- The potential for nonstate actors to develop and use the technology, especially if it has low barriers to entry (ERA technologies). If nations restrict the development or use of a technology by treaty but nonstate actors exploit it, the nations may be disadvantaged.

New military technologies or applications may sometimes have the potential to erode constraints initially imposed by existing treaties. Supporters of such treaties often view such erosion as a negative consequence of proceeding with a new military technology or application, and they argue that if a new technology or application is not addressed adequately under existing understandings, it should not be developed until new understandings are formulated that can in fact do so. Others argue that if existing understandings do not address a new technology or application, it should be allowable to proceed with its development until new constraining understandings are reached.

Recognizing concerns about such erosion, many treaties include provisions for addressing new scientific or technological developments that might affect constraints in the treaty.³⁰ Where rapidly changing technologies are involved, the forums established in accordance with these provisions are often quite active.

Advances in science and technology can also provide positive benefits for arms control treaties. For example, new technology can improve national capabilities to monitor compliance with treaties, carry out inspections, or investigate allegations of controlled or prohibited activities. Discussions of how S&T advances can support treaty implementation are common at many review conferences, along with discussion of potential negative impacts. In addition to improving traditional approaches, there

³⁰ For example, Article 8 of the Chemical Weapons Convention provides for a regular review conference to take into account “any relevant scientific and technological developments.” See <http://www.opcw.org/chemical-weapons-convention/articles/article-viii-the-organization/>.

is current interest in harnessing new data-mining, crowd-sourcing, and social media applications.³¹

A relevant ethical question derived from considering arms control treaties is the following:

- How and to what extent, if any, do a research effort and its foreseeable uses implicate existing arms control treaties? How, if at all, does the effort make the treaty regime harder or easier to sustain in the future?

4.4 SOCIAL AND BEHAVIORAL SCIENCES

The impacts of technology depend directly on human behavior, because people are intimately involved in the design, manufacture, inspection, deployment, monitoring, use, operation, maintenance, regulation, and financing of technology. Thus the social and behavioral sciences have an important role to play. They can help to predict the social effects of a new technology or application (e.g., how people are likely to react to a crisis, respond to contradictory information, develop new laws or policies, consume recreational drugs, maintain equipment, write and implement workplace rules, use media, and so on). They can also provide insight into when a proposed design makes unrealistic demands on operators' vigilance, provides perverse incentives (e.g., for denying problems), or can be easily captured by others. In response, the social and behavioral sciences can also affect those impacts by informing the design of new technologies (especially if they are involved early in the process). They can help to promote fair judgments of technology by contributing to the creation of sound and inclusive communication processes. And they can try to predict those judgments by eliciting commentary from members of various stakeholder groups.

Involving the social and behavioral sciences in the R&D process will help to produce better and more informed scientific outcomes. Including these human sciences in the initial design of an application is particularly important to increasing the usability of a new technology, without subsequent costly failures and retrofits. It will also identify the basic research needed for other aspects of the design (e.g., training programs, communication, user interfaces, organizational accommodations). Including the human sciences at later stages allows responding to the new knowledge that becomes available as a science or technology matures.

³¹ For example, see the State Department's "Innovation in Arms Control Challenge," which "sought creative ideas from the general public to use commonly available technologies to support arms control policy efforts." See <http://www.state.gov/r/pa/prs/ps/2013/03/205617.htm>.

The subsections below address possible insights from a number of specific social sciences.

4.4.1 Sociology and Anthropology

Sociology and anthropology provide some of the scientific foundations for anticipating how new technologies will be used and viewed. For example, the prevalent culture in any given society influences the views of its inhabitants on how and when to use force (that is, acts of physical violence). When two societies come into conflict,³² it is not surprising that one party to the conflict interprets the wartime behavior of the other society through its own cultural frame. If the two societies are culturally distant, they will almost surely have very different views on the appropriate roles and statuses of individuals engaged in the conflict, different norms regarding how and when force can be used, and different sanctions for violating those norms.

In some cases, cultural views of conflict are formally expressed in law. For example, as described above, the United States and many other nations codify some of their views of conflict through the law of armed conflict and arms control treaties such as the Chemical Weapons Convention. Of course, the fact that a nation may be party to an international agreement does not necessarily mean that members of its armed forces will always act in adherence to that agreement, or even that the nation itself will always comply with the requirements of the agreement.

Perhaps most importantly, norms and values—whether or not formally codified—are subordinate to the context of the conflict in which they may come into play. For example, a perceived serious threat to survival is likely to reduce adherence to even strongly held norms and values regarding conflict.³³

In her presentation to the committee, Montgomery McFate of the U.S. Naval War College introduced the concept of normative mismatch to describe differences in cultural perspectives on conflict. U.S. military forces may conduct themselves in combat against an adversary entirely in accordance with the laws of war, the Uniform Code of Military Justice,

³² In the context of the present discussion, the term “society” should be understood to refer to the groups that are engaged in conflict. Extrapolating a discussion of “society” to a discussion of “nation-state” makes sense only to the extent that within-nation variability of values and frames is not significant with respect to the discussion at hand. In some cases, the normative perceptions of a dominant group within a nation are most significant, and the views of other groups within that nation may not need to be considered. In other cases, consideration of within-nation variability is essential to the policy goal at hand.

³³ Eric Luis Uhlmann, David A. Pizarro, David Tannenbaum, and Peter H. Ditto, “The Motivated Use of Moral Principles,” *Judgment and Decision Making* 4(6):476-491, 2009.

and other relevant codified and uncodified norms of Western society regarding the use of force, but the adversary may well see the U.S. conduct as disrespectful and dishonorable—and thus subsequently employ tactics that it feels are justified against any disrespectful and dishonorable enemy.³⁴

The concept of normative mismatch is relevant to the development of new military technologies and applications. A first issue might be whether the concept of operation for a new application might point to potential normative mismatches.³⁵ Some examples include:

- *The range of a weapon.* Many U.S. concepts for weapons emphasize the ability to strike from a long distance away, whereas certain societies place different normative value on face-to-face or close-quarters combat.
- *The damage inflicted by a weapon.* A weapon that damages a warrior's dead body, after his death, may violate cultural norms about honor and death. For example, some cultures treat dead bodies as sacred items in a religious tradition.
- *The invasiveness of a device.* For example, a device that checks individuals for concealed weapons may violate cultural norms against inspection of female bodies.

Normative mismatches may occur at higher levels of abstraction as well. In his presentation to the committee, Steven Lee of the Hobart and William Smith Colleges noted the existence of a worldview based on fairness—either no one should have certain weapons that provide overwhelming advantage or every party to a conflict should have them. To the extent that emerging military technologies do provide such advantages over an adversary (as is the intent of the technologically enabled U.S. approach to armed conflict described in Chapter 1), their use potentially violates fairness norms that are held by that adversary.

Lee further argued that perceived violations of a fairness norm are partly responsible for adversaries resorting to terrorism as a method of conflict, even when they have norms regarding the moral impermissibility of targeting noncombatants in conflict. That is, given the inability of

³⁴ In an acknowledgment of such concerns, a speech by John Brennan recognized that the United States “must do a better job of addressing the mistaken belief among some foreign publics that we engage in these [drone] strikes casually, as if we are simply unwilling to expose U.S. forces to the dangers faced every day by people in those regions.” See John Brennan, Assistant to the President for Homeland Security and Counterterrorism, “The Efficacy and Ethics of U.S. Counterterrorism Strategy,” Wilson Center, April 30, 2012, available at <http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy>.

³⁵ The concept of operation for a weapon specifies how and the circumstances under which the weapon's users are expected to use the weapon.

an adversary to counter the stronger party using traditional means of warfare, the adversary may feel less reluctant to violate norms against targeting noncombatants.

A second issue is the impact and significance of the mismatch. The existence of a mismatch, by definition, points to an idea that is outside one's own normative frame of reference. Ideas that are unfamiliar in this sense may result in surprise—something not within one's own norms is likely to be outside one's own set of expectations. For example, the Japanese use of kamikaze missions in World War II came as a surprise to the U.S. Navy—suicide missions against adversaries were not within the Navy's normative expectations. More than a half-century later, the U.S. intelligence community failed to anticipate the use of airplanes as guided missiles, as the 9/11 Commission pointed out, even though every intelligence analyst was familiar with the idea of suicide bombers and Japanese kamikaze missions.

Still another issue is how to develop approaches for dealing with a normative mismatch. Here understanding the source of the norm is important. For example, a preference for face-to-face short-range combat may be rooted in part of a warrior's code, in a manner similar to other concepts such as vengeance. Suicide bombers may be driven by cultural honor codes. If a suicide bomber is motivated by honor, a countermeasure might be turning such bombing into a dishonorable act.³⁶

Cultural and societal issues also affect relationships with nations that are not overt adversaries. Such nations include long-term allies and allies of convenience and/or nonaligned nations.

Long-term allies generally share a set of common values and ethical standards with the United States. However, agreement in general does not necessarily translate into perfect agreement on all issues, and there are examples of military technologies on which the United States and its allies do not necessarily see eye to eye. For instance, the United States and the United Kingdom parted company in 2008 when the latter decided to sign the Convention on Cluster Munitions, which prohibits the use, production, stockpiling, and transfer of cluster munitions. A similar situation exists with respect to the Convention on the Prohibition of the Use, Stockpiling, Production, and Transfer of Anti-Personnel Mines and on Their Destruction (often known as the Ottawa Treaty)—the United States has refrained from signing this treaty, whereas a number of its closest allies have done so.

The fact that the United States has chosen to refrain from signing these treaties does not mean that it does not share the humanitarian

³⁶ Scott Atran, Robert Axelrod, and Richard Davis, "Sacred Barriers to Conflict Resolution," *Science* 317(5841):1039-1040, 2007.

concerns motivating these treaties—indeed, in both instances, the United States has stated through official channels that it understands and respects these concerns, and further that its policies will in many ways conform to or exceed the requirements provided for by these treaties. Nevertheless, its unwillingness to sign these treaties when some of its closest allies have been willing to do so suggests at least the possibility that differences between the United States and its allies may cause political friction under some circumstances or impede planning/execution of coalition operations.

The United States also has relationships with allies of convenience and nonaligned nations. Nations in this category may or may not share U.S. values and may have relationships with the United States that are simultaneously mutually dependent and/or beneficial on one hand and antagonistic and/or competitive on the other. Such relationships are often characterized by suspicion and mistrust.

In this environment, differences in ethical stances toward, for example, a novel military technology or application would not be surprising. A technology regarded by the United States as efficient, cutting-edge, and inexpensive may be seen by an ally of convenience as cruel and cowardly.

The United States has recognized such concerns with respect to the use of armed remotely piloted vehicles (RPVs). In a 2012 speech, John Brennan made the case for the legality, justness, and prudence of U.S. drone strikes, including such strikes in Pakistan.³⁷ He acknowledged that “the United States is the first nation to regularly conduct strikes using remotely piloted aircraft in armed conflict.” Because “many more nations are seeking” this technology and “more will succeed in acquiring it,” Brennan argued, the United States is “establishing precedents that other nations may follow.” “If we want other nations to use these technologies responsibly,” Brennan stated, “we must use them responsibly. If we want other nations to adhere to high and rigorous standards for their use, then we must do so as well. We cannot expect of others what we will not do ourselves.”

But this speech was given long after the first U.S. use of these weapons, during which time a backlash against such use developed. In trying to make an ethical, practical, and strategic case for the legitimate use of such weapons in combat in 2012, the United States was clearly reacting to the backlash rather than proactively leading and shaping the debate—and the former is clearly a weaker position than the latter.

³⁷ John Brennan, Assistant to the President for Homeland Security and Counterterrorism, “The Efficacy and Ethics of U.S. Counterterrorism Strategy,” Wilson Center, April 30, 2012, available at <http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy>.

Questions derived from sociology and anthropology include the following:

- Considering anticipated scenarios for using the results of a research effort, how, if at all, do such scenarios implicate values and norms held by users? By adversaries? By observers?

A psychological perspective on cultural issues is the focus of the subsection below titled “Social Psychology and Group Behavior.”

4.4.2 Psychology

Several branches of psychology are relevant to gaining insights on ethical, legal, and societal issues, including for example, behavioral decision science and the psychology of risk, social psychology and group behavior, political psychology, and human-systems integration.

Behavioral Decision Sciences and the Psychology of Risk

There is a substantial research literature, particularly in psychology, on how people perceive risk, manage those perceptions, and make decisions under conditions of risk. This includes research on specific questions related to scientific or technical risks (for example, nuclear radiation), willingness to accept risks of different kinds, and how risk perceptions change, including on the basis of S&T developments.³⁸

Risk analysis is relevant to the anticipation of ethical, legal, and societal issues as well.³⁹ Predicting the impacts of a technology that is both complex and uncertain—which generally characterizes analyses involving emerging technologies—requires the disciplined use of expert judgment.⁴⁰ Risk analysis provides a set of methods to assist in estimating the effects of complex, uncertain technologies (including both benefits and risks). In the end, of course, risk analysis can only inform judgment; it cannot replace it.

Ethics is relevant to risk analysis with respect to (1) which impacts should be considered (e.g., Does the environment have standing?);

³⁸ Paul C. Stern and Harvey V. Fineberg, eds., *Understanding Risk: Informing Decisions in a Democratic Society*, National Academy Press, Washington, D.C., 1996.

³⁹ Baruch Fischhoff and John Kadvan, *Risk: A Very Short Introduction*, Oxford University Press, Oxford, 2011.

⁴⁰ Ronald A. Howard, “Knowledge Maps,” *Management Science* 35:903-922, 1989; M. Granger Morgan, Max Henrion, and Mitchell Small, *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, Cambridge University Press, New York, 1990.

(2) how each impact should be measured (e.g., Are distributional effects considered, or just the mean?); and (3) how different outcomes should be weighted.⁴¹ For example, risk analysis of nuclear power plants might raise questions about their ability to deliver energy at the promised price, as well as about their potential threats to society. Those risks and benefits may involve human health, the environment, and the economy, as well as the distribution of these risks and benefits, all of which are central societal and ethical concerns. If the ethics of such matters are not explicitly considered, risk analysts are likely to resolve ethical issues by deferring to professional conventions (which are usually based on some ethical framework agreed on in advance) or by imposing their own ethical values and standards.⁴²

Risk analysis seeks to provide a disciplined, transparent way to integrate the knowledge of diverse experts in predicting the performance of a technology in advance of its deployment. It can focus the design process by comparing competing designs and identifying vulnerabilities requiring additional research (e.g., poorly understood properties of materials or social controls on potential uses).⁴³ It can show when the design team lacks critical expertise. It can help decision makers decide whether the benefits of a new technology outweigh its risks, as well as provide the evidence that they need to explain their choices to others.

Risk analyses are soundest when they accommodate a broad range of relevant evidence (e.g., not just readily quantified factors); when they retain awareness of factors that have not been analyzed (e.g., potential design flaws); when they elicit expert judgment with proven methods that are structured to obtain the maximum amount of information from experts; when they do not seek to defend a particular outcome or design or approach; and when they account for uncertainty in the available evidence (e.g., with sensitivity analyses).⁴⁴ Decision makers need candid

⁴¹ Canadian Standards Association, *Risk Management Guidelines for Decision Makers*, CAN/CSA-850, Ottawa, Ontario, 1997 (reaffirmed 2002); HM Treasury, *Managing Risks to the Public: Appraisal Guidance*, Her Majesty's Stationary Office, London, 2005; Sheldon Krinsky and Dominic Golding, *Social Theories of Risk*, Praeger, New York, 1992.

⁴² National Research Council, *Scientific Review of the Proposed Risk Assessment Bulletin from the Office of Management and Budget*, The National Academies Press, Washington, D.C., 2006; Presidential/Congressional Commission on Risk Assessment and Risk Management, *Risk Assessment and Risk Management in Regulatory Decision-Making*, riskworld.com, 1997, available at http://www.riskworld.com/Nreports/1996/risk_rpt/html/nr6aa001.htm.

⁴³ Baruch Fischhoff, *Risk Analysis and Human Behavior*, Routledge/Earthscan, Oxford, 2011; Michael S. Wogalter, *The Handbook of Warnings*, Lawrence Erlbaum Associates, Hillsdale, N.J., 2006.

⁴⁴ Anthony O' Hagan, Caitlin E. Buck, Alireza Daneshkhah, et al., *Uncertain Judgements: Eliciting Expert Probabilities*, John Wiley & Sons, Ltd., Chichester, West Sussex, 2006; E.C. Poulton, *Bias in Quantifying Judgment*, Lawrence Erlbaum, Hillsdale, N.J., 1989.

assessments of the quality of the knowledge that they have for making and defending their choices. Risk analyses can provide that assessment, as long as they are accompanied by acknowledgment of their own strengths and limits.⁴⁵

Some of the questions derived from the psychology of risk include the following:

- How can organizations responsible for technology development ensure that they have the expertise needed to assess all aspects of the technology's performance?
- How can technology-driven and technology-driving organizations improve their ability to identify, analyze, and manage risks?
- When do normal cognitive processes impede the development, deployment, and operation of technology (e.g., wishful thinking, fallacies of intuition, overconfidence)?
- How, if at all, can both deontological and utilitarian (cost-benefit) concerns be accommodated in decision-making processes?

Social Psychology and Group Behavior

An understanding of group behavior may yield insight into how an adversary might react to U.S. deployment or use of certain types of weapons. One of the most important areas of research in providing an understanding of individual and group behavior is the literature from social psychology on the origins and implications of group identity. For example, in a review of the lessons of social psychology for understanding the virulent nationalism plaguing international politics in the years immediately after the Cold War, Druckman suggested:

... they [social psychologists] have explored the factors that arouse feelings of group loyalty when such group loyalty promotes hostility toward other groups; how cross-cutting or multiple loyalties can change the face of nationalism; and how individual group loyalties influence and shape collective behavior.⁴⁶

A 2011 NIH/DOD workshop discussed psychologically motivating factors of terrorism under the rubric of terror management theory, which

⁴⁵ Silvio O. Funtowicz and Jerome R. Ravetz, *Uncertainty and Quality in Science for Policy*, Kluwer Academic Publishers, London, 1990; National Research Council, *Intelligence Analysis for Tomorrow*, The National Academies Press, Washington, D.C., 2011.

⁴⁶ Daniel Druckman, "Nationalism, Patriotism, and Group Loyalty: A Social Psychological Perspective," *Mershon International Studies Review* 38:43-68, 1994, available at <http://bev.berkeley.edu/Ethnic%20Religious%20Conflict/Ethnic%20and%20Religious%20Conflict/2%20National%20Identity/Druckman%20nationalism.pdf>.

states that “human beings are motivated to adopt and police a cultural belief system in order to allay their concerns over their own mortality. Sets of sacred values underpin strong belief systems; such values include those beliefs that an individual is unlikely to barter away or trade no matter how enticing the offer is.”⁴⁷ The workshop summary further noted that “sacred values may prove a pathway towards better understanding the deep underlying motivations behind certain acts of political violence and identifying values that are less resistant to change.”

There are other examples of ways in which the expertise of social psychology may be relevant. For example, experiments have also shown that individuals are more willing to inflict pain on or otherwise abuse those who are not part of “their” group.⁴⁸ How these fundamental aspects of human psychology play out in the context of conflict is addressed in the next section.

Some of the questions derived from social psychology include the following:

- When do attitudes toward a technology become a sacred value, so that groups support or oppose it as a matter of principle, indifferent to cost-benefit concerns?
- How do affinity groups form around new technologies, and when are they mobilized to action?
- How will knowledge about new technologies be disseminated through existing and evolving social networks, among allies and adversaries?
- How can prejudices regarding other groups affect assessments of their ability to use appropriate technologies?

Political Psychology

Political psychology is another relevant branch of psychology.⁴⁹ For example, the United States uses armed remotely piloted vehicles (RPVs) in Pakistan, a nominal ally in the fight against Al-Qaeda. Such use has

⁴⁷ Tessa Baker and Sarah Canna, “The Neurobiology of Political Violence: New Tools, New Insights,” Nsiteam.com, 2010, available at http://www.nsiteam.com/pubs/U_Neurobiology%20of%20Political%20Violence%20-%20Dec10%20Final%20Approved%20for%20Release%205.31.11.pdf.

⁴⁸ See, for example, James E. Waller, *Becoming Evil: How Ordinary People Commit Genocide and Mass Killing*, Oxford University Press, London, 2007; and Stanley Milgram, *Obedience to Authority*, Harper and Row, New York, 1974.

⁴⁹ A relevant paper providing an overview of some aspects of political psychology is Stephan Lewandowsky et al., “Misinformation and Its Correction: Continued Influence and Successful Debiasing,” *Psychological Science in the Public Interest* 13(3):106-131, 2012.

evoked a powerful psychological reaction in the Pakistani populace regarding the collateral damage to Pakistani civilians. In a paper commissioned by the committee, George Perkovich of the Carnegie Endowment for International Peace reports that although Pakistani citizens complain about and bitterly resent the use of such vehicles to fight Al-Qaeda, their resentment is based not on the actual use of RPVs or the collateral damage they cause, but rather on the fact that these vehicles are controlled by U.S. forces rather than Pakistani forces.⁵⁰

Perkovich explains this psychological reaction in two ways. First, the Pakistanis perceive Americans as being arrogant. Second, they also resent the inference of weakness which unequal participation reveals, that is, when one party (the United States) has possession of a needed technology and the second (Pakistan) is denied commensurate control.

Some of the questions derived from political psychology include the following:

- When will a technology be politicized, with the result that attitudes and beliefs about it are determined by ideology rather than by scientific assessments (as has occurred with climate science and evolution, in some quarters)?
- How, if at all, is it possible to correct misconceptions created by politically motivated disinformation campaigns?
- How can political partisans' convictions blind them to the flaws in the technologies with which they are identified?

Human–Systems Integration

The value of any technology depends on individuals' willingness and ability to use it. Having the best chance of realizing that value requires incorporating the best available science of human behavior in the technology's design from the beginning and then in evaluating its performance on an ongoing basis.

Numerous examples of inadequate attention to the human factor in technology design show how a technology's effectiveness can be reduced. For instance:

- *Night vision goggles.* Weight and poor mounting compatibility with standard helmets produce fatigue and decreased performance in visual

⁵⁰ George Perkovich, "Managing Ethical and Social Implications of Militarily Significant Technology: Lessons from Nuclear Technology and Drones," paper commissioned by the study committee, 2012.

and motor skills by users employing night vision goggles over extended time periods.⁵¹

- *Remote operation of unmanned ground vehicles.* A single human operator cannot effectively operate more than one unmanned ground vehicle under active combat conditions (e.g., during times of attack). Further, in the absence of other knowledge, operators of unmanned vehicles tend to use tactics, techniques, and procedures (TTPs) originally developed for operating manned vehicles, pointing to the need for TTPs for the use of unmanned ground vehicles that are specific to the tasks, features, and characteristics of those systems.⁵²

- *Passwords and cybersecurity.* Authentication of an asserted identity is central to controlling access to information technology resources. Passwords are an essential element—in many cases, the only element—of the most commonly used approaches to authentication. But it is well known that individuals tend to choose easy-to-remember passwords—thus making such passwords easy for an adversary to guess.

- *Body armor for female soldiers.* Traditionally, body armor has been designed to protect male bodies. Some research suggests that such armor is less protective of female bodies⁵³ and also that the poor fit of such armor on female soldiers makes it difficult for them to properly aim their weapons and enter or exit vehicles.⁵⁴

- *Coordination.* The effective operation of any complex system requires coordination among the individuals responsible for its design, operation, maintenance, and upgrading. When that coordination fails, designers may require operators to do the impossible, with a technology that they understand incompletely or cannot support with the resources available to them. Such failures affected Three Mile Island, Chernobyl, and Fukushima.⁵⁵

⁵¹ Albert L. Kubala, *Final Report: Human Factors Research in Military Organizations and Systems*, Human Resources Research Organization, Alexandria, Va., 1979, available at <http://www.dtic.mil/dtic/tr/fulltext/u2/a077339.pdf>.

⁵² Jessie Y.C. Chen, Ellen C. Haas, Krishna Pillalamarri, and Catherine N. Jacobson, *Human-Robot Interface: Issues in Operator Performance, Interface Design, and Technologies*, Army Research Laboratory, 2006, available at <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA451379>.

⁵³ Marianne Ressler Wilhelm, "A Biomechanical Assessment of Female Body Armor," *ETD Collection for Wayne State University*, Paper AAI3117255, January 1, 2003, available at <http://digitalcommons.wayne.edu/dissertations/AAI3117255>.

⁵⁴ Anna Mulrine, "Army Uses 'Xena: Warrior Princess' as Inspiration for New Body Armor for Women," July 9, 2012, *Christian Science Monitor Online*, available at <http://www.csmonitor.com/USA/Military/2012/0709/Army-uses-Xena-Warrior-Princess-as-inspiration-for-new-body-armor-for-women>.

⁵⁵ James R. Chiles, *Inviting Disaster: Lessons from the Edge of Technology*, Harper Collins, New York, 2002; Charles Perrow, *Normal Accidents: Living with High Risk Technologies*, Princeton University Press, Princeton, N.J., 1999.

Human factors engineering (also called ergonomics) has long been part of the design of many systems (e.g., cockpits, computer interfaces) in both the civilian and the defense sectors.⁵⁶ It is most useful when incorporated in the earliest stages of the design process, when there is a wide range of opportunities to respond to users' needs. At the other extreme, the need to rely on warning labels in many cases reflects a design failure.

Some of the questions derived from human–systems integration include the following:

- How can requirements be written in order to ensure that technologies can be operated and maintained under field conditions?
- How can the acquisition process evaluate and ensure the operational usability of future technologies?
- What are the institutional barriers to incorporating human-systems expertise in the design process?
- What kinds of expertise and social organization are needed to support a technology, by the United States (so as to increase operability) and by its adversaries (so as to limit the technology's appropriation by them)?

4.5 SCIENTIFIC AND TECHNOLOGICAL FRAMING

In some cases, ethical insights emerge from a scientific and technological framing different from that which is initially offered. To the extent that a given technology or application is based on an erroneous or an incomplete scientific understanding, any risk analysis of that technology or application will itself be incomplete. New ethical, legal, and societal issues may well emerge if and when the underlying science becomes more complete.

For example, assumptions of system linearity and decomposability often enable scientists to make headway in their investigations of phenomena, and so it is natural to turn at first to techniques based on these assumptions. But some systems are not well characterized by these assumptions in the domains of interest to investigators, although it may take some time to recognize this reality. In other instances, there is considerable uncertainty about the relevant data, for example, because they have not yet been collected, or there may be defects in the data that have been collected. In still other cases, system behavior may be emergent and path-

⁵⁶ Steven Casey, *Set Phasers on Stun: And Other True Tales of Design, Technology, and Human Error*, Aegean, New York, 1993; Peter A. Hancock, *Human Performance and Ergonomics: Perceptual and Cognitive Principles*, Academic Press, New York, 1999; and Christopher D. Wickens, Sallie E. Gordon, and Yili Liu, *An Introduction to Human Factors Engineering*, Prentice-Hall, New York, 2004. A historical perspective can be found in Paul M. Fitts, ed., *Psychological Research and Equipment Design*, U.S. Government Printing Office, Washington, D.C., 1947.

dependent, may be very sensitive to initial conditions, or may depend on incompletely known relationships between the system and its environment. Predictions about system behavior may be possible only through high-fidelity computer simulations, may be probabilistic in nature, or may be exponentially inaccurate depending on the time horizons in question. If these realities are not recognized when ethical, legal, and societal issues are considered, such a consideration will be based on an incomplete scientific understanding.

Systems with some of the analytically problematic characteristics are often biological or environmental in nature. For example, early in the history of biology, a “one-gene, one-protein” phenomenology was widely accepted. Today, it is generally accepted that many noncoding parts of DNA control the circumstances under which a specific gene will be expressed, and the rules governing regulation are not well understood. In addition, it is not always possible to predict how natural selection will act on a system over time.

Concerns over ethical, legal, and societal issues may thus sometimes be rooted in disagreements over the fundamental science involved. Are the nonlinearities in the system in question significant? Does the model being used to understand the relevant phenomena capture all essential elements? How sensitive is the model to initial conditions? How far into the future can a model’s predictions be trusted?

A relevant ethical question derived from considering scientific framing is the following:

- How and to what extent, if any, are known ethical, legal, and societal issues related to uncertainties in the underlying science or maturity of the technology?

4.6 THE PRECAUTIONARY PRINCIPLE AND COST-BENEFIT ANALYSIS

Commentators differ in their psychological as well as social orientation toward technology development and application. Those most concerned about potential negative results tend to promote the precautionary principle,⁵⁷ doing so in response to traditional cost-benefit analysis that they regard as using approaches that give innovation the benefit of the doubt.

⁵⁷ A substantial amount of background information on the precautionary principle can be found in Ragnar E. Löfstedt, Baruch Fischhoff, and Ilya Fischhoff, “Precautionary Principles: General Definitions and Specific Applications to Genetically Modified Organisms (GMOs),” *Journal of Policy Analysis and Management* 21(3):381-407, 2002.

The strongest form of the precautionary principle states that when a technology or an application threatens harm—to society, to individuals, to the environment, and so on—precautionary measures should be taken before a decision is made to proceed with developing that technology or application and in general the technology should not be pursued until those concerns are decisively addressed.

Some formulations of the precautionary principle require strong evidence of risks, in the sense of developing a full set of relevant cause-and-effect relationships. Other formulations require less evidence, suggesting that high levels of uncertainty about causality should not be a bar to precautionary action. In these latter formulations, the postulated harms can be merely possible and may be speculative in the sense that the full set of relevant cause-and-effect relationships (that is, relationships between developing the technology or application and the harm that may result) may not have been established with sufficient scientific rigor, or in the sense that the probability of the harms occurring may be low.

The precautionary principle places the burden of proof on those who advocate certain technologies to produce evidence that will reassure reasonable skeptics, rather than on the public to show that development can cause unacceptable harm. Further, the principle often requires that precautionary measures be taken before any development work occurs, and such measures may include a complete cessation of all development work. Advocates of the precautionary principle often invoke ethical commitments to protect the environment from the results of humans' mistakes and to safeguard the public from terrorists.⁵⁸ In the view of these critics, one of the biggest risks is that science and technology will move forward too quickly, causing irreversible damage. An example of applying the precautionary principle to biological research could be the outcome of the 1975 Asilomar Conference on Recombinant DNA Research, discussed in Chapter 1.

A different principle is traditional cost-benefit analysis, which is fundamentally rooted in utilitarian ethics. Cost-benefit analysis relies on the ability to quantify and weigh the value of putative costs and benefits. Quantification is intended to make the assessment of costs and benefits a more objective process, although serious analysts usually recognize the value-laden nature of quantification. For example, in some formulations of cost-benefit analysis, uncertainty about costs or benefits implies that those costs or benefits can be discounted or even dismissed. Costs or benefits that cannot be objectively quantified are not taken into account at all. Examples of such costs could include the costs to the credibility of an organization when a technology fails, is introduced improperly, or causes

⁵⁸ See <http://www.synbioproject.org/process/assets/files/6334/synbio3.pdf>.

harm, or the costs of disruptions to social systems caused by particular technologies. Some versions of cost-benefit analysis do seek to address such matters as well as the impact of uncertainty and risk tolerance.

Any calculation must treat the distribution of risks and benefits in some way, if only to ignore them, without regard for whether those who bear the risks do not get the benefits. A common compromise is to ask whether the beneficiaries from a project could, in principle, compensate the losers—without ensuring that there are mechanisms for effecting those transfers. In cost-benefit analysis, opponents of developing a new technology or application bear the burden of proof of showing that costs outweigh benefits.

Differences among those who advocate cost-benefit analysis can be found in their relative weightings of benefits and costs, how and when to account for uncertainty, and how to bound the universe of costs and benefits. For example, benefits and costs may be realized in the short term or in the long term: How and to what extent, if any, should long-term benefits and costs be discounted compared to short-term benefits and costs? Benefits and costs may be unequally distributed throughout the world: Which parties have standing in the world to claim that their costs or benefits must be taken into account? Inaction is itself an action: How should the costs and benefits of the status quo factor into the weighing of overall costs and benefits?

In practice, a middle ground can often be found between the precautionary principle and cost-benefit analysis. For example, a less traditional approach to cost-benefit analysis sometimes attempts to quantify intangible and long-term costs that would not usually be taken into account in a traditional cost-benefit analysis. One less extreme form of the precautionary principle allows precautionary measures to be taken when there is uncertainty about costs and harms, but does not require such measures. Another less extreme form requires the existence of some scientific evidence relating to both the likelihood and magnitude of harm and the significance of such harm should it occur.

A middle ground requires calculating the costs and benefits of all outcomes for which there are robust methods, along with explicit disclosure of the quality of those analyses, the ethical assumptions that they entail (e.g., regarding distributional effects), the uncertainty surrounding them, and the issues that are ignored. Seeing the limits to the analysis allows decision makers to assess the measure of precaution that is needed.

Some relevant ethical questions derived from considering cost-benefit analysis and the precautionary principle are the following:

- How and to what extent, if any, can ELSI-related tensions between cost-benefit analysis and the precautionary principle be reconciled in any given research effort?

- If a cost-benefit approach is adopted, how will intangible costs and benefits of a research effort be taken into account?
- If a precautionary approach is adopted, what level of risk must be posed by a research effort before precautionary actions are required?

4.7 RISK COMMUNICATION

Those who fund, design, and deploy new technologies must communicate the associated risks and benefits effectively both to those who would use them and to the public that will pass judgment on their work. If users misunderstand a technology's costs and capabilities, they may forgo useful options or invest in ones that leave them vulnerable if they fail to fulfill their promise. If the public misunderstands a technology's risks and benefits, then it may prevent the development of valuable options or allow ones that undermine its welfare.

Communicating about complex, uncertain, risky technologies poses special problems and is often done poorly,⁵⁹ in part because technical experts often have poor intuitions about and/or understanding of their audiences' knowledge and needs. Scientific approaches to that communication have been developed over the past 40 years, building on basic research in cognitive psychology and decision science. The National Research Council's report *Improving Risk Communication* (1989) provided an early introduction to that research.⁶⁰ There are many other sources,⁶¹ including an upcoming special issue of the *Proceedings of the National Academy of Sciences* with scientific papers from the May 2012 Sackler Colloquium on the Science of Science Communication.

⁵⁹ Baruch Fischhoff, "Communicating the Risks of Terrorism (and Anything Else)," *American Psychologist* 66(6):520-531, 2011; Raymond S. Nickerson, "How We Know—and Sometimes Misjudge—What Others Know," *Psychological Bulletin* 125(6):737-759, 1999.

⁶⁰ National Research Council, *Improving Risk Communication*, National Academy Press, Washington, D.C., 1989.

⁶¹ Baruch Fischhoff and Dietram A. Scheufele (eds.), "The Science of Science Communication," Arthur M. Sackler Colloquium, National Academy of Sciences, held May 21-22, 2012, printed in *Proceedings of the National Academy of Sciences of the United States of America* 110(Supplement 3):13696 and 14031-14110, August 20, 2013; Baruch Fischhoff, Noel T. Brewer, and Julie S. Downs, eds., *Communicating Risks and Benefits: An Evidence-Based User's Guide*, U.S. Food and Drug Administration, Washington, D.C., 2011; M. Granger Morgan, Baruch Fischhoff, Ann Bostrom, and Cynthia J. Atman, *Risk Communication: A Mental Models Approach*, Cambridge University Press, New York, 2001; Paul Slovic, *The Perception of Risk*, Earthscan, London, 2000; and Baruch Fischhoff, "Risk Perception and Communication," pp. 940-952 in *Oxford Textbook of Public Health*, 5th Edition, R. Detels, R. Beaglehole, M.A. Lansang, and M. Gulliford, eds., Oxford University Press, Oxford, 2009, reprinted in *Judgement and Decision Making*, N.K. Chater, ed., Sage, Thousand Oaks, Calif., 2011, available at <http://www.hss.cmu.edu/departments/sds/media/pdfs/fischhoff/RiskPerceptionCommunication.pdf>.

All these sources prescribe roughly the same process for developing and vetting a strategic approach to communication, a defensible risk/benefit analysis in advance of any controversy, and communication activities that are both audience-driven and interactive. This process calls for:

- Identifying the information regarding context and scientific background that is most critical to members of the audience for making the decisions that they face (e.g., whether to accept or adopt a technology, how to use it, whether it is still effective). That information may differ from the facts most important to an expert or the ones that the expert would love to convey in a teachable moment.
- Conducting empirical research to identify audience members' current beliefs, including the terms they use and their organizing mental models.⁶² Effective messages depend as much on the nature of the target audience as on the content of the messages themselves. Crafting effective messages nearly always requires the participation of and input from individuals who are representative of the audience. And since it is often impossible to obtain participation and input from the target audience on the time scales needed for response, such input must be obtained before controversies erupt.
- Designing messages that close the critical gaps between what people know and what they need to know, taking advantage of existing knowledge and the research base for communicating particular kinds of information (e.g., uncertainty).⁶³
- Evaluating those messages until the audience reaches acceptable levels of understanding.
- Developing in advance multiple channels of communication to the relevant audiences, including channels based on media contacts, opinion leaders, and Internet-based and more traditional social networks, and avoiding undue dependence on traditional media and public authorities for such communication.⁶⁴
- Disclosing problematic ethical, legal, and societal issues earlier rather than later. Early disclosure is almost always in the interest of the researchers and/or sponsoring agency, provided the disclosure can be

⁶² Dedre Gentner and Albert Stevens, eds., *Mental Models*, Erlbaum, Hillsdale, N.J., 1983.

⁶³ David V. Budescu, Stephen Broomell, and Han-Hui Por, "Improving Communication of Uncertainty in the Reports of the Intergovernmental Panel on Climate Change," *Psychological Science* 20(8):299-308, 2009; Mary C. Politi, Paul K.J. Han, and Nananda F. Col, "Communicating the Uncertainty of Harms and Benefits of Medical Procedures," *Medical Decision Making* 27(5, September-October):681-695, 2007.

⁶⁴ Philip Campbell, "Understanding the Receivers and the Reception of Science's Uncertain Messages," *Philosophical Transactions of the Royal Society A: Mathematical, Physical, and Engineering Sciences* 369:4891-4912, 2011.

handled properly (e.g., without initially providing information that turns out to be wrong and controversial).

- Ensuring that messages reach the intended audiences in a prompt and timely fashion. Controversies can emerge and grow on the time scale of a day, requiring responses on similar time scales. Any message will be less effective if audience members have already formed their opinions or feel that its content was not forthcoming.
- Persisting in such public engagements even over long periods of time.⁶⁵

Achieving these goals typically requires a modest investment of resources, along with a strategic commitment to ensuring that critical audiences are informed—and not blindsided.⁶⁶ Nonetheless, the comments above should not be taken to mean that the process of risk communication is an easy one. Some of the important issues that arise in crafting an appropriate strategy for risk communication include the following:

- *Identifying stakeholders and social networks.* For any emerging and readily available technology, the stakeholders are likely to vary. Identification of the appropriate stakeholder groups and the communication environment in which those stakeholders interact is key to understanding their engagement and their beliefs, attitudes, and values.⁶⁷ Information is commonly shared among interpersonal networks. Understanding the way information is shared among social networks should be foundational to risk communication activities. Research in this area examines how members of social systems share information, how normative information is communicated, the role of group identification in this process, and so on.⁶⁸
- *Identifying the goal(s) of communication.* Communication efforts may be designed with any number of potential goals in mind: enhancing knowledge about an issue, influencing attitudes or behaviors, facilitating decision making, and so on. The specific goal drives formative data col-

⁶⁵ Campbell, "Understanding the Receivers and the Reception of Science's Uncertain Messages," 2011.

⁶⁶ Thomas Dietz and Paul C. Stern, eds., *Public Participation in Environmental Assessment and Decision Making*, The National Academies Press, Washington, D.C., 2008; Presidential/Congressional Commission on Risk, *Risk Management*, Washington, D.C., 1998.

⁶⁷ Rajiv N. Rimal and A. Dawn Adkins, "Using Computers to Narrowcast Health Messages: The Role of Audience Segmentation, Targeting, and Tailoring in Health Promotion," pp. 497-514 in *Handbook of Health Communication*, T.L. Thompson, A.M. Dorsey, K.I. Miller, and R. Parrott, eds., Lawrence Erlbaum and Associates, Mahwah, N.J., 2003.

⁶⁸ Saar Mollen, Rajiv N. Rimal, and Maria Knight Lapinski, "What Is Normative in Health Communication Research on Norms? A Review and Recommendations for Future Scholarship," *Health Communication* 25(6-7, September):544-547, 2010.

lection and subsequent content, as well as choices about channels for communication. Once the goal of communication efforts is clearly identified, crafting the content of information and messages that are shared with stakeholder groups is critical. Message design and rapid message testing methodologies address the *content* of communication interventions—from the types of appeals used in messages to the nature of evidence and arguments presented in communications.⁶⁹

- *Enhancing public perceptions of source credibility, especially in an environment of ubiquitous media and multitudes of sources.* Expertise, similarity, and other cues about people are known to influence how we respond to those people—audiences gather such information through communication. Since the early 1960s,⁷⁰ researchers have documented the effects of perceptions of source credibility (trust, expertise, etc.) on responses to information.⁷¹

- *Accounting for the role of emotion in risk communication processes that might facilitate or inhibit appropriate behavior.* As identified by Janoske et al.,⁷² these emotions include anger, sadness, fear, and anxiety. Acknowledging the impact of such emotions helps in designing more effective communication processes. For example, fear arises in situations over which individuals cannot exercise control—thus, effective risk communication will suggest specific actions or preparedness activities that can be undertaken.

- *Maximizing the positive utility of social media and other emergent communications technologies.* Research addressing the role of new and emerging media in risk communication processes is in its infancy, but research might be conducted on media effects, uses, the spread of information

⁶⁹ Charles Salmon and Charles Atkin, “Using Media Campaigns for Health Promotion,” pp. 263-284 in *Handbook of Health Communication*, T.L. Thompson, A.M. Dorsey, K.I. Miller, and R. Parrott, eds., Lawrence Erlbaum and Associates, Mahwah, N.J., 2003.

⁷⁰ J.C. McCroskey, “Scales for the Measurement of Ethos,” *Speech Monographs* 33: 65-72, 1966.

⁷¹ Salmon and Atkin, “Using Media Campaigns for Health Promotion,” 2003.

⁷² See for example, Melissa Janoske, Brooke Liu, and Ben Sheppard, “Understanding Risk Communication Best Practices: A Guide for Emergency Managers and Communicators,” Report to Human Factors/Behavioral Sciences Division, Science and Technology Directorate, U.S. Department of Homeland Security, College Park, Md.: START, 2012. Available at <http://www.start.umd.edu/start/publications/UnderstandingRiskCommunicationBestPractices.pdf>; Monique Mitchell Turner, “Using Emotion in Risk Communication: The Anger-Activism Model,” *Public Relations Review* 33:114-119, 2007; Kim Witte, “Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model,” *Communication Monographs* 59:329-349, 1992; and Robin L. Nabi, “A Cognitive-Functional Model for the Effects of Discrete Negative Emotions on Information Processing, Attitude Change, and Recall,” *Communication Theory* 9:3:292-320, 2006.

through social media, data mining as a mechanism for media monitoring, and so on.

Last, effective risk communication has a relationship to other ethical, legal, and societal issues, such as informed consent. That is, the process of obtaining informed consent can be viewed as a risk communication event.⁷³ Taking such a view suggests questions such as: When do people make decisions about consenting in research studies? How are the risks and benefits communicated to potential participants? What is the nature of the communication in informed consent documents? What is the role of the sources of information (their characteristics) in this process? What are the cultural and social dynamics of the risk communication process?

Some of the questions derived from risk communication include the following:

- How can technology developers communicate the risks and benefits of technologies to the American public, so as to ensure a fair judgment, without revealing properties that would aid U.S. adversaries?
- What aspects of a technology are fundamentally difficult to understand by nonexperts? How can communications be developed to create the mental models needed for informed consent?
- How can technology developers communicate with the public (and its representatives) to reveal concerns early enough in the development process to address them in the design (rather than with costly last-minute changes)?
- How can communication channels be modeled so as to ensure that members of different groups hear and are heard at appropriate times?
- How can organizations ensure the leadership needed to treat communication as a strategic activity, which can determine the success and acceptability of a technology?

4.8 USING SOURCES OF ELSI INSIGHT

The sources of ELSI insight described above are varied and heterogeneous. This report provides such a variegated list because consideration of each of these sources potentially provides insight into ethical, legal, and societal issues from different perspectives. But in considering what

⁷³ See, for example, Terrence L. Albrecht, Louis A. Penner, Rebecca J.W. Cline, Susan S. Eggly, and John C. Ruckdeschel, "Studying the Process of Clinical Communication: Issues of Context, Concepts, and Research Directions," *Journal of Health Communication* 14, Supplement 1:47-56, January 2009.

insights these sources might offer in the context of any specific science or technology effort, two points are worth noting.

First, many of the sources described above are linked. For example, philosophical ethics—suitably elaborated—is in part a basis for disciplinary ethics and law. Differences between the precautionary principle and cost-benefit analysis mirror distinctions between deontology and consequentialism. The social sciences provide tools to examine the realities of behavior and thought when humans are confronted with the need to make ethical choices.

Second, consideration of a problem from multiple perspectives may from time to time lead to conflicting assessments of the ethics of alternative courses of action. Indeed, perfect consistency across these different perspectives is unlikely. If such consistency is indeed the case, then perhaps the celebration of a brief moment of ethical clarity is in order. But experience suggests that a finding of such consistency sometimes (often) results from either an unconscious attempt to reduce cognitive dissonance and/or a deliberate “stacking of the deck” toward favorable assumptions or data selection to build support for a particular position.

In the more likely case that the assessments from each perspective are not wholly congruent with each other, debate and discussion of the points of difference often help to enrich understanding in a way that premature convergence on one point of view cannot.

5

An Analytical Framework for Identifying Ethical, Legal, and Societal Issues

This chapter presents a possible framework for identifying and assessing ethical, legal, and societal issues that may be associated with a given research effort. Derived from considering the sources of insight described in Chapter 4 and ELSI commonalities that appear in many of the technologies discussed in Chapters 2 and 3, the framework is an organized list of ELSI-related questions that decision makers could ask about the development of any technology or application. The framework has two equally important parts. The first part describes the parties that have a stake, either direct or indirect, in ethical, legal, and societal issues, and it poses questions that might be relevant to these stakeholders. The second part of the framework poses questions in relation to crosscutting themes that arise for many or all of these stakeholders. The chapter then illustrates a worked example of how the framework might be used in practice, and it puts the framework in context by considering its utility from a variety of perspectives. Note that the framework is offered as a starting point for discussion and is not intended to be comprehensive. It is useful primarily for raising ELSI concerns that might not otherwise have been apparent to decision makers.

The approach taken in this framework—posing questions that are useful to assessment of ethical, legal, and societal issues in the context of R&D on emerging and readily available (ERA) technologies that are relevant to national security and providing some discussion of why answers to these questions may be relevant—is similar to the approach described in the framework for assessment of information-based programs offered

in the 2008 National Research Council report *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment*.¹ That framework was intended to help public officials charged with making decisions about the development, procurement, and use of information-based programs to determine the effectiveness of such programs in achieving their intended goals, consistent with national and societal values, compliant with the laws of the nation, and reflective of the values of society. The Government Accountability Office has made use of that framework in assessing a number of programs.²

5.1 STAKEHOLDERS

The first component of the framework described in the present report is organized by stakeholder. That is, any given research project has a variety of stakeholders—parties that have an interest in the project because the project may, directly or indirectly, in the short term or in the long term, have a positive or negative impact on them. This report identifies as possible stakeholders in any research project those involved in or connected to the conduct of the research, the intended users of applications enabled by that research, adversaries against whom those applications may be directed, nonmilitary users of such applications, organizations, noncombatants, and other nations. Not all of these groups are necessarily stakeholders for any given research project or program, and an effort to identify the relevant stakeholder groups is therefore an essential part of any ELSI assessment.

In principle and in fact, ethical, legal, and societal issues affect many groups of stakeholders, many of which are described below. However, not every technology or application will touch the interests of every one of these stakeholders, and part of an analysis of ethical, legal, and societal issues for any given technology or application is to determine the relevant stakeholder groups. An additional analytical step is to determine how the interests of each of these groups should be weighed (e.g., equally or with some other weighting). The science of effective public participation is summarized by a recent National Research Council report.³

¹ National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, The National Academies Press, Washington D.C., 2008, available at http://www.nap.edu/catalog.php?record_id=12452.

² For example, see Government Accountability Office, *9/11 Anniversary Observations on TSA's Progress and Challenges in Strengthening Aviation Security*, GAO-12-1024T, Washington, D.C., 2012, available at <http://www.gao.gov/products/GAO-12-1024T>.

³ Thomas Dietz and Paul C. Stern, eds., *Public Participation in Environmental Assessment and Decision Making*, The National Academies Press, Washington, D.C., 2008, available at http://www.nap.edu/catalog.php?record_id=12434.

The sections below provide a brief description of stakeholder groups along with a number of ELSI-related questions that could apply to each group.

5.1.1 Those Involved in or Connected to the Conduct of Research

The conduct of research in many ERA technology and application domains raises ethical, legal, and societal issues that are most troublesome when the research itself affects humans, which may include human beings directly involved by deliberate intent in the R&D, human beings who are not directly involved in the R&D, and human beings affected through changes in the environment that may occur as the result of the R&D.

In addition, a variety of different impacts may need to be considered—direct and indirect impacts on physical, emotional, or psychological health and well-being; infringements on civil rights; economic status; and so on. For example, titration of a pharmaceutical agent to determine dose-response relationships is an essential element of research on such agents. In the context of incapacitating nonlethal weapons, titration is an issue in determining dosages that will incapacitate the largest percentage of individuals while still being simultaneously nonlethal to them. Mood-altering drugs may need to be tested to determine if they have long-term effects.

But the impact on operators and users of technology is relevant as well. Soldiers with prostheses that can enhance their function over normal human function or pilots of remotely piloted vehicles who execute their missions far away from immediate danger have a psychological relationship to their jobs different from that of soldiers who are not as privileged. Before widespread deployment of such technologies is contemplated, policy makers may wish to understand the psychological effects of such phenomena—raising the question of how such research might be conducted.

Matters such as the scope of populations to include as test subjects, the nature and duration of contemplated harms, and so on are well understood to be within the purview of mechanisms existing in the civilian sector for the protection of humans used as experimental subjects. For example, in testing incapacitants, the question of whether to include young children or the elderly or pregnant women in the test population would arise.

The Belmont report (described in Chapter 4) articulated three ethical principles that can be generalized to the conduct of most R&D: beneficence, respect for persons, and justice.⁴ The remainder of this subsection

⁴ The Belmont report can be found at <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>.

(Section 5.1.1) provides that generalization, and readers interested in the original analysis of the Belmont report should consult that source.

Beneficence

In the context of conducting R&D, the principle of beneficence suggests that the research effort should maximize the benefits and minimize the harms that result. Some key considerations include the following:

- What defines “benefit” and “harm”? Note that a risk of harm is not necessarily the same thing as harm. How can an R&D effort benefit or harm research subjects? The investigator? Society at large?
- When R&D is being conducted for applications that are intended to harm an adversary, how can the nature and extent of harm be ascertained in research? Note that there are many kinds of harm that may be at issue, as suggested in the previous question. Harm may include physical, mental, emotional, financial, and psychological harms.
- How do the definitions of “benefit” and “harm” differ when different stakeholders are involved? For example, different criteria may apply for individuals indirectly affected by a project and for those directly affected as research subjects.
- How should benefits and harms to different stakeholder groups be determined, aggregated, and compared?
- Learning what the benefits of an R&D effort may be sometimes requires exposing stakeholders to some harm or risk of harm. How should learning about possible benefits be weighed against actual or possible harm?

As the Belmont report stated, “The problem posed by these imperatives is to decide when it is justifiable to seek certain benefits despite the risks involved, and when the benefits should be foregone because of the risks.”

Respect for Persons

In the context of conducting R&D, the principle of respect for persons suggests that the effort should obtain voluntary informed consent from parties that are directly involved in such research and act in the best interests of parties that are not capable of providing such consent (e.g., those indirectly affected by the research). Some considerations are as follows:

- What constitutes genuine “informed consent” when information derived from possibly sensitive intelligence sources is part of a threat

assessment? For example, consider a research project to develop a vaccine against a particular biological agent. Specifics of the threat posed by the agent may well be derived from classified sources. How, if at all, is such information to be a part of any “informed consent” process?

- If parties directly involved in research related to a particular application are members of the U.S. armed forces, how and to what extent—if any—is there a conflict between their obligation to obey legal orders and their provision of informed consent on a voluntary basis? For example, Section 3 of Executive Order 12139 authorizes the President to waive informed consent for deployed military personnel for the administration of certain investigational drugs, provided that the President determines that obtaining consent is not feasible; is contrary to the best interests of the (service) member; or is not in the interests of national security.⁵ Have undue inducements been offered to persuade individuals to “volunteer”? What counts as an “undue” inducement?

- Who, if anyone, will speak for the best interests of parties that are not capable of providing informed consent? Almost by definition, such parties are not themselves capable of articulating their interests. For example, the parties may be physically or temporally distant—in other words, future persons—or those with environmental concerns may be affected by certain R&D efforts. How should such concerns be identified, assessed, and ultimately weighed?

Justice

The principle of justice suggests that the benefits and burdens associated with R&D should be fairly distributed. To paraphrase the Belmont report, injustice occurs if some benefit to which a person is entitled is denied improperly or when some burden is imposed unduly. Some considerations include the following:

- On what basis are specific parties or groups of parties selected for direct involvement in a research effort? For example, why is one group rather than another chosen to be the pool of research subjects? Why is one geographical location rather than another the choice for situating a potentially dangerous research facility?

- How and to what extent, if at all, do national security considerations demand that certain groups (e.g., warfighters) accept an exceptional or a higher level of risk than that accepted by or imposed on other groups (e.g., civilians)?

- How and to what extent, if at all, should new knowledge derived

⁵ See <http://www.gpo.gov/fdsys/pkg/FR-1999-10-05/pdf/99-26078.pdf>.

from research be subject to restrictions on distribution? For example, should such knowledge be kept from certain allies or the rest of the world? Should it be restricted from public distribution? If so, why?

5.1.2 Users of an Application

Users are the parties that are intended to use an application—those who make decisions about how and when the application is deployed and operated in the field, and those who use it based on those decisions.

- What could be the nature of the impact, if any, on users of an application? For example, the extended use of a particular application may cause physical damage (e.g., it may require a user to sit at a keyboard for extended periods of time and thereby cause repetitive stress injuries) or psychological stress (e.g., a weapons operator may feel stress if the concept of operations is something with which he is morally uncomfortable).

- What could be the cumulative impact, if any, on users of an application? For example, the insertion of one prosthetic implant may not be harmful, but the insertion of multiple implants or the use of a certain implant with certain drugs may be harmful. By definition, cumulative effects will appear only when the application in question interacts with other components in the user's environment or biology.

- What could be the long-term impact, if any, on users of an application? The short-term impact on a user may be benign, but over the long term, the impact may be harmful. Hearing loss due to repeated exposure to loud noises is an example of such a long-term impact. The history of Agent Orange provides an example of long-term consequences.⁶

5.1.3 Adversaries

Adversaries are parties against which an application might intentionally be directed or parties that might seek to harm U.S. interests. Adversaries are not “stakeholders” in the traditional sense understood in domestic policy matters—obviously, one does not seek adversary input or agreement on weapons intended to affect them, for example. Nonetheless, adversaries certainly are parties that a research project might affect, and

⁶ Agent Orange was a herbicide/defoliant used as a chemical weapon by the U.S. military during the Vietnam War which killed thousands and caused birth defects. See Le Cao Dai, *Agent Orange in the Vietnam War: History and Consequences*, Vietnam Red Cross Society, 2000. An Institute of Medicine (IOM) report addressing a number of ethical, legal, and societal issues related to Agent Orange is Institute of Medicine, *Veterans and Agent Orange: Update 2010*, The National Academies Press, Washington, D.C., 2011, available at www.nap.edu/catalog.php?record_id=13166.

adversaries do have interests that the law of armed conflict requires all nations to take into account.

Thus, considering adversary reactions to the use of new military applications against them is an important part of a framework for assessment of ethical, legal, and societal issues. These reactions fall into at least three general categories:

- *Adversary acquisition of similar applications for their own uses.* The successful use of any new military application of technology is an affirmative demonstration of its feasibility and value, and often carries much more weight with policy makers than any report or study regarding its utility. For example, Stuxnet was the first known operational use of cyber weapons to cause physical damage to infrastructure.⁷ The possibility and feasibility of such an attack were discussed in many reports on cybersecurity, but Stuxnet galvanized the policy community as never before. U.S. use of remotely piloted vehicles in Afghanistan and Iraq has conclusively demonstrated their value in many battlefield situations, and dozens of nations are today pursuing the development of such systems for their own use. Further, such pursuits may from time to time result in systems that are even more advanced than those available to the United States. A final relevant point is that in using such applications against the United States, adversaries may not feel constrained in their observance of the law of armed conflict, as, for example, when they use human shields.

- *Adversary development of countermeasures that negate or reduce the advantages afforded by new military applications.* For example, the microwave-based Active Denial System can be countered through the use of aluminum foil to protect exposed areas of skin.⁸ In some cases, a remotely piloted vehicle can be “spoofed” into thinking that its location is a long way from where it actually is.⁹ For those cases in which countermeasures are relatively easy and inexpensive to develop, the wisdom of pursuing a given application may be questionable unless the primary value of the

⁷ The Stuxnet computer worm, first discovered in June 2010, was aimed at disrupting the operation of Iran’s uranium enrichment facilities. See http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html.

⁸ The Active Denial System (ADS) is a directed-energy nonlethal weapon first developed in the mid-2000s and designed for keeping humans out of certain areas. The ADS aims a beam of microwave energy at a target such as a human being, thus causing an intense burning sensation on the human’s skin. However, because the beam does not penetrate very far into the skin, it causes little lasting damage (no lasting damage in nearly all cases). The pain is intended to cause the human to turn away and flee the area.

⁹ Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys, “Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle,” *GPS World*, August 1, 2012, pp. 30-33, available at http://radionavlab.ae.utexas.edu/images/stories/files/papers/drone_hack_shepard.pdf.

application can be realized before countermeasures emerge. Indeed, ethical, legal, and societal issues may arise without the hoped-for benefits of an application ever having been realized.

- *Adversary perceptions of a military application's uses against them.* The possible emotional and psychological reactions of an adversary to an application's use span a wide range. At one end, an adversary may be so discouraged by the use of a very potent application that he simply loses the will to continue engaging in conflict. At the other end, an adversary may be so outraged and incensed by the use of a very potent application that he redoubles his hostile efforts and recruits others to his cause—such outcomes are made more likely when the use of such an application has caused nonnegligible collateral damage.

Some questions that arise from these kinds of adversary reactions include the following:

- What is the nature of the direct impact, if any, of use of an application against adversaries? Not all applications have a direct negative impact against adversaries—examples might include better battlefield medical care and sources of alternative fuel.

- How and to what extent can the application's impact be reversed?
- How do considerations of symmetry apply? That is, what are the ELSI implications of an adversary pursuing the same technology development path as the United States? For example:

—Under what circumstances, if any, would an adversary's use of the same application against the United States, its allies, or its interests be regarded as unethical?

—Assuming that the United States is conducting R&D on application X, how would the United States interpret the intentions of an adversary conducting similar research?

- In the long term, what is the impact of an application on adversary behavior and perceptions?

—How and to what extent could an adversary develop similar capabilities? What is the time scale on which an adversary could do so? How could an adversary use these capabilities? What advantages could an adversary gain from using these capabilities free of legal and ethical constraints?

—How do the benefits to the United States of pursuing a particular application unilaterally compare to the potential losses should an adversary develop similar applications in the future?

—What countermeasures might an adversary take to negate the advantages conferred by the application in question? How long would it take for the adversary to obtain those countermeasures? How, if at all, could the developed countermeasure be worse in some way from an ethical standpoint than the application itself?

—How could the application affect the adversary's perception of the United States? For example, the application might instill a fear in the adversary that would inhibit the adversary from taking action against the United States, or it might instill a resentment or hatred that might inspire still others to take additional action against the United States.

—What, if any, could be the application's effect on deterrence? Note that the United States justifies nearly all military programs by their (putatively) enhancing effects on deterrence. But adversaries may not necessarily see U.S. military R&D activities in the same light, and in fact may initiate their own similar program *because* the United States appears to be seeking a technological advantage.

—What effect, if any, could U.S. restraint in pursuing a particular application have on inducing an adversary to exercise similar restraint? A relevant precedent is the ban on assassinations promulgated by Executive Order 12333.¹⁰ The original rationale for this ban was the concern that in its absence, assassinations of U.S. political leaders would be legitimized.

—What, if any, opportunities for adversary propaganda could an application enable or facilitate? For example, how, if at all, could an adversary be able to point to a U.S. program as indicative of an immoral, unethical, and hostile stance toward it?

5.1.4 Nonmilitary Users

Military applications also sometimes have value to nonmilitary users. Changing the problem domain from a military to a civilian one can and often does raise other ethical and societal issues. Three of the most prominent nonmilitary problem domains are those of law enforcement, commerce, and the general public.

Law Enforcement

From a technical standpoint, many of the problems facing law enforcement have military or other national security counterparts. Such problems include those of personal protection, surveillance, and intelligence analy-

¹⁰See <http://www.archives.gov/federal-register/codification/executive-order/12333.html>.

sis. But law enforcement authorities, at least in the United States, operate under an entirely different legal regime than do military or other national security authorities, one premise of which is that residents of the United States enjoy certain rights that other groups (e.g., enemy combatants) do not have. For example, the U.S. military is legally permitted to participate in domestic law enforcement operations only at the request of civilian law enforcement authorities. Thus, a relevant question is the following:

- If the military application in question were deployed to support law enforcement operations, how and to what extent, if any, could such deployment raise ethical, legal, and societal issues that do not arise in the military context? Possible differences include the different legal authorities provided in Title 18, Title 10, and Title 50 of the U.S. Code (dealing with criminal law enforcement, military, and intelligence affairs, respectively), and possible restrictions imposed by the U.S. Constitution on the U.S. government acting domestically.

Commerce

Technologies developed for military applications sometimes have commercial and economic relevance. A good example is the evolution of packet-switched communications, originally developed by the U.S. Air Force to enhance the survivability of military communications networks,¹¹ into the ARPANET (supported by DARPA) and then the Internet. Again, commerce in the private sector is a different problem domain and thus raises different ethical issues. A relevant question is the following:

- How and to what extent, if any, could a commercial adaptation of a military application raise ethical, legal, and societal issues that do not arise in the military context? Such issues might include issues of access (which commercial companies might profit from government efforts to develop the application), accountability (public accountability regimes of private-sector companies differ from those of the government), and possible adoption of technologies by adversaries after commercialization (such uses may be different from adoption as described above).

The General Public

Technologies developed for national security applications sometimes can be adapted for use by ordinary citizens, uses both good and bad. For

¹¹ Paul Baran, "On Distributed Communications: Summary Overview," RM-3767-PR, Rand Corporation, Santa Monica, Calif., August 1964.

example, it is possible today to purchase over-the-counter a remotely piloted aircraft for a few hundred dollars. Controlled via Wi-Fi, this airframe—called a quadricopter—can stay aloft for about 20 minutes and has an onboard video camera whose uses are limited only by the operator's imagination. A relevant question is thus:

- How and to what extent could adaptations of a military application be used by ordinary citizens? What are the ELSI implications of such use?

5.1.5 Organizations

For the U.S. armed forces, military applications of technology do not exist in a vacuum. The introduction of new technologies into military organizations often has a significant impact on the practices, procedures, and lines of authority embedded in those organizations. Individuals make decisions about deployment and use, and these individuals are themselves embedded in organizations and are thus affected by the structure and culture of those organizations. Organizational structure and culture are the foundations of accountability and chains of command, and affect matters such as promotion, respect, levels of cooperation between units, and influence within a hierarchy. Organizations determine rules of engagement and other orders that specify the conditions under which various applications may be used.

For example, the significance of cyber conflict (in both its offensive and defensive aspects) has led the Department of Defense to establish Cyber Command, an entirely new element of U.S. Strategic Command and likely to become its own combatant command co-equal to other combatant commands. The U.S. Air Force is reorganizing itself to accommodate a large influx of pilots for remotely piloted vehicles, and such reorganization will inevitably have an impact on the Air Force's organizational culture.

Introducing new technology that affords new capabilities often affects the assumptions on which an organization is structured, and thus may have implications for the organization. Relevant questions may include the following:

- How and to what extent, if at all, could a new military application influence or change traditional structures and mechanisms of accountability and responsibility for its use? For example, some applications are intended to drive certain kinds of battlefield decision making to lower ranks in the military hierarchy. How will the organization react to such tendencies? How, if at all, will accountability for the use of the application in question be maintained? Conversely, might the application make it less likely for someone in the lower ranks to raise questions about ethical use?

- Military organizations often place great value on personal bravery in combat. How and to what extent, if at all, could a technological application used in combat change such valuation?
- Promotions in many military organizations are sometimes based on command opportunities. How and to what extent, if any, could an application change command structures? For example, will piloting a remotely piloted vehicle confer the same cachet and status as piloting a crewed air vehicle?

5.1.6 Noncombatants

Noncombatants are those who do not participate directly in hostilities, and they include bystanders on the battlefield, family members of combatants, civilians in nonbattlefield areas, civilians who may be affected by environmental damage, personnel from nongovernmental organizations, and future generations.

Questions relevant for noncombatants as stakeholders in the use of new military applications may include the following:

- How and to what extent could an application affect noncombatants on and off the battlefield? Although it is true that a weapon can be used in ways that cause excessive collateral damage and other ways that do not, a weapon that is inherently incapable of discriminating between combatants and noncombatants may well raise ethical, legal, and societal issues. This question is routinely asked in the Department of Defense laws-of-war review of new weapons systems, described in Chapter 7.
- How might the public at large perceive a given application? As noted in passing in Chapter 3, the Martens clause of the Geneva Conventions prohibits the use of weapons whose use violates “the principles of humanity” and the “dictates of public conscience,” even if the precise meaning of this clause in the case of any given weapon is not necessarily clear. In so doing, this clause in principle gives standing to the public at large to object to the use of such weapons.
- How and to what extent could an application affect future generations? For example, could operating an application cause genetic changes in users? And what might be the effects of such operation on those targeted by the application?
- How and to what extent could the operation of an application—especially large-scale operations—harm the environment? An illustration is that the use of depleted uranium in ammunition in large quantities may have significant radiation effects on the environment in which it is used, thus potentially placing in danger individuals present in that environment now or sometime in the future.

5.1.7 Other Nations

The behavior of the United States can affect perceptions and attitudes in other nations. For example, long-term allies who tend to share U.S. values may nevertheless disagree over the ethics of certain military applications, as noted in Section 1.6 (“What Is and Is Not Within the Scope of This Report”). Relevant questions may include the following:

- What, if any, could be the impact of a new military technology or application on political solidarity with the United States?
- How, if at all, could the technology or application raise questions about the strength of U.S. commitments to other nations or allies?
- What could be the impact, if any, on U.S. reluctance to share a technology or application with its allies?
- How, if at all, could a technology or application affect the willingness of allies to participate in coalition efforts with the United States if the latter uses this technology?

In addition to long-term allies, the United States must also consider its relationships with allies of convenience and non-aligned nations. Some relevant questions include:

- How and to what extent, if any, could U.S. restraint in pursuing a new military application induce other nations to exercise similar restraint?
- How and to what extent, if any, could an application help to compromise human rights if used by another nation on its own citizens?

5.2 CROSSCUTTING THEMES

The second component of the framework described in this chapter is a set of themes that cut across different stakeholder groups. That is, in some cases, similar ethical, legal, and societal issues appear in considering the perspectives of a number of stakeholders. This report identifies as crosscutting themes issues related to scale, humanity, technological imperfections, unanticipated military uses, crossovers to civilian use, changing ethical standards, ELSI considerations in a classified environment, and opportunity costs. Last, the sources of insight from Chapter 4 suggest other themes that from time to time cut across different stakeholder groups.

5.2.1 Scale

Against the backdrop of stakeholder concerns described above, it is helpful to keep in mind several dimensions of scale in thinking about

ethical, legal, and societal issues both in research and in its applications and their use.

Societal Scope

In principle, an application might have an impact on a specific military situation, on the military as an institution, on the ways in which conflicts are prosecuted, on specific parts of society, or on large segments of society. Relevant questions regarding scope may include the following:

- How and to what extent, if any, could a change in the scale of deployment or use of a technology or application change an ethical calculation? For example, if an application provides value to one soldier, does the overall value or risk of the application increase if that application is used by many soldiers?

- How and to what extent, if any, are the costs of using a particular application transferred from its immediate users to other entities? Economics gives the label “externalities” to describe situations in which such costs, which may include costs that go beyond immediate financial costs alone, are indeed transferred in this manner—with the result that the immediate users do not bear the full costs of their activities and therefore tend to overuse the resource in question.

- If an application becomes successful because of the increased functionality it affords to its users, and such functionality becomes essential for individuals participating in society, how and to what extent, if any, can the costs of obtaining an essential application be made broadly affordable so that all individuals can obtain its benefits equally? This question is especially relevant to military applications that turn out to have civilian utility, as might be the case for advanced prosthetic limbs originally designed to serve the medical needs of soldiers injured in battle.

Degree of Harm

The degree of inadvertent or undesirable harm associated with an application may span a very broad range. Some research on or uses of one application may cause only minor and unmemorable inconvenience to those affected, whereas other research or uses involving another application may kill people or destroy property on a large scale. How and to what extent, if any, does the degree of inadvertent or undesirable harm compare to the benefits obtained from using that application?

The Nature of the Activity

From research to use is a very long path, and different ethical, legal, and societal issues arise when an activity is considered basic research, applied research, development, testing, deployment, and use.

- How does the scale of ethical, legal, and societal issues differ along the continuum from basic research to use of an application? How do the stakeholders and their interests change?

Timing Considerations

- What are the ELSI considerations in weighing short-term benefits against long-term costs and how does the scale of such benefits and costs affect these considerations?

5.2.2 Humanity

Many ethical issues raised by new technologies or applications revolve around what it means to be human. In some ways, this should not be surprising—the very purpose of tools (that is, technology) is to extend the abilities of humans. Today, the technologies of reading and writing are taken for granted as part of human existence, but Socrates noted around 370 BC that:

... this discovery of yours [writing] will create forgetfulness in the learners' souls, because they will not use their memories; they will trust to the external written characters and not remember of themselves. The specific which you have discovered is an aid not to memory, but to reminiscence, and you give your disciples not truth, but only the semblance of truth; they will be hearers of many things and will have learned nothing; they will appear to be omniscient and will generally know nothing; they will be tiresome company, having the show of wisdom without the reality.¹²

In a military context, many applications of technology pose issues related to extending human capabilities. Prostheses could be developed to enhance human functions—physical functions such as lifting strength and running speed and sensory functions such as night vision and enhanced smell. Advances in neuroscience might be able to help soldiers process information more quickly, operate equipment through a direct brain-machine interface, and remember more information, or they might enable the creation of false human memories or make it possible to induce differ-

¹² Alexander Nehamas and Paul Woodruff, eds., *Plato's "Phaedrus,"* Hackett Publishing Company, Indianapolis, Ind., 1995.

ent emotional states (e.g., reduced or increased fear, feelings of anger or calm). Information technology underlies increasing automation of many functions previously delegated to people,¹³ but today and more so in the future, computers may make decisions that have traditionally been made by responsible humans in positions of authority.¹⁴

More broadly, responsible stewardship for the humanity of the soldiers that the nation asks to go to war is an important concern for policy makers—and the technology of war may have an impact on that sense of humanity. Military psychologist David Grossman argues that the act of killing has important psychological effects on individuals that may affect their sense of humanity.¹⁵ Philosopher Shannon French argues that soldiers live by a “warrior’s code”—a code of values—about what is right and wrong in combat, and that this code is the shield that guards their humanity.¹⁶ She further argues that an individual’s sense of humanity and sense of himself or herself is endangered by, among other things, excessive distancing in war (e.g., the use of drones), dehumanization of the enemy, and the erosion of traditional warrior values.

In other words, asking soldiers to violate their code of values, explicitly or implicitly, and thus to act unethically is inherently harmful to these soldiers—not physically, but psychologically. In particular, asking soldiers to use weapons in an unethical manner or to use weapons that violate a soldier’s sense of his or her obligations under the code may make it harder to reconcile their actions with their values, and may ultimately impede their healthy transition out of combat and back into civilian life.

Questions relevant to concerns about technologies’ effects on individuals’ sense of humanity may include the following:

- How and to what extent, if at all, does a new military application

¹³ For example, the World War II *Baltimore*-class cruiser (CA-68) displaced 13,600 tons and carried a crew ranging from 1650 to 1950 individuals. By contrast, the planned DDX *Zumwalt*-class destroyer (DDG-1000) is expected to displace approximately 14,500 tons and carry a crew of 140 individuals.

¹⁴ A critique of the idea that computers might replace human judges, for example, is found in Joseph Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation*, W.H. Freeman, San Francisco, 1976. A paper by law professor Anthony D’Amato advocates exactly this idea. See Anthony D’Amato, “Can/Should Computers Replace Judges?” Northwestern University School of Law, Evanston, Ill., 1977, available at <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1128&context=facultyworkingpapers>.

¹⁵ Dave Grossman, *On Killing: The Psychological Cost of Learning to Kill in War and Society*, Little, Brown and Company, Boston, 1995 (hardback), 1996 (paperback, in 18th printing as of 2008).

¹⁶ Shannon French, *Code of the Warrior: Exploring Warrior Values Past and Present*, Rowman and Littlefield Publishers, Inc., Lanham, Md., 2003.

compromise something essential about being human? How and to what extent, if at all, might users believe that the application is unethical?

- How and to what extent, if at all, is the application invasive of the human body or mind? This question applies both to users and adversaries, although perhaps in different ways.
- How and to what extent, if at all, could use of an application tread on religiously or culturally sensitive issues (e.g., notions of “playing God” or using animal parts in humans (aka the “ick” factor))?
- Does a technology threaten to cede control of combat capabilities to nonhuman systems to an unacceptable degree?

5.2.3 Technological Imperfections

The first operational use of a military application almost never marks the end of development work on that application. First generations of an application are refined in subsequent iterations to address flaws in the application’s design and/or implementation that become apparent through operational use and to improve its capabilities above and beyond those afforded by the first generation.

Technological imperfections raise ethical, legal, and societal issues for a number of reasons. Under the pressure of delivering a potentially important new capability, applications developers may make choices that provide less safety, reliability, or controllability than they can with subsequent generations—and ethical, legal, and societal issues arise when an application affords less safety, reliability, or controllability than it could afford.

A different take on technological imperfection is that sometimes a technology’s potential is limited by exogenous factors. For example, nearly all “nonlethal” weapons can be lethal under some circumstances. This can be the case because, for example, the maximum “sublethal” dose (of energy or a chemical substance, for example) can vary from individual to individual owing to differences in physiology (so that what is sublethal for one individual is lethal for another) or because one individual is exposed to a given weapon more than another individual in a particular situation (e.g., he or she is closer to a weapon than someone else). Recognizing this point, many analysts use the term “less lethal” weapons. Whether genuinely nonlethal weapons can be developed (the paradigm of which is the “stun” setting on a Star Trek phaser) remains to be seen, but no plausible mechanisms have been identified to date that would underlie a nonlethal weapon’s operation.

To the extent that an application depends on information technology, the reality of all complex software is that it is flawed in some way. Flaws in the software may have an impact on the behavior of an autonomous sys-

tem, and the resulting behavior may raise ethical, legal, and societal issues that properly written software would not raise. Such flaws may raise safety issues related to improper operation under certain circumstances.

An analogy exists with embedded control systems in automobiles and/or commercial transport aircraft. Vendors of these control systems make use of extensive quality control and testing measures during design and prototyping, but in neither case are the resulting systems flawless. Still, they are “safe enough” to meet the safety requirements for the corresponding applications. In other words, the alignment of design quality and assessment has happened, partly because the alignment process has been underway for decades. More generally, safety issues become resolved by a lengthy process of trial and error, adjustment, societal adaptation, and the like.

Standards of performance are also inherently social in nature. For example, the stated performance safety requirements of an application (e.g., that a new weapon must have at most a 1-in-10⁹ chance of harming its operator when it is fired) reflect not only technical inputs that determine what is possible but also economic and ethical judgments about how much safety can be obtained for different levels of expenditure.

Questions relevant to technological imperfections as they affect applications might include the following:

- Who decides the appropriate safety requirements associated with a new application?
- On what basis are such decisions made?
- What, if any, are the tradeoffs between an application’s functionality or use and the safety requirements imposed on it?

5.2.4 Unanticipated Military Uses

An application’s concept of operation is an articulation of how an application is expected to be used. But, of course, these expectations may not include all possible modes of usage for that application. In other words, there are generally a variety of unintended uses of an application that are not explicitly sanctioned by its proponents and that go beyond the stated concepts of operation.

For example, the discussion of nonlethal weapons in Chapter 3 suggests the possibility that nonlethal weapons could be used as a means for torture. Although such use is not part of the stated concepts of operation for these weapons, such unintended uses—if known—are properly part of an ELSI analysis of an application.

A relevant question may be the following:

- What military uses are possible for the application or technology in question that go beyond the stated concepts of operation? What are the ELSI implications of such uses?

5.2.5 Crossovers to Civilian Use

One obvious possibility for civilian use of new capabilities enabled by various emerging and readily available technologies is in law enforcement and domestic security. For example, some law enforcement authorities have argued for the use of certain autonomous systems (e.g., drones for surveillance, bomb disposal robots) and certain nonlethal weapons (e.g., tasers, dazzling lasers). When such resources are controlled by the Defense Department, their use by law enforcement authorities is limited by the Posse Comitatus Act (codified at 18 USC 1385), which prohibits the U.S. armed forces from taking part in domestic law enforcement, unless such actions are explicitly authorized by statute or the U.S. Constitution. (For example, 10 USC 371-381 of the U.S. Code explicitly allows the Department of Defense to provide federal, state, and local police with information, equipment, and training/expertise.) But law enforcement may not need to rely on DOD resources to gain access to the capabilities they afford. Indeed, vendors may well approach law enforcement authorities with proposals to sell versions of military applications customized for law enforcement purposes.

In any event, the civilian law enforcement use of an application originally intended to operate in a military context generally calls forth a different set of ELSI considerations. For example, legal restrictions on “unreasonable search” apply to the use of drones for law enforcement surveillance, but they do not apply in a military context. Rules of engagement for nonlethal weapons in a law enforcement context are very different from those that apply in a military context (for example, law enforcement officials are not generally given orders to “shoot on sight”). Onion routing and TOR—anonymizing technology developed by the Office of Naval Research—are used to advance U.S. foreign policy interests (such technology facilitates untraceable communications, which can be used by dissidents living under nondemocratic regimes).¹⁷ But onion routing has also been used to conceal criminal activity in democratic nations as well.

Civilian applications of existing military applications are potentially broader than their use for law enforcement. More speculative applications of use for law enforcement include various neuroscience-based applications (e.g., functional magnetic resonance imaging) to detect deception. Nor need the applications be confined to law enforcement. In a health

¹⁷ “Onion Routing,” Onion-Router.net, available at <http://www.onion-router.net>.

care context, physicians and others seek better prostheses to replace human functionality lost to accident or injury. Transportation companies (e.g., moving companies, taxi companies) may be able to use capabilities recently developed by DARPA for automated vehicle driving—a point suggesting that such technology has the potential to displace many jobs previously thought to require humans. Ordinary citizens could use inexpensive drone technology to follow children or to gather intelligence on spousal affairs.

All of these nonmilitary applications raise ethical, legal, and societal issues that do not appear in a military context, even if the technology needs only relatively minor changes in transitioning from military to civilian uses. For example, sophisticated prostheses generally provide more capability and thus cost more; increased costs are easier to accommodate politically when they support soldiers wounded in action than when they may be used to support civilians injured in the course of everyday life.

Such considerations related to civilian use of military applications raise the following questions:

- How and to what extent, if any, could civilian-oriented adaptations of military applications made widely available to citizens raise ethical and societal issues that do not arise in the military context? Consider also that “civilians” include both those using civilian adaptations and those who might be injured by such use.
- How fast should such military-to-civilian transfers of applications be made? What safeguards should be put into place before they are made? How should such safeguards vary with the technology involved?

5.2.6 Changing Ethical Standards

The use of a particular technology may well change the ethical standards associated with the problem being solved. For any given dimension of performance, is it sufficient that the standards for autonomous systems call for performance equal (on average) to what humans can do? Or should such systems be held to a much higher standard, perhaps a standard of near-perfection? Although the first (weaker) standard is an instance of technology not diminishing the degree of ethical behavior on the battlefield, it is also true that an ethically questionable action involving new technology will be subject to a high level of scrutiny and criticism, and this may be true even if the technology has built up a long record of ethically appropriate performance.

Thus, issues of legitimate expectations, due care, and reasonable control become relevant. The core recognition is that society expects that its institutions and their experts will field systems that include adequate

control and continuing due care. Society has a minimum standard for control and due care, even if it is not articulated explicitly, the violation of which results in public disapproval. Certain kinds of technology or application are of more and deeper concern for the public, and thus face more stringent scrutiny.

A second ethical standard—legally expressed in the laws of war—may also be affected by the availability of new weapons. One aspect of this issue is discussed in Chapter 4 under the general heading of force being a measure of last resort under principles of *jus ad bellum*—the availability of weapons that reduce the risks to decision makers may increase the likelihood of those decision makers deciding to use force.

A second aspect of this issue is that many new weapons are designed to be significantly more discriminating than those of earlier generations. Using such weapons is likely to produce less collateral damage, an outcome that serves the goals of the *jus in bello* law of armed conflict. At the same time, their availability may, under the principle of necessity, create obligations—ethical if not legal—to use such weapons rather than weapons that may be less discriminating. Many militaries reject such obligations, but militaries are only one of the stakeholders involved in ethical discussions.¹⁸

Such considerations regarding ethical standards raise the following questions:

- If an application is intended to address a military issue that previously had to be addressed by humans, what is the minimum standard of performance that the application must meet before it is deemed acceptable for widespread use?
- How and to what extent, if any, does a new application create new ethical obligations to use it in preference to older applications addressing similar problems that may raise ELSI concerns to a greater extent?

5.2.7 ELSI Considerations in a Classified Environment

Basic science is not tied to specific applications and is therefore usually unclassified, even if it is supported by the Department of Defense. But as a technology development gets closer to specific applications with military utility, the likelihood increases that such work will become clas-

¹⁸ Weapons in this category include precision-guided munitions (e.g., “smart” air-to-surface bombs that can be remotely guided with high accuracy), low-yield nuclear weapons for use against hard or deeply buried targets, “smart” antipersonnel land mines that self-destruct or self-neutralize after a predetermined period of time, various nonlethal weapons, armed drones, and cyber weapons. See, for example, David Koplow, *Death by Moderation: The U.S. Military’s Quest for Useable Weapons*, Cambridge University Press, Cambridge, 2009.

sified, at least in certain instances. At the same time, it is often only in the context of specific applications that certain kinds of ethical, legal, and societal issues arise.

This juxtaposition raises a dilemma that is unique to environments in which classified research is conducted—how to coordinate research in such environments when there may be different levels of secrecy associated with the research, and how to establish effective ELSI oversight in these environments. Staying abreast of developments and the associated benefits and risks can also be difficult for policy makers.

For example, certain neuroscience research is classified—and as noted in Chapter 2, even discussion of the ethics underlying such research may be classified. How can such work be reviewed? What is the appeals process for challenging classification designations that may have been assigned inappropriately?

Compartmented (special access) research is especially problematic. The DOD defines a special access program (SAP) as one involving “a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.”¹⁹ Access to SAPs for an agency’s senior leadership is an essential element of agency oversight, which would be diminished if “freelancing” on the part of agency staff is permitted.

Classified research raises a variety of ethical, legal, and societal issues. By assumption, classification means that the research in question is not subject to peer review from the broad scientific community, and thus those doing the research cannot benefit from input and criticism from that broad community. Limiting such input increases the likelihood that erroneous or incomplete results obtained in classified research will not be identified as quickly. Furthermore, classified research is often not directly relevant to helping the broader community address its research problems.

Other issues arise with restrictions on the involvement of non-U.S. citizens, such as foreign students in U.S. universities. Such restrictions generally arise with U.S. export control laws, which can regard the education of certain foreign students in certain disciplines as comparable to the actual export of technologies associated with those disciplines. Again, such restrictions prevent the research from benefiting from the largest possible talent pool.

These comments are not meant to imply that classified research is unnecessary or somehow wrong simply by virtue of its classification. But they do point out that there are downsides to classified research that must be taken into account in supporting such work.

¹⁹ See <http://www.dtic.mil/whs/directives/corres/pdf/520507p.pdf>.

Some questions that might be asked of classified programs include the following:

- How can research in a classified environment be reviewed for ELSI purposes?
- What is the appeals process for challenging classification designations that may have been assigned inappropriately? This question assumes that someone with the appropriate clearance would initiate the appeal. Otherwise, one could not know enough to make the challenge.

5.2.8 Opportunity Costs

Opportunity cost acknowledges the reality that resources (time, talent, money) are finite, and that not all valuable R&D can be conducted. Some considerations include the following:

- How should the value of an R&D effort be ascertained? Some approaches to valuation are quantitative and easily understood—how many lives or how many dollars might be saved by the effort in question? In other cases, it is not clear how to assign or to calculate value—how valuable is an increase in the probability that a given terrorist plot might be detected?
- Why is the R&D effort proposed more valuable than another effort whose cost and likelihood of success are comparable? For example, a program to reduce the cost of generating electricity for deployed forces at the end of a long supply chain may have to be weighed against a program to lighten the weight of body armor. On what basis should one program be chosen over another?
- How and to what extent does U.S. military effort in a selected R&D problem domain signal to adversaries that this domain may be a promising one for military applications?

5.2.9 Sources of Insight from Chapter 4

Chapter 4 describes a number of different possible sources of ELSI insight relevant to considering the impact of R&D on new technologies in a military context, including philosophical ethics and various disciplinary approaches to ethics; international law; sociology, anthropology, and psychology; scientific framing of research problems; the precautionary principle and cost-benefit analysis; and risk communication. Depending on the particular research effort at hand, one or more of these sources of insight might be regarded as a crosscutting approach offering questions relevant to decision making about how to proceed.

5.3 AN EXAMPLE OF USING THE FRAMEWORK

To show how the framework described above might be used in practice, the committee starts with a hypothetical scenario involving the need for decision making about R&D in a military context and then illustrates how the ELSI-related questions and thematic concerns raised in the sections above on stakeholders (Section 5.1) and crosscutting themes (Section 5.2) might apply.

5.3.1 A Hypothetical Scenario for Analysis

A hypothetical research scenario is as follows:

Josie Director has received a preliminary inquiry, with some supporting and confidential data, from a well-respected researcher who specializes in enhancing work performance in high-stress situations. The researcher believes that the data demonstrate that the drug compound he is testing will enable persons to stay awake and on task for up to a week—7 days and nights. The data show no detrimental effects once the administration of the drug ends. Director's research portfolio focuses on performance enhancement under extremely stressful battlefield conditions. She has recently been involved in a high-level meeting where operations indicated the need for an intervention that could improve the capability of small groups of troops to fight and hold on in difficult terrain where reinforcements are not available.

How might Director respond to the researcher's preliminary inquiry?

5.3.2 A Process for Identifying Ethical, Legal, and Societal Issues

The underlying premise of this report is that Josie Director is a scientifically knowledgeable and well-intentioned research director within a DOD science agency who is motivated to advance the frontiers of knowledge in the interests of U.S. national security and is also concerned about the ELSI dimensions of the work that she supports.

In this context, the framework offered in this report provides advice for Director if she wants to explore the latter concerns. The operative question is the extent and nature of the commonality, if any, between the technology in question and its application and other technologies raising ELSI concerns. Such characteristics include technological complexities and uncertainties as well as societal sensitivities about the technology and its application. There is considerable complexity and uncertainty with respect to the development and use of this technology, and about its long-term implications. Societal groups may be sensitive about administration of this type of medication in the circumstances in which it would be used, as well as about its likely broader penetration in society. These factors

mean that ethical principles and expertise from a number of sources, including social science expertise, may be helpful in formulating a course of action.

At the highest level of abstraction, advice in the National Academy of Engineering's workshop report *Ethics Education and Scientific and Engineering Research: What's Been Learned? What Should Be Done?*²⁰ provides some general top-level guidance for what it means to "consider the ethics of doing scientific research." That report identifies a number of useful steps:

- Framing the problem, including ethical dimensions and issues; recognizing it is an iterative process;
- Soliciting advice and opinions in the problem development phase and throughout the process as needed; developing communications strategies;
- Identifying relevant stakeholders and socio-technical systems; collecting relevant data about them;
- Understanding and evaluating relevant stakeholder perspectives;
- Identifying value conflicts;
- Constructing viable alternative courses of action or solutions and identifying constraints;
- Assessing alternatives in terms of consequences, public defensibility, institutional barriers, and so on;
- Engaging in reasoned dialogue or negotiations; and
- Revising options, plans, or actions.

Depending on the stakes and the nature of the decision required of Director, she might pursue these steps to varying degrees. For example, while she would not want to encourage submitting a proposal highly unlikely to be funded, a decision regarding whether to encourage a researcher to submit a full proposal has lower stakes than one regarding whether to fund the proposal. Because it is assumed that Director is a well-intentioned manager who wishes to proceed in an ELSI-responsible manner, she will use her best judgment about how far to carry any of these steps and whether or not any of these steps can be carried out in parallel with a decision or must be executed serially before a decision is made.

²⁰ National Academy of Engineering, *Ethics Education and Scientific and Engineering Research: What's Been Learned? What Should Be Done? Summary of a Workshop*, Rachele Hollander and Carol R. Arenberg, eds., The National Academies Press, Washington, D.C., 2009.

Framing the Problem

The scenario indicates that “Director’s research portfolio focuses on performance enhancement under extremely stressful battlefield conditions.” The portfolio contains a variety of kinds of projects, ranging from management strategies to bolster performance in small groups under stress, to new technologies to enable more timely and accurate communications, to administration of drugs such as mood stabilizers as well as performance enhancers. Questions arise in all of these modalities concerning effectiveness, negative side effects, and spillover. Director has not previously considered creating a portfolio component devoted specifically to experimental performance enhancement.

As a starting point for her framing of the problem, she might consider the four elements outlined in Box 5.1 that are often used to analyze the ethics of an action (or policy). Although there is no formulaic method for taking these elements into account, a serious consideration of the ethics of a given action will generally account for all of them. Alternative actions (including doing nothing) are likely to fare differently when these elements are taken into account, and an assessment of the various elements may well help a decision maker to compare the alternatives systematically. Revisiting these elements allows for reconsideration of prior decisions.

Soliciting Advice; Developing Communications Strategies

To go forward, Director might speak with trusted advisors and experts or construct an informal advisory group to provide background guidance in developing an options paper outlining what this proposal might consist of and accomplish. The paper could include identification and analysis of the ELSI questions that should be addressed in a decision to proceed, and of the societal concerns that may arise from undertaking such a program, as well as from its results. It should also outline a communications strategy for the effort. Her superiors and advisors can review and respond, and the document that results can be used to guide the effort.

The role of public communication often goes unaddressed in efforts to develop innovative technologies. Many times, experimenters and innovators regard public communication as something to try to avoid. This might happen because of a desire to protect intellectual property or from a fear of public response. Yet this type of effort can pay large benefits in garnering public support and also in forestalling public panic or fear or calls for stopping the effort. It can also pay benefits in forcing supporters of a technological innovation to confront associated problems that they would otherwise overlook.

Box 5.1 An Approach to Help Compare the Ethics of Different Policies or Actions

Decision makers must often make judgments about the ethics of different policies or actions. Four important standards or elements for analyzing the ethics of an action or policy include the following:

- *The foreseeable good and bad consequences of performing an action compared to alternative actions, including doing nothing.* The qualifier “foreseeable” is necessary because by definition it is impossible to know all possible consequences until the end of time. But what counts as foreseeable depends on the probabilities of different consequences. It is also important to consider the values of different consequences. The values can be based on widely accepted, common human values such as the promotion of life, happiness, health, abilities, security, knowledge, freedom, opportunities, and resources. Of course, the weight of these various values will vary among people to some extent, but all rational people share these values to some degree when it comes to themselves and the people they care about.
 - *Relevant duties and rights.* Under what circumstances should a duty or right be overridden? Duties and rights often arise from one’s designated roles—duties as an engineer, as a soldier, as a parent, as a human being, and so on. Here one needs to be concerned about setting precedents for future actions, particularly with respect to violations of rights and duties.
 - *Assignment of responsibilities.* People should know who is responsible for what. Thus, for example, actions that create moral hazards should be avoided if possible. Whistle blowers need protection. Avoiding these hazards and protecting whistleblowers allow people to fulfill their responsibilities.
 - *Justice.* Roughly, this criterion asks whether taking the action in question is fair to all relevant parties when all aspects of the situation are considered. If not, to whom is the action unfair and in what ways is it unfair?

These four elements cannot be considered or compared in an algorithmic fashion. But they provide an approach for systematically understanding similarities and differences in competing ethical claims, and they call attention to aspects of ethical action that have to be considered in justifying any given action or policy and when comparing a possible action with alternative actions (including doing nothing).

Identifying Stakeholders and Systems; Collecting Data

In the broadest sense, the stakeholders in this hypothetical case include those involved in and affected by the biomedical system of the United States. More particularly and directly, there is the entire hierarchy of the armed forces. Most directly, there are the men and women who are members of the groups in which the interventions would be tested and

implemented. If there are to be initial small-scale clinical trials, these may involve civilian volunteers and the staff administering the experiment.

If a decision is made to proceed, data at issue here include evidence of safety and effectiveness (or lack thereof), negative or positive side effects, and spillover or the potential for it (both positive and negative). A communication campaign could develop useful data about the priorities for drug design for various populations as well as issues that need attention as drug use spreads beyond the target group.

Understanding and Evaluating Stakeholder Perspectives

A communications strategy can have an important payoff in collecting data about the reactions of different stakeholder groups—from the most general level, including patient advocacy and family groups, to military veterans, as well as active members at various levels of the military hierarchy. Civilian sectors such as the sports industry and the transportation industry might also be consulted. The results of the R&D could provide interesting information both for drug design and for implementation of trials for the drug's use. The response of these stakeholders to the identification and assessment of ethical issues would also be useful, as the next section suggests.

Identifying Value Conflicts

People have given human enhancement technologies a mixed reception. Although there is little controversy about therapeutic interventions intended to overcome disease or disability, such is not the case for the wide range of interventions to bolster abilities and performance. In these cases, people are concerned that the enhancements might contribute to inequities between populations and that they might lend themselves to abuse. Performance-enhancing drugs might also spread into many different sectors of society, with uncertain implications. On the other side is the potential for enhancing performance and, in certain instances, limiting death and injury as a result. From this perspective, delay in development and use of these drugs for U.S. troops on the battlefield might be placing them at significant risk.

Questions concerning benefit and equity have been central in biomedical ethics, which asks if particular ethical principles can be satisfied and how they can be satisfied or reconciled in particular settings. If they can be, the focus can turn to how such research should be done to satisfy the principles—with what populations and protections, for whose benefit, and at what costs.

Constructing Viable Alternative Courses of Action; Identifying Constraints

Director has at least several viable alternatives to consider. She has already developed an active program to improve troop management as well as communications between troop members and between the members and other responsible military personnel—a program that is paying dividends on the battlefield. Is the likely benefit from augmenting her program to include the proposed new area worth the diversion of investment from these other areas? What information would help to address this question? What values need to be considered?

Assessing Consequences, Public Defensibility, and Institutional Barriers

There are ways for Director to test her moral intuitions about the activities she is supporting and the one she has under consideration. She can ask herself what guidance her colleagues or profession might provide. She can consult an ethics officer or the office of the general counsel in her organization. (There may not be an ethics officer, but legal advice is almost certainly available.) She can ask about potential harms, as noted above and taken up again below. She can ask whether she could comfortably defend the additional activities publicly and whether, should harm come to her as a result of one of these activities, she would still think it was good to have supported it.²¹

Undertaking a research program to augment human performance by using drugs raises ethical questions about the potential benefits, risks, and costs. Evidence of effectiveness is not beyond dispute, and there is considerable evidence that administration of certain drugs can lead to a variety of abuses. Even without abuse, a major area for concern is the equity implications in a system where availability may be based on ability to pay. Thus, the virtues of performance enhancement, in uneven expansion to the wealthy, may exacerbate inequalities. Further, dystopian fiction has long made a vice of the virtue of such interventions—pointing out that they may become required rather than elected.

On the other side, enhancements for certain limited purposes may receive a more positive reception, particularly if they can be shown to preserve lives and lower injury. If this research is under consideration in military agencies, institutional barriers may be low. Should the decision of this program director about whether or not to proceed take account of

²¹ Daniel A. Vallero, citing M. Davis, in Google e-book, “Biomedical Ethics for Engineers: Ethics and Decision Making in Biomedical and Biosystems Engineering,” April 1, 2011, Academic Press, Waltham, Mass., p. 339.

the broader societal concerns, or should she set them aside? Surveys of her advisors, superiors, and segments of the broader public may provide interesting results that she can use to inform her decision. Openness about the research could provide some evidence as to whether the program has or can gain public acceptability.

Biomedical ethics identifies significant ethical questions that will arise with the administration of an experimental drug to enhance performance in any setting, even away from the battlefield. Director and her advisors should consider the overarching principles from biomedical ethics—beneficence, nonmaleficence, justice, and respect for autonomy—as well as the rules of procedure intended to implement those principles. Application of these principles and procedures may result in a finding that it would be premature to proceed with use of this experimental intervention in battlefield contexts until further research results are available. Respect for autonomy and the associated requirements for informed consent would also have to receive special attention when drug testing moves to those contexts, in which standard voluntary informed consent will not be available, although it is possible that an acceptable facsimile can be created.

Engaging in Dialogue

If Director decides to proceed, she may be well served to initiate dialogues with the various stakeholders as noted above. These discussions may change the research design and implementation and thus be likely to lead to different outcomes.

Revising Plans

Proceeding through the set of deliberations outlined above is likely to have resulted in various revisions to the decision as to whether and how to proceed. As further questions and issues arise, Director should revisit the previous steps and revise the effort(s) accordingly.

5.3.3 Questions Related to Stakeholders and Crosscutting Themes

As for the ELSI content that Director's analysis may uncover, the questions in the "Stakeholders" and "Crosscutting Themes" sections above, perhaps in modified form, are relevant to issues that may emerge. The approach taken in the present section describes the parties that have a stake, either direct or indirect, in the treatment of ethical, legal, and societal issues, and it poses questions that might be relevant to these stakeholders. It then identifies some themes that arise for many or all

of these stakeholders and raises related questions to suggest some ways to use the framework productively in identifying and assessing ethical, legal, and societal issues.

The issues range from those involving persons directly connected to the conduct of research, to those that are distant, such as nonmilitary users and organizations and even nations. The discussion that follows extracts from the material in the preceding sections those questions that seem of most relevance to Director's circumstances.

Again, the working assumption for understanding the discussion above is that Director is a well-intentioned manager who wishes to proceed in an ELSI-responsible manner consistent with her responsibilities for advancing science and technology for national security purposes. She understands that exploring ethical, legal, and societal issues is a potentially unbounded enterprise, and that she is responsible for exercising her best judgment in determining how far to carry such exploration. She recognizes that exploring ethical, legal, and societal issues is often best done in parallel with the conduct of research, but that some level of preliminary exploration may be necessary to make such a determination.

Stakeholders

Research Performers, Subjects, and Users

Using the bioethical principles from the Belmont report (described in Chapter 4), Director would examine issues of beneficence, interpreted as maximizing benefits and minimizing harms. She might ask:

- What benefits and harms can arise for research subjects and performers? What are the costs and risks, and the potential benefits to military users and to society at large? How and to what extent might this application affect future generations? Are changes to military operations likely to arise, and how would they be accommodated? In the context of the drug compound in question, she might ask what it means to say "use of the drug exhibits no detrimental effects." What specifically are the detrimental effects for which evidence was sought? How long was the drug used and in what dosages? Why was it possible to rule out detrimental effects after long-term use? How might use of the drug affect the logistics chain needed to support soldiers who use the drug? For example, will they need to eat more food and consume more water when on the drug?
- Are adversaries likely to benefit from the results? How, if at all, could the drug be kept away from adversaries? Is U.S. military operation better off if the United States and its adversaries have the drug? Why or why not?

- How should benefits and harms to U.S. and other stakeholder groups be determined, aggregated, and weighed and compared?
- Learning what the benefits may be sometimes requires exposing stakeholders to some harm or risk of harm. How should learning about possible benefits be weighed against actual or possible harm?

Another Belmont report principle requires respect for persons. Director would also have to consider how voluntary, informed consent would be obtained in trials or other circumstances where this intervention might be administered.

- If parties directly involved in such research are members of the U.S. armed forces, they could have an obligation to obey legal orders to participate in the research. Those giving orders would then have a conflict with the duty to provide for voluntary informed consent. If the commanding officers did not give an order, there would not be a conflict, but that might interfere with good research design.
- If the circumstances do not allow voluntary, informed consent, who, if anyone, will speak for the best interests of those parties? How should those speaking for the subjects or participants identify, assess, and weigh these interests?

The principle of justice suggests that the benefits and burdens associated with R&D should be fairly distributed.

- On what basis are specific parties or groups of parties selected for direct involvement in the research? Does the selection of these groups satisfy concerns for fair distribution of benefits and burdens? Should the compound be tested only in frontline soldiers? Only in ground soldiers (versus pilots or sailors)? Only in officers? Only in enlisted personnel? These different groups have different responsibilities in combat, and the drug might differentially affect abilities to execute such responsibilities.
- How and to what extent, if at all, do national security considerations demand that certain groups (e.g., warfighters) accept an exceptional or a higher level of risk than that accepted by other groups (e.g., civilians)? Does higher potential benefit justify increased risk?
- How and to what extent, if at all, should new knowledge derived from the research in question be subject to restrictions on distribution? Should it, for example, be kept from certain allies or the rest of the world? Should it be restricted from public distribution? If so, would the reasons withstand public scrutiny?

Actual use of the drug compound resulting from the research in question might raise other ethical, legal, and societal issues. But even though any need to address those issues is contingent on the success of the research, Director may wish to consider these issues at least in a preliminary fashion, taking into account the type, likelihood, and extent of these issues.

- What might the nature of the impact on users be? For example, how might the use of performance-enhancing drugs affect group cohesiveness? Under what circumstances, if any, might military users of the compound continue to have access to the compound once they are no longer directly participating in combat activities or have returned to civilian life?
- What, if any, could be the longer-term impacts on users? Such an inquiry could be addressed very broadly, but what is the appropriate scope of the inquiry for Director to consider? The inquiry is most relevant when the nature and the extent of potential risks and harms are greater than is apparent here. But given societal concerns about enhancement drugs, the benefits of considering this potential issue may outweigh the costs.
- Might an enhancement of the type being considered lead to heightening the stress that warfighters are under, for example by extending the period of time in which they are left in a battle zone?

Adversaries

The framework discussed in this chapter raises a set of questions about ethical issues that might be associated with the adoption of a technology or application by adversaries. In the case of the research posited in the scenario above, the questions do not appear to be grave ones. Is it likely that adversaries could or would easily adopt this innovation or develop countermeasures? Since the application does not have a directly harmful effect on adversaries, the answer to this question seems likely to be negative or at least of relatively trivial consequence. Similarly, it seems unlikely that the United States would regard an adversary's pursuit of this research to be unethical, or that U.S. pursuit would have negative consequences for adversary behavior and perceptions or propaganda against the United States. The answer to the question of whether other non-adversarial countries might pursue this research also seems likely to be negative. If they did pursue it, the United States would likely be able to adopt it easily.

Civilian Users, in the United States and Elsewhere

There is a strong likelihood that a performance-enhancing drug such as the one Director's researcher would like to develop would be perceived as having benefits in a wide variety of applications. People often want to stay awake and alert and often find themselves in contexts where their ability to perform well is highly valuable and valued. Pressures to use the drug, and inequities in its availability, are likely.

A broader social conversation about the merits of investing in research on drug-based or drug-induced performance enhancement could be beneficial. What role might or should Director play in encouraging such a conversation? A wide variety of issues different from those pertinent to military contexts are likely to arise, including issues of access (which commercial companies might profit from government efforts to develop the application), accountability (public accountability regimes of private-sector companies differ from those of the government), and adoption of technologies by other nations, adversaries as well as allies, after commercialization (such uses may raise concerns very different from those arising in military situations).

Organizations

Director is concerned about enhancing performance, and she recognizes that this goal must take organizational as well as individual effectiveness into account. The introduction of this technology can have significant impacts on practices, procedures, and lines of authority in military organizations. Relevant questions may include the following:

- How and to what extent, if at all, could the application in question influence or change traditional structures and mechanisms of accountability and responsibility for its use? Could it drive certain kinds of battlefield decision making to lower ranks in the military hierarchy? How will the organization react to such tendencies? How, if at all, will accountability for the use of the application in question be maintained? Conversely, might the application make it less likely for someone in the lower ranks to raise questions about ethical use?

- Military organizations often place great value on personal fortitude and endurance in combat. How and to what extent, if at all, could the use of a performance-enhancing drug by soldiers on the battlefield change such valuation?

- Promotions in many military organizations are sometimes based on command opportunities. How and to what extent, if any, could the use of an enhancement drug change command structures? For example, might soldiers' reduced need for sleep mean that units could be smaller? How

might promotion opportunities be affected if commanders commanded smaller units?

Crosscutting Themes

Director can consider whether the crosscutting themes in the framework apply in the case of the proposed research on an enhancement technology. The themes are scale, humanity, unanticipated military uses, technological imperfections, crossover to civilian use, changing ethical standards, ELSI considerations in a classified environment, and opportunity costs. Although some of these issues are discussed above, particular aspects as they arise in some of these thematic areas are worth highlighting. (The discussion below omits mention of unanticipated military uses and changing ethical standards, illustrating the point that not all question categories in the framework are necessarily applicable.)

Scale

Large-scale deployment of the type of enhancement in question may have consequences that are difficult to predict. This possibility may increase the ethical difficulties of doing a cost or risk benefit analysis going beyond the consequences to research subjects or experimental deployment. Will deployment increase costs to segments of society that do not receive the benefits? Is cheap access to the enhancement beneficial? If widespread deployment creates unexpected harms, can the performance-enhancing drug be recalled?

Humanity

Enhancement technologies seem often to raise ethical issues about what it means to be human. In a military context, might enhanced performance lead to decreased empathy and less group adhesion or solidarity?

Technological Imperfections

How much experimental iteration should occur before an innovation can justifiably be used in an operational context? What are the safety and efficacy criteria? Given bodily intrusion, should these standards be higher than those for weapons or other technological innovations?

Crossovers to Civilian Use

How might the drug in question be used by civilians? How do the risks of using the drug vary in the population at large? What would the

drug cost? If there is a limited supply of the drug, which civilians should receive the drug first?

ELSI Considerations in a Classified Environment

Director might be faced with considerations about whether certain neuroscience experimentation for purposes of human enhancement would or should be classified. Were the research to require classification, the questions of ethics in the research and deployment process would be complicated by secrecy requirements. She would need to be satisfied that agency procedures and oversight were sufficient to justify the classification and assure an ethical research process. The process would also affect her relationship to the research performer, who would have to adhere to secrecy restrictions. Community feedback for improvements would also be greatly limited if not totally unavailable. Although limiting access to the results of the research on a performance-enhancing drug has benefits as well as negative implications, the potential for public outcry should problems arise or security be breached may be greater.

Opportunity Costs

For Director, supporting the proposed research endeavor means that others will not be supported. Valuation of research options is never easy. Within the frame of a program to enhance battlefield performance, Director needs to consider and weigh her current priorities with and without this new possibility. Advice from a variety of sources can help in this assessment.

5.3.4 Developing a Future Course of Action

Director can use the framework offered in this report to identify ethical concerns and relevant questions associated with each stakeholder. She can use this knowledge to determine how and to what extent, if any, a program or project might be modified—or in extreme cases abandoned—because of ELSI concerns. The framework does not substitute for other processes and procedures that may be applicable for other reasons such as legal requirements. As she gains more experience with identifying and assessing ethical and societal issues, Director may well add to the framework and incorporate it into a standard procedure that can last throughout the lifetime of a given program.

What actions might emerge from the use of the analysis described above? The space of possible actions is large. For example, Director could:

- Decide that ethical questions as well as insufficiencies in the data and demonstrable potential mean that she should not encourage proceeding;
- Encourage research on the broader social and ethical implications of developing drugs with these characteristics;
- Examine the broader contexts in which such a drug is likely to be used;
- Involve operations in testing the intervention in battlefield conditions;
- Encourage the researcher to proceed with a limited effort, involving further testing on a larger population while continuing to monitor the previous subjects; and/or
- Encourage the researcher to submit a proposal to continue and expand the effort, without specifically raising ethical considerations.

Several of these options can be pursued at the same time and, undoubtedly, there are other options for proceeding as well. But the most important feature of this list is that there are more than two options—that is, Director has choices other than ignoring ethical, legal, and societal issues entirely or discouraging the researcher entirely.

Again, the working assumption for understanding the discussion below is that Director is a well-intentioned manager who wishes to proceed in an ELSI-responsible manner consistent with her responsibilities for advancing science and technology for national security purposes. She understands that exploring ethical, legal, and societal issues is a potentially unbounded enterprise, and that she is responsible for exercising her best judgment in determining how far to carry such exploration. As before, she recognizes that exploring ethical, legal, and societal issues is often best done in parallel with the conduct of research, but some level of preliminary exploration may be necessary to make such a determination.

5.4 THE FRAMEWORK IN CONTEXT

5.4.1 A Summary of the Framework's Questions

This section pulls out of the “Stakeholders” and “Crosscutting Themes” sections all of the questions posed and discussed in the framework. (In the interest of brevity, explanatory material such as examples is omitted. Readers should refer to the sections above for such material.)

Questions of Relevance by Stakeholder

Researchers (and Those Otherwise Associated with Research)

- Beneficence

—What defines “benefit” and “harm”? (Note that a risk of harm is not necessarily the same thing as harm.) How can an R&D effort benefit or harm research subjects? The investigator? Society at large?

—When R&D is being conducted for applications that are intended to harm an adversary, how can the nature and extent of harm be ascertained in research? (Note that there are many kinds of harm that may be at issue.)

—How do the definitions of “benefit” and “harm” differ when different stakeholders are involved?

—How should benefits and harms to different stakeholder groups be determined, aggregated, and compared?

—How should learning about possible benefits be weighed against actual or possible harm?

- Respect for persons

—What constitutes genuine informed consent when information derived from possibly sensitive intelligence sources is part of a threat assessment?

—If parties directly involved in research related to a particular application are members of the U.S. armed forces, how and to what extent—if any—is there a conflict between their obligation to obey legal orders and their provision of informed consent on a voluntary basis? Have undue inducements been offered to persuade individuals to “volunteer”? What counts as an “undue” inducement?

—Who, if anyone, will speak for the best interests of parties that are not capable of providing informed consent? How should such concerns be identified, assessed, and ultimately weighed?

- Justice

—On what basis are specific parties or groups of parties selected for direct involvement in a research effort? For example, why is one group rather than another chosen to be the pool of research subjects? Why is one geographical location rather than another the choice for situating a potentially dangerous research facility?

—How and to what extent, if at all, do national security considerations demand that certain groups (e.g., warfighters) accept

an exceptional or a higher level of risk than that accepted by or imposed on other groups (e.g., civilians)?

—How and to what extent, if at all, should new knowledge derived from research be subject to restrictions on distribution?

Users of an Application

- What could be the nature of the impact, if any, on users of an application?
- What could be the cumulative impact, if any, on users of an application?
- What could be the long-term impact, if any, on users of an application?

Adversaries

- What, if any, is the nature of the direct impact of use of an application against adversaries?
- How and to what extent can the application's impact be reversed?
- How do considerations of symmetry apply? That is, what are the ELSI implications of an adversary pursuing the same technology development path as the United States?
- In the long term, what is the impact of an application on adversary behavior and perceptions?

—How and to what extent could an adversary develop similar capabilities? What is the time scale on which an adversary could do so? How could an adversary use these capabilities? What advantages could an adversary gain from using these capabilities free of legal and ethical constraints?

—What countermeasures might an adversary take to negate the advantages conferred by the application in question? How long would it take for the adversary to obtain those countermeasures? How, if at all, could the developed countermeasure be worse in some way from an ethical standpoint than the application itself?

—How could the application affect the adversary's perception of the United States?

—What, if any, could be the application's effect on deterrence?

—What effect, if any, could U.S. restraint in pursuing a particular application have on inducing an adversary to exercise similar restraint?

—What, if any, opportunities for adversary propaganda could an application enable or facilitate?

Nonmilitary Users

- Law enforcement

—If the military application in question were deployed to support law enforcement operations, how and to what extent, if any, could such deployment raise ethical, legal, and societal issues that do not arise in the military context?

- Commerce

—How and to what extent, if any, could a commercial adaptation of a military application in question raise ethical, legal, and societal issues that do not arise in the military context?

- The general public

—How and to what extent could adaptations of a military application be used by ordinary citizens? What are the ELSI implications of such use?

Organizations

- How and to what extent, if at all, could a new military application influence or change traditional structures and mechanisms of accountability and responsibility for its use? How will the organization react to such tendencies? How, if at all, will accountability for the use of the application in question be maintained? Conversely, might the application make it less likely for someone in the lower ranks to raise questions about ethical use?

- Military organizations often place great value on personal bravery in combat. How and to what extent, if at all, could a technological application used in combat change such valuation?

- Promotions in many military organizations are sometimes based on command opportunities. How and to what extent, if any, could an application change command structures?

Noncombatants

- How and to what extent could an application affect noncombatants on and off the battlefield?

- How might the public at large perceive a given application?

- How and to what extent could an application affect future generations? And what might be the effects of such operation on those targeted by the application?

- How and to what extent could the operation of an application—especially large-scale operations—harm the environment?

Other Nations

- What, if any, could be the impact of a new military technology or application on political solidarity with the United States?
- How, if at all, could the technology or application raise questions about the strength of U.S. commitments to other nations or allies?
- What could be the impact, if any, on U.S. reluctance to share a technology or application with its allies?
- How, if at all, could a technology or application affect the willingness of allies and nonaligned nations to participate in coalition efforts with the United States if the latter uses this technology?
- How and to what extent, if any, could U.S. restraint in pursuing a new military application induce other nations to exercise similar restraint?
- How and to what extent, if any, could an application help to compromise human rights if used by another nation on its own citizens?

Questions of Relevance by Crosscutting Issue

Scale

- Societal scope
 - How and to what extent, if any, could a change in the scale of deployment or use of a technology or application change an ethical calculation?
 - How and to what extent, if any, are the costs of using a particular application transferred from its immediate users to other entities?
 - If an application becomes successful because of the increased functionality it affords to its users and such functionality becomes essential for individuals participating in society, how and to what extent, if any, can the costs of obtaining an essential application be made broadly affordable so that all individuals can obtain its benefits equally?
- Degree of harm
 - How and to what extent, if any, does the degree of inadvertent or undesirable harm compare to the benefits obtained from using that application?

- The nature of the activity
 - How does the scale of ethical, legal, and societal issues differ along the continuum from basic research to use of an application? How do the stakeholders and their interests change?
- Timing considerations
 - What are the ELSI considerations in weighing short-term benefits against long-term costs, and how does the scale of such benefits and costs affect these considerations?

Humanity

- How and to what extent, if at all, does a new military application compromise something essential about being human? How and to what extent, if at all, might users believe that the application is unethical?
 - How and to what extent, if at all, is the application invasive of the human body or mind?
 - How and to what extent, if at all, could use of an application tread on religiously or culturally sensitive issues?
 - Does a technology threaten to cede control of combat capabilities to nonhuman systems to an unacceptable degree?

Technological Imperfections

- Who decides the appropriate safety requirements associated with a new application?
 - On what basis are such decisions made?
 - What, if any, are the tradeoffs between an application's functionality or use and the safety requirements imposed on it?

Unanticipated Military Uses

- What military uses are possible for the application or technology in question that go beyond the stated concepts of operation? What are the ELSI implications of such uses?

Crossovers to Civilian Use

- How and to what extent, if any, could civilian-oriented adaptations of military applications made widely available to citizens raise ethical and societal issues that do not arise in the military context?

- How fast should such military-to-civilian transfers of applications be made? What safeguards should be put into place before they are made? How should such safeguards vary with the technology involved?

Changing Ethical Standards

- If an application is intended to address a military issue that previously had to be addressed by humans, what is the minimum standard of performance that the application must meet before it is deemed acceptable for widespread use?
- How and to what extent, if any, does a new application create new ethical obligations to use it in preference to older applications addressing similar problems that may raise ELSI concerns to a greater extent?

ELSI Considerations in a Classified Environment

- How can research in a classified environment be reviewed for ELSI purposes?
- What is the appeals process for challenging classification designations that may have been assigned inappropriately?

Opportunity Costs

- How should the value of an R&D effort be ascertained?
- Why is the R&D effort proposed more valuable than another effort whose cost and likelihood of success are comparable? On what basis should one program be chosen over another?
- How and to what extent does U.S. military effort in a selected R&D problem domain signal to adversaries that this domain may be a promising one for military applications?

Questions of Relevance by Source of Insight

Chapter 4 describes a number of different sources of ELSI insight, and the discussion includes illustrative ELSI-related questions that may be derived from considering each of those sources.

5.4.2 Utility of the Framework

Readers of this report who identify ethical, legal, and societal issues inherent in the above described scenario (Section 5.3.1) that do not derive from use of the framework may be dismayed about that fact. Such dismay would foreshadow material presented in Chapter 6, which argues that a

comprehensive identification of ethical, legal, and societal issues associated with a given technology development is difficult indeed.

Put differently, the framework is itself a starting point for discussion and is not comprehensive. The framework provides some structure for thinking through various ethical, legal, and societal issues, but as the sampling of such issues across various technologies and applications suggests, it is not necessary to treat all issues in the framework as equally important for any given technology or application—judgment is necessary to make the most effective use of the framework. That is, different ethical, legal, and societal issues may come into play or a given ELSI concern may be significant to varying degrees depending on the technology in question. On the other hand, not considering any given element in the framework must itself be a thoughtful and defensible decision rather than a reflexive one—a good and plausible argument must be available as to why that particular element is not relevant.

As decision makers gain more experience with identifying and assessing ethical, legal, and societal issues, it should be expected that the content embedded in the framework will evolve. Years from now, it would be surprising indeed if the questions that policy makers posed regarding ethical and societal issues had not changed at all.

Policy makers might wish to use this framework for new or existing R&D programs or projects. In addition, it may be appropriate to apply this framework when some unanticipated application emerges. One might regard use of this framework as part of an ongoing process that lasts throughout the lifetime of a given program.

The purpose of this framework is not to impose compliance requirements on program managers, but rather to help them to do their jobs better and to help ensure that basic American ethical values are not compromised. The analytical framework is necessarily cast in somewhat broad and abstract terms because it is designed to apply to most R&D programs; consequently, not all questions in the framework will necessarily be relevant to any specific technology or application.

Furthermore, although it may not be likely that a contentious issue identified through this framework will be resolved in a decisive or final manner, this fact is not an adequate rationale for dismissing or ignoring the issues. Honest, well-reasoned analyses are useful to policy makers, even if they might be incomplete, and such analyses can be supplemented or corrected through adaptive processes as additional knowledge is gained over time, as discussed in Chapter 6.

As for the framework itself, the number of stakeholder groups and the number of crosscutting themes described in this chapter are both large, reflecting the breadth of possible technologies whose ethical, legal, and societal consequences must be considered and the large number of inter-

ested parties, as well as the diverse nature of the concerns that any given stakeholder may bring to bear. Indeed, the committee found that attempts to make these lists more concise—in general an effort worthwhile as an analytical goal—would constrain the intended broad applicability of the framework. In part, the framework fills the role of a checklist, a mechanism that is often used to remind decision makers to consider the possible relevance to the project at hand of a wide range of issues that may not be related to each other.

The framework provides information about ethical foundations and approaches that many people and organizations find useful in considering difficult questions about research for technological innovations, without choosing a particular orientation from among them. This approach recognizes that weighting different ethical constraints and opportunities is difficult and does not lend itself to an algorithmic decision-making procedure. Under some set of specific circumstances and technological characteristics, certain criteria may have priority, whereas under a different set of circumstances, different criteria may have priority.

At the level of generality at which this framework is cast, a few caveats are necessary. First, a full consideration of ethical issues sometimes produces a cacophony of methodologies and perspectives that leads to dissonance and controversy. Similarly, “societal” issues range across such a broad range of possibilities that attempts to limit the scope of such issues inevitably generates questions about why this issue or that issue was included or excluded. Third, decision makers will surely face tradeoffs, satisfying no stakeholder fully in any ethically or societally controversial enterprise. Fourth, the framework does not provide a methodology for resolving or settling competing ethical claims, for choosing between ethical theories, or for providing specific answers to ethical questions, although it does call for decision makers to attend to a variety of ethical positions and approaches.

At the same time, the framework does not assume that “anything goes,” and it posits that through deliberation and discussion, it is often possible to identify initial ethical positions that are more well grounded and defensible or less so. Further deliberation and discussion may well lead to evolution in these initial positions and decisions. Because such discussion increases the likelihood that major ethical, legal, and societal concerns will be identified before any given technology R&D program or project gets underway, and casting the initial net broadly rather than narrowly will help to limit ELSI-related surprises, the committee believes that such a discussion is worthwhile as a part of any ELSI assessment.

The framework above is useful primarily for bringing ethical, legal, and societal concerns to the surface that would not otherwise have been apparent to decision makers and program managers. The ELSI-related

questions included within the framework are intended to help decision makers develop useful knowledge on a variety of ethical, legal, and societal issues regarding specific military science and technology programs and projects. The framework was developed to apply to decision making in a U.S. context, although decision makers and program officials in other nations may nonetheless find parts of it useful.

In the end, the use of this framework can only provide input to decision makers, who will have to make judgments about how, if at all, to proceed with a particular R&D program or project, and such judgments should be undertaken after the decision makers have examined the issues posed by the framework rather than before. Different individuals may develop different answers to the various questions raised by the framework about a given technology, but the important aspect of this process is that the questions be asked and that a discussion take place.

This framework does not substitute for other processes and procedures that may be applicable for other reasons. In particular, program managers are obligated to conduct their programs in accordance with applicable law and regulation (such as the Common Rule,²² which sets forth federal policy for the protection of human subjects used in research). Judgments about the compliance of a specific program with applicable laws are beyond the scope of this report, although the report draws on relevant national and international standards in its discussion.

5.4.3 Identifying Fraught Technologies

Not all technologies or applications are equally fraught from an ELSI standpoint. Technologies or applications are likely to be highly fraught if they satisfy one or more of the following attributes:

- A technology or application that is relevant to multiple fields (for example, an enabling technology or application) will almost surely have more ELSI impact in the long run than one whose scope of relevance is narrow.
- A technology or application whose operation has the potential to result in intended or unintended consequences that could cause harm to people on a very large scale is likely to raise more ELSI concerns than one without such potential.
- A technology or application that challenges traditional (and often religious) notions of life and humanity or appears to do so is likely to

²² See <http://www.hhs.gov/ohrp/humansubjects/commonrule/index.html>.

raise more ELSI concerns. Under this heading are some concerns that the Wilson Center report describes as concerns over “nonphysical” harms.²³

A technology or application for which one of these statements is true is worthy of special consideration and effort to understand ELSI concerns, and a technology or application for which more than one is true is even more worthy of such consideration. Examples from history that have all of these attributes in some measure might include genetic engineering and recombinant DNA research, and Chapter 2 highlights the current discussion of what synthetic biology, as a similar kind of research, might produce and how its potential benefits are accompanied by a range of ethical, legal, and societal issues that its proponents have worked hard to address.

5.4.4 Frequently Heard Arguments

Finally, it is helpful to address a number of frequently heard arguments about ethics as they apply to new military technologies. Specifically, one common thread of the arguments discussed below is that they are often made with the intent or desire of cutting off debate or discussion about ethical issues.

- *An argument.* U.S. adversaries are unethical, and so ethics should not be a constraint in using advanced weaponry against them. Moreover, they seek every advantage over the United States that they can obtain, and thus the United States, too, must do the same in any conflict with adversaries.

Response. The United States has publicly stated a commitment to abide by certain constraints in how it engages in conflict regardless of how its adversaries behave; these commitments are embodied in domestic law that criminalizes violations of the Geneva Conventions by the U.S. armed forces, and also by certain treaties that the United States has signed and ratified. The real question is not whether we constrain ourselves ethically but how and under what circumstances, and with what decision-making procedures we do so.

- *An argument.* U.S. adversaries will pursue all technological opportunities that serve their interests, and if the United States doesn't pursue those opportunities as well, it will wind up being at a military disadvantage.

²³ The full report can be found at <http://www.synbioproject.org/process/assets/files/6334/synbio3.pdf>.

Response. From the standpoint of decision makers, there is a world of difference between the possibility that technology X could provide military advantages and a clear demonstration that technology X does provide military advantages in specific and important operational scenarios. That is, the latter provides a proof of principle that technology X is worth a significant investment. This point argues that in some cases, it may make sense to separate decisions about exploring the value of a technology (a preliminary step) from decisions based on demonstrating how it can be used to confer military advantages (a more decisive step), and to make such decisions separately.

- *An argument.* We don't know the significance of technology X, so we *must* work on it in order to understand its implications, and we would be unwise to give up on it without knowing if and how it might have value to the United States.

Response. This argument poses a false choice between cessation of all investigatory work on X and proceeding to work on X without any constraints at all. In fact, there are a variety of choices available in between these two extremes, the most significant of which is something along the lines of "proceed, but carefully." Intermediate choices are addressed in Chapters 4 and 5 and in the recommendations made in Chapter 8.

- *An argument.* Consideration of ethical, legal, and societal issues will slow the innovation process to an unacceptable degree.

Response. Although the argument is surely true in some cases, it is not necessarily true in all cases. For example, it depends on the nature and extent of such consideration. Moreover, a consideration of ethical, legal, and societal issues is hardly the only dimension of the military acquisition process on which that process may be slowed. Finally, a small slowdown in the process up front may in fact be worth the cost if it helps to prevent a subsequent explosion of concern that takes program managers by surprise.

- *An argument.* Research on and development of defensive technologies and applications is morally justified, whereas work on offensive technologies is morally suspect.

Response. The categories of "offensive" and "defensive" technologies are not conceptually clear, because offensive technologies (that is, technologies that can kill or destroy) can be used for defensive purposes, and, similarly, defensive technologies (that is, technologies that prevent or reduce death or destruction) can be used for

offensive purposes. An example of the first is a defender's use of an offensive weapon to destroy an incoming offensive weapon—in this case, the defender uses its offensive weapon to prevent or reduce the death and destruction that the attacker's offensive weapon would otherwise cause. An example of the second is the use of a defensive system to protect an attacker that has launched a first strike—in this case, the attacker's possession of a defensive system enables the attacker to attack without fear of retaliation, thus increasing the likelihood that it will in fact attack. In short, the distinction between the two categories often fails in practice.

It should be stressed here that the responses to the various arguments outlined above are not intended to dismiss out of hand any of the frequently heard arguments. That is, all of the frequently heard arguments described above sometimes have at least a grain of truth that may be worth considering. At the same time, those grains of truth should not be amplified to the point that they render discussion of ELSI considerations illegitimate—the short responses to the frequently heard arguments are intended essentially as points of departure for further dialogue.

6

Going Beyond Initial A Priori Analysis

6.1 UNANTICIPATED IMPACTS

Unanticipated impacts of a given science, technology, or application are a frequent source of ethical, legal, and societal issues; it is therefore important that decision makers and scientists and engineers give consideration to as broad a range of potential impacts as possible. By doing so, scientists and engineers maximize their ability to improve designs in ways that can reduce risks and increase benefits, and decision makers and scientists and engineers can consider how best to engage with citizens in consideration of what technologies to develop and how to deploy and evaluate the applications and their uses.

The analytical framework described in Chapter 5 is based on the idea that undertaking a systematic search for ethical, legal, and societal issues that could come up in the context of a given technology or application will surface more possible issues than if no such search is undertaken. That is, there is value in an a priori consideration of ELSI concerns before a technology or an application is developed. But how might one anticipate ethical, legal, and societal issues associated with unknown applications that may—or may not—lie in the future?

Predictive analysis is arguably the most difficult task in any assessment of ethical, legal, and societal issues. Indeed, it sometimes has overtones of “expecting the unexpected” and identifying issues before they can be known. To be sure, literal talk of anticipating unanticipated ethical, legal, and societal issues is oxymoronic. But the ability to respond quickly to unanticipated issues that do arise can be enhanced by addressing in

advance a wide variety of identified issues, because that exercise provides building blocks out of which responses to unanticipated ethical, legal, and societal issues can be crafted.

Moor argues that

because new technology allows us to perform activities in new ways, situations may arise in which we do not have adequate policies in place to guide us. . . . [Furthermore,] the subtlety of the situation may escape us at least initially, and we will find ourselves in a situation of assessing the matter as consequences unfold. Formulating and justifying new policies is made more complex by the fact that the concepts that we bring to a situation involving policy vacuums may not provide a unique understanding of the situation. The situation may have analogies with different and competing traditional situations. We find ourselves in a conceptual muddle about which way to understand the matter in order to formulate and justify a policy.¹

6.2 LIMITS OF A PRIORI ANALYSIS

6.2.1 The Limited Utility of Technology Forecasting

Anticipating ethical, legal, and societal issues associated with applications that may—or may not—lie in the future should, in principle, be enhanced by good technology forecasting. If the specific trajectory of a given science or technology development were known in advance, anticipating the ethical, legal, and societal implications associated with that trajectory would be little different from anticipating the ethical, legal, and societal implications associated with a known application of that technology.

But as it turns out, it is very difficult to predict trajectories of science or technology development. The history of technology forecasting suggests that inaccurate technology forecasts are the rule rather than the exception—and these inaccuracies are major rather than minor. In very broad terms, a variety of trajectories for any given scientific or technological development are possible. Some unanticipated applications have positive impacts—it had been expected that the most common use of the ARPANET (the forerunner of the Internet) would be the remote use of computer facilities of a university from a second university a long distance away. Instead, the Internet has richly and densely connected people as well as computers. Other unanticipated applications have negative impacts—the introduction of nonlethal weapons into a police force

¹ James H. Moor, “Why We Need Better Ethics for Emerging Technologies,” *Ethics and Information Technology* 7:111-119, 2005.

can result in an increased use of force overall, as noted in Chapter 3. But what a great deal of experience with technology development shows is that unanticipated outcomes are quite common and indeed are more the rule than the exception.

For example, from an initial orientation toward particular military applications, one might consider unanticipated “off-label” military applications or nonmilitary applications. Examples of off-label military applications include the use of timing signals from Global Positioning System satellites to synchronize frequency-hopping communications systems, the use of bulldozers as weapons to bury enemy soldiers in trenches,² and the use of helmets as cooking pots. The primary characteristic of an off-label military application is that the designers of the application did not intend for it to be used that way in practice. Such applications are generally improvised in the field after soldiers have been provided with the technology in question.

In addition, it is often said that the short-term impact of a given technology is overestimated and that the long-term impact is underestimated. Excessive optimism about short-term effects may lead to disillusionment—and as a given technology falls out of favor for its promised applications, pressures will arise to preserve investments already made by considering other applications. Underestimation of long-term effects reflects the substantial difficulties in making predictions with long time horizons—and it is in the long term that many actual real-world consequences that raise ELSI concerns will become manifest.

6.2.2 Sources of Uncertainty in Technology Forecasting

What helps to explain the limited utility of technology forecasting in addressing ethical, legal, and societal issues in advance of their appearance? It is helpful to consider multiple sources of uncertainty in such forecasts.

Unproven Fundamental Science

The fundamental science underlying a proposed application must be sound. From time to time, advanced applications are proposed or suggested when the fundamental underlying science has not yet been proven or, more often, has simply not been adequately developed. In such cases,

² Patrick J. Sloyan, “Iraqis Buried Alive—U.S. Attacked with Bulldozers During Gulf War Ground Attack,” *Newsday*, September 12, 1991, available at <http://community.seattletimes.nwsourc.com/archive/?date=19910912&slug=1305069>.

the applications in question are both speculative and grand in their scope and scale.

As an example, consider the promises of virtually unlimited and free energy made when cold fusion first made the headlines. Martin Fleischmann testified to the U.S. Congress that cold fusion was about “cheaper energy . . . unlimited energy, and energy that may be less destabilizing to our environment.”³ In the same hearing, a senior Administration advisor at the time advocated a development model in which “even before [the] basic science is proven, applied research [would] begin . . . , product developments [would be] undertaken, market research [would be] done, and manufacturing processes [would be] working.” He further argued against “dawdling and waiting” until the science of cold fusion is proven. It is not hard to imagine such thinking applied in a wartime situation when development of a new technology needs to happen rapidly.

Lack of Real-World Viability Despite Technology Proof of Principle

Even when the fundamental science is sound, it is an open question as to whether anything immediately useful can be accomplished with the knowledge discovered. Many important fields of science do not easily lend themselves to practical application, at least not on a time scale shorter than many years. And although there are many definitions of practical application, a necessary if not sufficient condition is that the science can help accomplish a task that at least some elements of society find useful.

In this context, “useful” should be understood as something that some humans value in an absolute rather than a relative sense—that is, a means of accomplishing a task at lower expense and with higher confidence than is possible by another, and thus less useful, means.

An example in this category comes from synthetic biology. The fundamental principles of synthetic biology have been scientifically validated, and some “in-principle” demonstrations have been conducted—cyanobacteria that produce hydrocarbon fuel,⁴ *E. coli* modified to produce amorphadiene, a precursor for the antimalarial drug artemisinin,⁵ and

³ U.S. House Committee on Science, Space, and Technology, “Recent Developments in Fusion Energy Research: Hearing before the Committee on Science, Space, and Technology,” 101st Congress, 1st Session, April 26, 1989.

⁴ Anne M. Ruffing, “Engineered Cyanobacteria: Teaching an Old Bug New Tricks,” *Bioengineer Bug* 2(3):136-149 (citing inventors P.G. Roessler, Y. Chen, B. Liu, and C.N. Dodge, “Secretion of Fatty Acids by Photosynthetic Microorganisms,” U.S. patent application publication number W02009076559A1, Synthetic Genomics, applicant, June 18, 2009).

⁵ Steven A. Benner and A. Michael Sismour, “Synthetic Biology,” *Nature Reviews Genetics* 6(7):533-543, 2005.

E. coli modified to detect arsenic in water.⁶ But none of these demonstrations has yet yielded commercial value, thus illustrating that proof of principle is not the same as marketplace viability. (In a military context, a technology or application does not have to demonstrate commercial value in the same sense, but does need to be “weaponized” to be useful. For example, weaponizing a technology that demonstrates proof of principle may involve making it sufficiently rugged to use in the field, simplifying its operation so that large amounts of training are not necessary to use it, and so on.)

As for certain more futuristic applications, being able to control even a very simple operating organism based on a synthesized genome is today an achievement that strains the current state of the art.⁷ Indeed, in this case, the term “synthesized genome” does not refer to a genome designed from scratch but rather one whose biological functionality is based primarily on the genome of an existing organism (and hence shares many of the same DNA sequences). The work referred to was rightly hailed as a major step forward toward the synthesis of novel and useful life-forms, but it is nevertheless just the first step in a very long journey of scientific discovery. Still, some of those responsible for this achievement write that “the ability to routinely write the software of life will usher in a new era in science, and with it, new products and applications such as advanced biofuels, clean water technology, and new vaccines and medicines.”⁸

Dependence of Technology Advancement on Nontechnical Influences

Scientific progress and technology refinement do not necessarily stop at the point that the first useful application is conceived or implemented. But the pace at which such progress and refinement take place is dependent on many factors other than the science and scientists themselves. Such factors include politics, budgets, the state of the economy, the availability of appropriate human capital, and so on.

To take one example, Moore’s law is often cited as an example of the inexorable development of information technology (in its most basic form, Moore’s law states that the areal density of transistors on a chip increases

⁶ Jennifer Chu, “A Safe and Simple Arsenic Detector” January 25, 2007, *MIT Technology Review*, available at <http://www.technologyreview.com/news/407222/a-safe-and-simple-arsenic-detector/>. Read more at <http://www.ukessays.com/essays/biology/synthetic-biology-and-development-of-biofuels.php#ixzz2KFdcGUeL>.

⁷ Daniel G. Gibson et al., “Creation of a Bacterial Cell Controlled by a Chemically Synthesized Genome,” *Science* 329(5987):52-56, July 2, 2010, available at <http://www.sciencemag.org/content/329/5987/52.full>.

⁸ See <http://www.jcvi.org/cms/research/projects/first-self-replicating-synthetic-bacterial-cell/overview/>.

exponentially with time with a doubling time of 18 months). And indeed that pace of technology advancement has been an important driver/enabler. But no law of nature underlies it, and in fact concerns have been raised in two dimensions. First, fundamental physics *does* limit the physical size of transistors, and thus there is indeed a limit to the areal density of transistors on a chip. Can other high-density technologies be developed to store and process information? Perhaps. But even that question changes the form of Moore's law from one involving the number of transistors on a chip to one involving (for instance) the number of bits on a chip. So the metric of progress must be chosen carefully. And the question of how far into the future Moore's law will hold is an open one.

Second, Moore's law is at least as much an economic statement as a technological statement—the fact that the areal density of transistors has followed an exponential growth curve with a doubling time of 18 months reflects the investments that semiconductor and semiconductor equipment manufacturers have made in new fabrication plants, and they have been able to financially justify such expenditures of capital. If they did not believe that they were capable of extracting appropriate value from such expenditures, they would not have made them in the first place—and the doubling time would no longer be 18 months.⁹

Building on this example, economics is often one of the most unpredictable and powerful influences on technology evolution. If the cost of implementing an application becomes very low because of manufacturing advances (e.g., as described by Moore's law), commodity component markets (a particular concern for IT hardware and software), or other factors, the application may become affordable for uses and users that were not initially anticipated. This is a common trajectory that lowers the barrier to entry for a technology and turns a technology into one that is readily available.

Competitiveness with Respect to Possible Alternatives

A proof of principle is only the first step in developing a viable application—that is, an application that is at least a good or a better way to accomplish a needed task. If there is no other way to accomplish that task, then the path forward is likely to be more straightforward, and perhaps more predictable, simply because there are no alternatives.

But the situation is much more complicated when an application based on new technology must compete with existing or proven alterna-

⁹ David E. Liddle, "The Wider Impact of Moore's Law," *Journal of Solid State Circuits* 11(5):28-30, September 2006, available at <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4785858>.

tives. Compared to the existing alternatives, the new application must perform the task better, or afford the user a wider range of advantages, or be cheaper, or easier to produce, or less environmentally damaging, and so on. If the new application for performing a task affords no advantages over existing ones that perform the same task, there is no compelling reason for anyone to adopt it. When the new application offers only incremental advantages over existing applications, there is often uncertainty about whether those incremental advantages are sufficiently important, although during times of national emergency (such as being in a war), incremental advantages are often sought with less attention to matters such as cost.

If the new application can be shown to be competitive with existing alternatives, it has a chance of being widely adopted. Wide adoption of such an application, in turn, lays a foundation for even more applications to be developed using the underlying technology. But predicting such an outcome, given the large set of ELSI concerns that must be resolved successfully, is thus problematic.

ELSI Acceptability of Anticipated Use

Even when a new application can be shown to be competitive with existing alternatives, it may not succeed when ethical, legal, and societal issues are a concern. For example, an application may be competitive only when certain intangible costs are ignored, and controversy over the magnitude or significance of those costs may emerge. Advocates of the application will argue that those costs are low, or that because they are intangible, they should not be considered at all; opponents of the application will argue the reverse position. Such controversy may well delay or even halt the adoption of an otherwise promising application.

One example is the Active Denial System (ADS), a directed-energy nonlethal weapon first developed in the mid-2000s and designed for keeping humans out of certain areas.¹⁰ The ADS aims at a target such as a human being a beam of microwave energy that causes an intense burning sensation on the human's skin. However, because the beam does not penetrate very far into the skin, it causes little lasting damage (no lasting damage in nearly all cases). The pain is intended to cause the human to turn away and flee the area.

In 2003, a senior U.S. Air Force scientist asserted that the use of the ADS would have averted an incident in which U.S. soldiers in Iraq fired into a crowd that was protesting their presence in the city of Fallujah.¹¹

¹⁰ See <http://www.globalsecurity.org/military/systems/ground/v-mads.htm>.

¹¹ See <http://www.wired.com/dangerroom/2007/08/no-pain-ray-for/>.

The ADS could have been used to force the crowd to disperse. However, the Department of Defense refused to deploy the weapon as late as December 2006, apparently in part because the weapon might have been misconstrued by the public as a device for torture.

A second example is the various lasers that have been considered for use as antipersonnel weapons, as discussed in Chapter 3. Such weapons would have been able to injure (blind) enemy soldiers at long range; furthermore, by inflicting serious injury on enemy soldiers but not killing them, such weapons could have seriously increased the logistical burden on the enemy to care for injured soldiers. However, despite such operational advantages, the United States promulgated policy that prohibited the use of lasers “specifically designed to cause permanent blindness of unenhanced vision”¹² and later signed on to an international treaty banning such use, in part for ethical reasons.

Unanticipated Uses

A given technology that spawns one widely adopted application often spawns others that were entirely unanticipated when the first application was conceived. And the success of these unanticipated uses often depends on the development of other technologies. For example, although lasers were recognized at first for being applicable to communications, such applications were wireless. The use of lasers for fiber-optic communications depended on the availability of low-cost fiber optics, a technology that was for the most part unanticipated when lasers were first invented.

6.3 BROADENING PREDICTIVE ANALYSIS OF ETHICAL, LEGAL, AND SOCIETAL ISSUES

Any one of the several factors described above entails some degree of uncertainty as to outcome. But when the uncertainties associated with all of these factors are compounded, it should not be surprising that in general, long-term predictions about a technology’s effects are not particularly accurate. This observation, along with the potential for unanticipated use mentioned above, is applicable to nearly any kind of new technology.

Technologies that are easily accessible to many parties introduce two additional noteworthy complications. First, increasing the number of parties with access to a technology will increase the number of applications that will come to fruition. Increasing the number of applications that will

¹² See <http://www.defense.gov/releases/release.aspx?releaseid=608>.

be fruitful makes it less likely that any kind of a priori process to anticipate trajectories of technology evolution will anticipate all of them.

Second, increasing the number of parties—especially across international (and thus cultural) lines—increases the likelihood that different ELSI perspectives on a given technology or application will be relevant to any consideration of the ethical, legal, and societal issues. In this context, knowing where important ELSI differences will arise becomes problematic, especially when the process is limited to an analytic process conducted by only a few people with narrow perspectives. Alternative approaches to consider for identifying, anticipating, and addressing ethical, legal, and societal issues include the use of deliberative processes to tap a broad range of perspectives; anticipating governance, a new approach to examining societal dimensions of R&D; and adaptive planning and policy making.

6.3.1 Use of Deliberative Processes

The analytical framework outlined in Chapter 5 speaks to insights that can be obtained through a careful consideration of various domains of possible ethical concern. Thus, it is an important tool for anticipating and predicting ethical, legal, and societal issues that might be associated with the pursuit of a given technology or application. A policy maker faced with deciding about how or whether to proceed in a particular technological direction might examine each of the sources of insight described in Chapter 4 and ask if the particular direction in question might raise relevant ELSI questions in any of them.

But as Chapter 5 points out and the discussion at the outset of the present chapter suggests, that framework cannot be regarded as comprehensive. To improve their capability for anticipating and predicting and to exploit opportunities to gain new insights, policy makers have sometimes turned to deliberative processes that seek to identify a broad range of perspectives and possible stakeholders in discussions of any given issue.

Deliberative processes were described in a 1996 report of the National Research Council entitled *Understanding Risk: Informing Decisions in a Democratic Society*.¹³ The study committee responsible for that report was originally charged with developing an approach to risk analysis structured to enable making better and more broadly acceptable governmental decisions regarding regulatory actions. The report noted that risk characterization involved “complex, value-laden judgments” and required “effective dialogue between technical experts and interested and affected

¹³ National Research Council, *Understanding Risk: Informing Decisions in a Democratic Society*, National Academy Press, Washington D.C., 1996.

citizens who may lack technical expertise, yet have essential information and often hold strong views and substantial power in our democratic society.”

In particular, the 1996 report drew a contrast between analytical and deliberative modes of inquiry as “complementary approaches to gaining knowledge about the world, forming understandings on the basis of knowledge, and reaching agreement among people.” Key to an analytical mode of inquiry was the involvement of an expert community that was capable of answering factual questions. By contrast, a deliberative mode of inquiry emphasizes communication among stakeholders and between stakeholders and policy makers and collective consideration of issues. In the words of the report, “participants in deliberation discuss, ponder, exchange observations and views, reflect upon information and judgments concerning matters of mutual interest, and attempt to persuade each other.” Both modes of inquiry, the report argued, were essential to effective risk characterization.

The 1996 report articulated three separate rationales for broad participation in risk decisions: normative, substantive, and instrumental.

- From a normative standpoint, the principle that government should obtain the consent of the governed drives the idea that citizens have the right to participate meaningfully in public decision making.

- From a substantive standpoint, the report argued that “relevant wisdom is not limited to scientific specialists and public officials and that participation by diverse groups and individuals will provide essential information and insights about a risk situation” and further that “nonspecialists may contribute substantively to risk characterization . . . by identifying aspects of hazards needing analysis, by raising important questions of fact that scientists have not addressed, and by offering knowledge about specific conditions that can contribute more realistic assumptions for risk analysis . . . [and by] help[ing] design decision processes that allow for explicit examination, consideration, and weighing of social, ethical, and political values that cannot be addressed solely by analytic techniques.”

- From an instrumental standpoint, the report argued that “broad public participation may decrease conflict and increase acceptance of or trust in decisions by government agencies” and that “mistrust is often at the root of the conflicts that arise over risk analysis in the United States.” Furthermore, the report said that “providing people an opportunity to learn about the problem, the decision making process, and the expected benefits of a decision may improve the likelihood that they will support the decision” and/or “clear up misunderstandings about the nature of a controversy and the views of various participants. And it may contribute

generally to building trust in the process, with benefits for dealing with similar issues in the future.”

After describing these rationales, the 1996 report went on to argue that deliberative processes could be used to surface a broader range of risks that would not be identified by less inclusive processes, and that these risks could, when necessary, be addressed more formally and rigorously using more traditional analytical means.

Many of the lessons of this 1996 study regarding the value of deliberative processes to risk characterization are applicable to anticipating and identifying ethical, legal, and societal issues associated with new technologies and applications. Indeed, at least the substantive and instrumental rationales can be carried over to the ELSI context directly: non-specialists in the technology or application under consideration may have relevant wisdom, and broad participation in decision making (especially politically controversial decision making) may make the outcome of those decisions more stable.

More recently, Worthington et al. argued that ordinary citizens should have a role in shaping technologies that pervade society, and that they can and should play a role in technology assessment.¹⁴ They further note that in the past two decades, participatory practices have expanded considerably in a number of dimensions, including greater racial and gender inclusivity of the people who constitute the professional workforce in scientific and engineering fields; increased involvement in research by ordinary people (e.g., through citizens collecting data for scientific analysis or through the origination of scientific research projects in citizen concerns); challenges by citizens to the authority of experts and their sponsors; and more frequent emergence of dissidents inside science and engineering fields who challenge research programs backed by industry, government, and scientific institutions.

Broad participation is also relevant because of another reality of decision-making processes—that when potentially controversial issues are addressed, opponents of a particular policy will seek support for their opposition from all plausible sources. Ethical concerns may play into the logic driving their opposition—indeed, opponents of a particular policy may well be more sensitive to and aware of ethical concerns than are the policy’s proponents, who may have used an analytical process that is not sensitive to these positions and perceptions, and sometimes the most

¹⁴ Richard Worthington et al., *Technology Assessment and Public Participation: From TA to pTA*, December 6, 2012, available at <http://ecastnetwork.wordpress.com/technology-assessment-and-public-participation-from-ta-to-pta/>.

salient expression of ethical concerns is the emergence of a political or public controversy.

Rather than resisting or dismissing ethical concerns that opponents raise (even if their stated ethical concerns are not in fact the “real” reasons for their opposition), policy makers can take advantage of the opportunity to gain ethical insights that might otherwise be unavailable. This is not to say that all concerns are necessarily dispositive, but some may be worthy of intellectual effort to address.

On the other hand, ethical, legal, and societal issues are not analogous to most of the risks considered in the 1996 NRC report cited above. In particular, there is no analytical or technical resolution to many ELSI dilemmas—and seeking resolution or consensus with respect to such dilemmas can result in a never-ending debate. Thus, in an ELSI context, deliberative processes should be regarded primarily as a way to surface relevant issues that would not otherwise be revealed, and, second, as a way to gather ideas for possible resolutions to the issues. Deliberative processes also help to educate more people about the technology and the ethical, legal, and societal issues involved. If nothing else, deliberative processes provide a broad range of parties with the opportunity to state their concerns—and reduce the credibility of future claims that they have been entirely left out of any decision making.

Against all of these considerations is one major downside: the possibility—indeed, the likelihood—that deliberative processes will delay the relevant decision-making processes and increase the time it takes for valuable and useful technology to be delivered to troops in the field. Two observations are relevant here.

First, this downside takes on the most significance when the application in question has direct relevance to problems that these troops are facing on an ongoing and frequent basis, but less significance when useful applications lie in the far future.

Second, the use of deliberative processes may help to defuse potential future concerns and possibly head off protracted and politically dangerous controversy in the future that could delay to an even greater extent or even kill promising and useful technologies. Two relevant examples of a failure to anticipate controversy may be the Total Information Awareness program and the Policy Analysis Market program of DARPA (Box 6.1), both of which were abandoned for the ethical controversies they raised—controversies that might have become evident beforehand as a result of deliberative processes aimed at eliciting a wide range of input regarding relevant ethical issues.

Finally, the committee observes that community engagement is sometimes difficult and expensive. Finding expert facilitators of community engagement processes, identifying the appropriate communities, and

Box 6.1 Past DARPA Projects That Have Raised Controversy

The Total Information Awareness (TIA) program, later designated the Terrorism Information Awareness program, was a DARPA project initiated in 2002. TIA was aimed at detecting and averting terrorist threats through increased data sharing between federal agencies. Specifically, TIA deployed “data-mining and profiling technologies that could analyze commercial transactions and private communications” such as individuals’ “financial, educational, travel, . . . medical records . . . [and] criminal records.”¹ According to the *New York Times*, the program operated on the premise that the “best way to catch terrorists is to allow federal agencies to share information about American citizens and aliens that is currently stored in separate databases.”² This project raised concern among many privacy advocates including the American Civil Liberties Union, the Electronic Frontier Foundation, and the Electronic Privacy Information Center. “This was a hugely unpopular program with a mission far outside what most Americans would consider acceptable in our democracy,” said Timothy Edgar, a legislative counsel for the American Civil Liberties Union office in Washington, D.C.³ By 2003, continued privacy concerns raised by a number of groups encouraged Congress to act. First, Congress passed a law ordering a report detailing the project in Public Law 108-87.⁴ The requested report was to:

include a detailed explanation for each project and activity of the Total Information Awareness program—the actual and intended use of funds; the schedule for proposed research and development; and target dates for deployment. It must assess the likely efficacy of systems such as the Total Information Awareness program; the likely impact of the implementation of the Total Information Awareness program on privacy and civil liberties; and provide a list of the laws and regulations that govern the information to be collected by the Total Information Awareness program, and a description of any modifications required to use the information in the manner proposed.⁵

The congressionally ordered report framed as key concerns about the TIA project its possibly raising “significant and novel privacy and civil liberties policy issues,” questions as to “whether the safeguards against unauthorized access and use are sufficiently rigorous,” and the possibility that the “performance and promise of the tools might lead . . . [to] increasing the extent of the collection and use of information already obtained”⁶ Continued concern led Congress to pass legislation defunding the specific project in defense fiscal appropriations bill HR 2658.^{7,8} While the legislation effectively ended the specific TIA program, the legislation still “allowed [certain agencies] the use of ‘processing, analysis and collaboration tools’ . . . for foreign intelligence operations.”⁹ Even under these narrower conditions, concern over the possible uses of the technology remained. The Electronic Frontier Foundation explained that “while EFF is pleased that these tools will not be developed specifically for domestic use, we are concerned that their development for foreign intelligence purposes continues to pose civil liberties risks—especially since it appears that they are to be developed under a classified ‘black budget’ with little, if any, public accountability.”¹⁰

A second program that raised public controversy was the Policy Analysis Market (PAM) (also known as Terrorism Futures Market, FutureMAP, or Electronic Market-Based Decision Support), a project initiated by DARPA in 2001 to apply de-

cision market theories to predict world events. The “market” would allow individuals to bet on certain events occurring, such as regime changes in the Middle East, acts of terrorism, and other political and economic events. The market was to go live in July 2003 but was canceled, right after it was announced, due to public outcry.

The markets in the PAM program actually reflected an attempt to harness the judgments of many people to improve predictive power and thus to provide better information for decision making.¹¹ The decision markets were designed to work much like other economic markets in which investors could make bids and the prices would reflect the aggregate thinking about the likelihood of an event occurring. Such markets have proved accurate in a number of contexts, including sporting events, Hollywood movie revenues, and Oscar winners.¹² Of particular interest was that a political futures market studied at the University of Iowa predicted U.S. election outcomes more accurately than either opinion polls or political pundits.¹³

Critics complained that unlike markets for forecasting U.S. election or Oscar winners, decision markets focused on predicting possible terrorist acts. One critic argued, “Trading on corn futures is real different than trading on terrorism and atrocity futures. One is morally fine and represents free enterprise, and the other one is morally over the line.”¹⁴ Others objected to the project on the grounds that “it was unethical and in bad taste to accept wagers on the fate of foreign leaders and the likelihood of terrorist attacks.”¹⁵ There was also concern that the market would actually incentivize terrorism actions such that “investors” could “profit from the accurate prediction of attacks that they carry out.”¹⁶

Politically, the proposed PAM program resulted in a firestorm of criticism. Senator Ron Wyden described the PAM program as “a federal betting parlor on atrocities and terrorism,” calling it “ridiculous and . . . grotesque.”¹⁷ He further stated that “betting on terrorism is morally wrong.” Senator Byron Dorgan characterized the PAM program as “the most Byzantine thing I have ever seen proposed by a federal agency.”¹⁸ Senator Hillary Rodham Clinton added her opinion that it was “. . . a market in death and destruction, and not in keeping with our values.”¹⁹ As a result of these criticisms, the PAM program was shut down within a day of its public announcement.

¹ Jeffrey Rosen, “Total Information Awareness,” *New York Times*, December 15, 2002, available at <http://www.nytimes.com/2002/12/15/magazine/15TOTA.html>.

² *Ibid.*

³ Carl Hulse, “Congress Shuts Pentagon Unit Over Privacy,” *New York Times*, September 26, 2003, available at <http://www.nytimes.com/2003/09/26/politics/26SURV.html>.

⁴ *Report to Congress Regarding the Terrorism Information Awareness Program*, May 20, 2003, available at http://epic.org/privacy/profiling/tia/may03_report.pdf.

⁵ Congressional Research Service, “Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws,” RL31730, 2003, available at <http://www.fas.org/irp/crs/RL31730.pdf>.

⁶ *Report to Congress Regarding the Terrorism Information Awareness Program*, 2003, available at <http://hanson.gmu.edu/PAM/govt/DARPA-report-to-congress-5-20-03.pdf>.

⁷ Electronic Frontier Foundation, “Total/Terrorism Information Awareness (TIA): Is It Truly Dead?”, 2004, available at http://w2.eff.org/Privacy/TIA/20031003_comments.php.

continued

Box 6.1 Continued

⁸ HR 2628, later Public Law 108-87 states: “Sec. 8131. (a) . . . [N]one of the funds appropriated or otherwise made available in this or any other Act may be obligated for the Terrorism Information Awareness Program” . . . [but] this limitation shall not apply to the program hereby authorized for processing, analysis, and collaboration tools for counterterrorism foreign intelligence.”

⁹ Carl Hulse, “Congress Shuts Pentagon Unit Over Privacy,” *New York Times*, September 26, 2003, available at <http://www.nytimes.com/2003/09/26/politics/26SURV.html>.

¹⁰ Electronic Frontier Foundation, “Total/Terrorism Information Awareness (TIA): Is It Truly Dead?,” 2004.

¹¹ Robert Looney, “DARPA’s Policy Analysis Market for Intelligence: Outside the Box or Off the Wall?,” *Strategic Insights* 2(9, September):1-10, 2003, available at http://www.au.af.mil/au/awc/awcgate/nps/pam/si_pam.htm.

¹² See <http://hanson.gmu.edu/PAM/press2/FRQ-Sum-04.pdf>.

¹³ Joyce Berg, Robert Forsythe, Forrest Nelson, and Thomas Rietz, *Results from a Dozen Years of Election Futures Markets Research*, College of Business Administration, University of Iowa, Iowa City, 2000, available at http://tipie.uiowa.edu/iem/archive/bfnr_2000.pdf.

¹⁴ John Schoen, “Pentagon Kills ‘Terror Futures Market’,” *nbcnews.com*, July 29, 2003, available at <http://www.nbcnews.com/id/3072985/>.

¹⁵ Robert Looney, “DARPA’s Policy Analysis Market for Intelligence: Outside the Box or Off the Wall?,” 2003.

¹⁶ Schoen, “Pentagon Kills ‘Terror Futures Market’,” 2003.

¹⁷ Senators Ron Wyden and Byron Dorgan, News Conference on Terror Financing Scheme, July 28, 2003, available at <http://hanson.gmu.edu/PAM/govt/senator-wyden-dorgan-press-conf-7-28-03.txt>.

¹⁸ *Ibid.*

¹⁹ See Celeste Biever and Damian Carrington, “Pentagon Cancels Futures Market on Terror,” *newsscientist.com*, July 30, 2003, available at <http://www.newsscientist.com/article/dn4007-pentagon-cancels-futures-market-on-terror.html>.

engaging with each of these communities all take time and money. Decision makers who adopt deliberative processes will thus have to make tradeoffs between more comprehensive engagement with relevant communities and the financial and schedule resources available.

6.3.2 Anticipatory Governance

In the first decade of the 21st century, the fields of science and technology studies and practical ethics have begun to develop a new approach to examining the societal dimensions of R&D work in science and engineering. A central premise of this examination holds that research trajectories have value dimensions that can be identified in all phases of the work, and that in fact need to be identified if important consequences are to be adequately considered—whether they are consequences involving benefits or harms, or issues of social equities or inequities.

The approach is called anticipatory governance or anticipatory ethics.¹⁵ It is different from standard approaches to technology forecasting, insofar as it does not treat the R&D process as a “black box” implying that consideration of ethical or value issues comes after the R&D itself. Anticipatory governance presumes that there are ethical and value issues that are resolved—whether explicitly, implicitly, or by default—in the doing of the R&D, whether it is in selecting a research direction and research procedures, deciding what counts as a significant finding, examining or ignoring what benefits or harms might accrue and to whom, and so forth.

Most important, this approach does not require that its adherents be able to predict the consequences of R&D to proceed in an ELSI-responsible manner. Instead, it posits that R&D managers have a responsibility to be aware that the efforts they support have and will have ELSI dimensions that need elucidation and examination at all stages, thus enabling anticipatory responsibility throughout.

6.3.3 Adaptive Planning

Policy makers have sometimes turned to adaptive processes that allow them to respond quickly to new information and concerns as they arise in the course of technology development and use. In a 2001 article, Walker et al. note that public policies must be formulated despite profound uncertainties about the future.¹⁶ In such an environment, policies made today should account for the possibility of new information and/or new circumstances emerging tomorrow that can reduce these uncertainties. Walker et al. suggest an “adaptive” approach to policy making that responds to new information and that makes explicit provisions for learning. Thus, they argue, the inevitable policy changes (also known as midcourse corrections) that happen over time are part of a larger, recognized process and in particular are not forced by circumstance to be made on an ad hoc basis.

Walker et al. propose that adaptive policies should contain a variety of policy options, some of which are intended for immediate implementation and others held in reserve as contingency plans to be activated only if and when certain things happen. That is, adaptive policies involve taking

¹⁵ For more information on anticipatory governance, see Daniel Barben, Erik Fisher, Cynthia Lea Selin, and David H. Guston, “Anticipatory Governance of Nanotechnology: Foresight, Engagement, and Integration,” in *The New Handbook of Science and Technology Studies*, MIT Press, 2008; and D.G. Johnson, “The Role of Ethics in Science and Engineering,” *Trends in Biotechnology* 28(12, Dec.):589-590, 2010.

¹⁶ Warren E. Walker, S. Adnan Rahman, and Jonathan Cave, “Adaptive Policies, Policy Analysis, and Policy-Making,” *European Journal of Operational Research* 128(2):282-289, 2001.

only those actions that are necessary now and institutionalizing a process for learning and later action—and such policies are incremental, adaptive, and conditional.

Adaptive approaches to risk regulation have been used from time to time in the United States. In 2010, McCray et al. identified an adaptive approach to risk regulation in the development of human health standards for air pollutants, air transportation safety, pharmaceutical regulation, human nutrition, and animal nutrition.¹⁷ These cases had in common a prior commitment to subject existing policy to de novo re-evaluation and systematic efforts to obtain new factual information for use when the re-evaluation takes place. McCray et al. concluded that adaptive regulation has been at least minimally effective in improving policy in these cases and indeed may be a valuable approach to try in other domains as well.

An adaptive approach to addressing ethical, legal, and societal issues may prove valuable as well. Even if the analytical framework presented in Chapter 5 is augmented through the use of the deliberative processes described above, it is highly unlikely that all relevant ethical, legal, and societal issues will be identified before any given technology or applications development begins. That is, some initially unforeseen ELSI concerns may well arise over the course of development. An adaptive approach to addressing ethical, legal, and societal issues would thus involve the following:

- Plans that would be immediately put into action to address ethical, legal, and societal issues known to be relevant at the initiation of an R&D effort.
- Contingency plans tied to specific ethical, legal, and societal issues to be put into action if and when those issues emerge as the R&D effort unfolds. (These issues would be the issues that an a priori process can identify.)
- Criteria for recognizing the emergence of these issues and an organizational structure for receiving reports of such emergence.
- A schedule for formally determining if new circumstances, experiences, or knowledge warrant midcourse corrections to the original plan. This schedule may be tied to the calendar or to project milestones or any other reasonable set of events.
- Provisions for monitoring media, conferences, chat groups, and so on to identify unexpected ethical, legal, and societal issues that may be suggested.

¹⁷ Lawrence E. McCray, Kenneth A. Oye, and Arthur C. Petersen, “Planned Adaptation in Risk Regulation: An Initial Survey of U.S. Environmental, Health, and Safety Regulation,” *Technological Forecasting and Social Change* 77:951-959, 2010.

What is the downside of adaptive planning? One disadvantage is that preparation of various contingency plans can be costly, in terms of both money and personnel. Such costs are incurred before the initiation of a project and over the course of the project. In addition, what seems like the wisdom to revise plans in the face of new information can be perceived by stakeholders or observers as “weakness or unprincipled malleability in the face of political pressure.”¹⁸

A third objection to adaptive planning is that it is often better suited for addressing consequentialist (utilitarian) concerns that can be mitigated and softened by adjusting and modifying a technology development path going forward. (From time to time, but probably rarely, it will be the case that no amount of program adjustment or modification, short of complete cessation, will address ELSI concerns adequately.) Note, however, that in practice, real human thinkers generally do not take these extreme views; indeed, one philosopher-ethicist—William David Ross—proposes the notion of *prima facie* duties, a concept that allows for the possibility of consequences overriding deontological duties if the consequences are horrific enough but that also stresses the importance of giving such duties weight and not being overridden simply because there happens to be some consequentialist payoff.¹⁹

Last, adaptive planning is by assumption arguably less stable than traditional planning, which generally does not admit the possibility of midcourse corrections at all. Without adaptation, *a priori* planning may fail because the discrepancy between what was assumed and what is actually happening becomes too large. But at some point, too much adaptation (too many midcourse adjustments that are too large) eliminates the benefits of planning and reduces decision making to an entirely reactive and *ad hoc* enterprise. So the sweet spot in adaptive planning is somewhere between zero adaptation and too much adaptation—and where to find that spot is a matter of judgment.

¹⁸ McCray et al., “Planned Adaptation in Risk Regulation,” 2010.

¹⁹ Anthony Skelton, “William David Ross,” *Stanford Encyclopedia of Philosophy*, Summer 2012 Edition, Edward N. Zalta, ed., available at <http://plato.stanford.edu/archives/sum2012/entries/william-david-ross/>.

7

Mechanisms for Addressing Ethical, Legal, and Societal Issues

7.1 CHARACTERIZING POSSIBLE MECHANISMS FOR ADDRESSING ETHICAL, LEGAL, AND SOCIETAL ISSUES

Assessment of ethical, legal, and societal issues associated with military R&D can be considered in light of the fact that many nonmilitary organizations, both public and private, have established mechanisms for attending to such issues. These mechanisms span a broad range along a number of interrelated dimensions.

For example, the degree of formality may vary. Formal mechanisms are similar to process-oriented proceedings (in some cases, they are legal proceedings) in that they are governed by specified procedures, and their operation and often their existence are backed by law and governmental power. Informal mechanisms are more akin to conversations between colleagues and friends that enlighten and provide information to those who must make decisions about ELSI concerns. Lightweight and flexible, informal mechanisms tend to have a cooperative and advisory character, and whether these characteristics are an advantage or a disadvantage often depends on the perspective of the viewer. In between are voluntary mechanisms such as government-developed guidelines that do not have the force of law or regulation but nevertheless reflect government policy decisions. For example, a research-performing institution may be required to adhere to certain research guidelines, which might touch on

ELSI concerns, developed by a particular agency as a condition of receiving funding from that agency.¹

Mechanisms also differ in their degree of authority. Binding mechanisms result in rulings, decisions, and regulations to which all parties to a dispute must accede, even if some parties may dispute the particulars in any given case. Generally, rulings, decisions, contractual agreements, and regulations can be enforced by law, although there are mechanisms for court challenges. Nonbinding mechanisms are established to encourage thought and attention to various ethical, legal, and societal issues.

In general, formal and binding mechanisms are established in adversarial contexts when parties that might be critical of a decision do not trust that policy makers will take their interests into account to an adequate degree. But it can also happen that an agency forced or required by law to engage in a formal process may eventually internalize the rationale for that process.²

Another differentiating characteristic of various mechanisms for addressing ELSI concerns is the degree to which a mechanism is integrated with or operates independently of a science or technology research effort. Either approach can work well, although one may be more appropriate than the other depending on the circumstances. They can also be used in tandem.

When an ELSI effort is conducted independently of the associated R&D, it can, in the experience of some committee members, operate with more autonomy and with greater control of its resources, thus enabling the pursuit of a long-term ELSI research agenda that aligns well with institutions' disciplinary perspectives expressed, for example, in a science-technology-society (STS) program or a public policy program. The integration of technical and STS/policy work is harder to achieve, however, when the institutions involved are separate.

One major advantage of a mechanism for addressing ELSI concerns that is integrated with R&D is the easy access to detailed knowledge of the technical work, knowledge that is often integral to the effective pur-

¹ For example, all research projects involving recombinant DNA if funded by the National Institutes of Health or if conducted at an institution receiving any NIH funding at all must comply with the NIH Guidelines for Research Involving Recombinant or Synthetic Nucleic Acid Molecules. See http://oba.od.nih.gov/oba/rac/Guidelines/NIH_Guidelines.htm#_Toc351276220.

² For example, a 1979 book by Daniel A. Mazmanian and Jeanne Nienaber Clarke (*Can Organizations Change?: Environmental Protection, Citizen Participation, and the Corps of Engineers*, Brookings Institution, Washington, D.C., 1979) expressed optimism that the Army Corps of Engineers might be changing its decision-making processes based on what it had learned from using environmental impact statements. See <http://www.hks.harvard.edu/saguaro/pdfs/sandereisandsklessons.pdf>. See also <http://www.mvp.usace.army.mil/docs/history/04.chaptertwo.pdf>.

suit of STS/policy-oriented research (e.g., research involving biosecurity, biosafety, or intellectual property rights). In addition, in an integrated effort technical work can be informed by work on ethical, legal, and societal issues grounded in the social sciences. In the experience of some committee members, one disadvantage of the integrated model has been the frequent lack of adequate funding for research on ethical, legal, and societal issues and for social science research and a corresponding lack of autonomy to shape a research agenda. Integrated mechanisms are also potentially subject to a certain degree of co-optation, in which the original intent of the mechanism may be undermined to some extent by the way in which it is implemented.

Different mechanisms for addressing ELSI concerns also differ substantially in their financial cost, with formal mechanisms tending to cost more than informal ones. Nevertheless, it is unrealistic to expect that addressing ethical, legal, and societal issues will be cost-free, and investments in mechanisms to address such issues may be cost-effective if they help policy makers to avoid expenses that might be incurred in the future when programmatic changes are harder and more costly to make.

It should be noted that good judgment is the first and foremost mechanism for identifying problematic ethical, legal, and societal issues that may be associated with a given research project. Scientific research is supported largely on the assumption that researchers will make positive contributions to society, an assumption that posits a “floor” for ethical standards. Project proposers are expected to exercise good judgment in not submitting proposals that are unethical with respect to either the conduct of the research that would be supported or the applications that they anticipate will result from that research.

The same applies to program officials, who are expected not to approve or support projects that are unethical. Indeed, senior program officials such as agency directors—who admittedly may not know in detail of every project undertaken in their agencies—sometimes say they hope their actions and agencies are kept off the front pages of the *New York Times* and the *Washington Post*; such sentiments reflect awareness that they are accountable for projects that might cause public outrage for whatever reason (including ELSI concerns).

But these expectations for good judgment are generally not reflected in any explicit or systematic guidance to program officials, or to project proposers. Thus, these individuals must rely on their own sensitivities, awareness, and knowledge of ELSI-relevant history to make such judgments or even to know that there are judgments to be made. Although it is most likely that project proposers and program officials do not believe that proposals in question are problematic from an ELSI standpoint, they

may not have even considered the question of what ethical, legal, and societal issues could arise.

Thus, good judgment cannot be taken for granted. Indeed, good judgment needs to be fostered, developed, and reinforced. To go beyond the judgment of individual program managers and individual researchers who submit proposals, a number of mechanisms with larger scope have been used to address ELSI concerns—some apply to research, and some to actual deployments of technology.

7.2 WHAT MECHANISMS HAVE BEEN USED TO ADDRESS ETHICAL, LEGAL, AND SOCIETAL ISSUES?

7.2.1 Self-regulation and Self-awareness

Effective self-regulation goes beyond the judgment of individual scientists working on individual projects. Self-regulation in an ELSI context is generally understood to mean scientists themselves working deeply to understand ethical, legal, and societal issues associated with their research fields and then developing responses to these issues. An implicit goal is to create an ELSI-sensitive culture among such scientists. There are a number of successful examples of such efforts:

- The Asilomar Conference on Recombinant DNA of 1975 mentioned in Chapter 1 was convened by concerned scientists to consider dangers of research in recombinant DNA; it led to recommendations on a variety of safety guidelines for overseeing DNA-related research and also prohibited certain kinds of experiments. This multidisciplinary conference brought together a number of scientists, health care practitioners, and lawyers. Notably, it was organized entirely at the initiative of bench scientists without direct involvement by governmental representatives.
- In 2004, the National Academies initiated a project to develop guidelines for all human embryonic stem cell research (that is, without regard for funding source) that took both ethical and legal concerns into account.³ The covered research included the “use and derivation of new stem cell lines derived from surplus blastocysts, from blastocysts produced with donated gametes, or from blastocysts produced using nuclear transfer.” The study also considered health science policy issues related to the development and use of human embryonic stem cells for eventual therapeutic purposes. As a result of the complexity and novelty of

³ National Research Council and Institute of Medicine, *Guidelines for Human Embryonic Stem Cell Research*, The National Academies Press, Washington, D.C., 2005, available at https://download.nap.edu/catalog.php?record_id=11278.

many issues involved in this cell research, the report recommended that involved research institutions create special review bodies that would be responsible for ensuring that all applicable regulatory requirements were met and that cell research was conducted according to report guidelines. This project is addressed in greater detail in Appendix D.

- An exercise in the synthetic biology community is underway today to incorporate social science expertise into understanding ELSI dimensions of such research.⁴ On May 26, 2006, synthetic biologists issued the Declaration of the Second International Meeting on Synthetic Biology, which addressed several widespread challenges in the field, such as commercial providers accepting orders for DNA sequences that may encode hazardous biological agents.⁵ The declaration called for the synthetic biology community to adopt the use of software tools and best practice to check for DNA sequences that encode hazardous biological agents, as well as to engage in discussions with various stakeholders and policy makers to develop governance options for the community.

Some critics have argued against self-regulation. For example, Patrick Taylor argues that many efforts at self-regulation fail because of “conflicts of interest . . . , fragmented, disconnected oversight; and failure to embody genuine scientific and public consensus.”⁶ To be credible and effective, he argues, self-regulation must be “inclusive and multidisciplinary, publicly engaged, sufficiently disinterested, [and] operationally integrated with institutional goals, and must implement a genuine consensus among scientists and the public. The mechanisms of self-regulation must be sufficiently broad in their oversight, and interconnected with other institutional forces and actors, that they do not create fragmented solutions.”

Nonetheless, self-regulation has been used with considerable success in a number of instances, although its acceptability to the community as a regulatory mechanism continues to be in question. Because self-regulation is driven by scientists themselves (and especially so when Nobel laureates and other luminaries in the field are known to be the driving forces), the recommendations of self-regulatory bodies can have considerable credibility in the scientific community and are less likely to be perceived as overbearing and excessive.

⁴ Lewis D. Solomon, *Synthetic Biology: Science, Business, and Policy*, p. 160, Transaction Publishers, New Brunswick, N.J., 2011.

⁵ “Declaration of the Second International Meeting on Synthetic Biology,” Berkeley, Calif., May 29, 2006, available at <http://syntheticbiology.org/SB2Declaration.html>.

⁶ Patrick L. Taylor, “Scientific Self-Regulation—So Good, How Can It Fail?”, *Science and Engineering Ethics* 15(3):395-406, 2009, available at <http://www.springerlink.com/content/pnn32878785v1n33/fulltext.pdf>.

7.2.2 Established Institutional Mechanisms

As noted above, many civilian organizations have established mechanisms addressing ethical, legal, and societal concerns. Sometimes, these mechanisms address such concerns in a specific field or problem domain, such as nanotechnology or drug approval. A number of these mechanisms are described below in summary form and without references. These established mechanisms are discussed in more detail in Appendix D, which also provides references when necessary.

- *DOD law-of-armed-conflict review and treaty compliance.* Weapons acquired by the Department of Defense are subject to a review early in the acquisition process that determines whether the normal or expected use of the weapon is consistent with the law of armed conflict (LOAC). However, such reviews are not required to foresee or analyze all possible misuses of a weapon. R&D is also not subject to such review. Similar processes attach to efforts that might implicate obligations stemming from treaties that constrain or restrict research or development in some way.

- *Codes of ethics and social responsibility in medicine, engineering, and science.* Medicine, engineering, and science are fields that generally hold practitioners accountable for considering at least some of the ethical ramifications of their medical, technical, or scientific work. Professional standards and codes of ethics may be implied or implicit rather than codified or formalized, and incorporate both standards for behavior (what must a responsible practitioner do in providing services to clients) and social responsibility (e.g., a responsibility for practitioners to provide services and expertise to society in addition to those they provide to their clients; a responsibility to protect a vulnerable public from harm).

- *Research on ethical, legal, and societal issues.* The federal government has supported such research in the context of specific scientific efforts such as genome research and the National Nanotechnology Initiative. Through the National Science Foundation, it has also supported a research program on improving knowledge of ethical and value dimensions in science, engineering, and technology and a program focusing on ethics education for graduate students in science and engineering. Both individual ELSI investigators and ELSI research centers have been supported by various U.S. government efforts. In addition, there are some efforts to integrate ELSI research into individual proposals for certain scientific research, so that knowledge about ethical, legal, and societal issues can have an impact on how the scientific research is conducted.

- *Oversight bodies.* Established by federal law, institutional review boards (IRBs) address ELSI issues directly related to the safety of human subjects that arise in the conduct of research (usually of a biomedical, social, or behavioral nature). IRB approval is needed before any federally

funded research involving human subjects can begin at an affected institution. (Separately, many institutions have biosafety committees, radiation safety committees, and so on.) In addition, some institutions performing embryonic stem cell research have established oversight committees to oversee all issues related to derivation and use of human embryonic stem cells; these committees are also supposed to approve the scientific merit of research proposals.

- *Advisory boards.* Advisory boards and committees are a time-honored way to focus attention on ELSI issues associated with S&T. For example, the Recombinant DNA Advisory Committee informs and advises the NIH on certain ethical, legal, and societal issues related to recombinant DNA research and reviews human gene transfer research. The National Science Advisory Board for Biosecurity provides advice regarding biosecurity oversight of legitimate biological research that may be misused to pose a public health and/or national security threat. The Presidential Commission for the Study of Bioethical Issues advises the President on bioethical issues arising from advances in biomedicine and related areas of science and technology. Community acceptance panels are convened by the National Institute of Justice to gather input regarding new research and development initiatives from relevant communities.

- *Research ethics consultation services.* Such services have been established in a number of research environments to help raise awareness of issues related to the ethics of human subjects research and to assist investigators in resolving these issues. Using an “ELSI consultants on call” model, these services provide real-time advice to scientists about how to recognize and address ELSI concerns in ongoing research and at the same may lead those involved to discuss broader ethical, legal, and societal issues.

- *Chief privacy officers.* Privacy is widely regarded as a key ELSI concern associated with technology in many contexts. Many institutions have vested responsibility for protecting the privacy of citizens and customers in the public and private sectors, respectively, in chief privacy officers (CPOs). Such officers are intended to be part of an institution’s senior management. In many institutions, the CPO does not take an adversarial role with respect to its programs, but rather works with those programs to find ways of meeting program objectives without harming privacy.

- *Environmental assessments and environmental impact statements.* Under federal law, certain federal projects that potentially affect the environment require an environmental assessment (EA) that provides evidence and analysis for determining whether a project has a significant environmental impact. If so, an environmental impact statement (EIS) must be prepared. An EA is typically a short document. If an EIS is required, an analysis is prepared that systematically addresses environmental dimensions of the project in question. An EIS must articulate the beneficial and

harmful environmental impacts of a proposed action as well as alternative courses of action. Public input is often sought in these processes.

- *Drug evaluation and approval.* The Food and Drug Administration has long faced decisions with ethical, legal, and societal issues having certain properties similar to those faced by military R&D: innovative products offering unique benefits and risks, proprietary information that must be protected, technical information whose evaluation requires scientific expertise, uncertainty that may be reduced by research conducted before or after usage begins, and time pressure that must be respected. As illustrated in Box 7.1, the FDA has developed procedures for addressing ELSI concerns in drug development that are intended to be expert driven, confidential, advisory, predictable, constructive, timely, and efficient.

7.2.3 Existing DARPA Efforts to Manage ELSI Concerns

DARPA acknowledges publicly that there is often a tension between research on novel technological concepts and an underdeveloped ethical, legal, and societal framework for addressing the full implications of such research, noting that “[i]f we [DARPA] do our research well, we will necessarily bump up against these concerns. Our responsibility to the defense of the Nation is such that we must thoughtfully address these issues, while simultaneously pursuing our work.”⁷

For example, citing privacy as an ELSI concern of the first order and recognizing the history of its own Total Information Awareness program as being at “the leading edge of the tension created between new technological approaches to addressing threats to the Nation’s security and individual privacy or civil liberties that are core values for the Nation,” DARPA has enunciated a number of principles to describe its renewed commitment to addressing privacy implications throughout an R&D program’s life cycle.⁸ These principles call on DARPA to do the following:

- Consistently examine the impact of its research and development on privacy.
- Responsibly analyze the privacy dimension of its ongoing research endeavors with respect to their ethical, legal, and societal implications.
- Transparently respond to the findings of its assessments of its unclassified work, and ensure independent review of its classified work, in accordance with a commitment to shared responsibility for addressing the privacy issue.

⁷ These principles were listed on the DARPA Web site on September 1, 2013, but the Web page has since been taken down. However, an archived version can be found at http://web.archive.org/web/20130901062709/http://www.darpa.mil/About/Initiative/DARPA%E2%80%99s_S_T_Privacy_Principles.aspx.

⁸ Ibid.

Box 7.1 The FDA Center for Drug Evaluation and Research

To manage ethical, legal, and societal issues associated with drug approval, the Food and Drug Administration (FDA) established the Center for Drug Evaluation and Research (CDER) to take responsibility for approving drugs.¹ Its decisions determine the availability of drugs, but not their use, because the FDA does not regulate the practice of medicine. The FDA's reviewers focus on the proposed use of a product (e.g., to treat initial infections from a disease). They may, however, note other potential uses that FDA's decision makers may wish to consider when making the approval decision (e.g., use for repeated infections or with more vulnerable populations than those in the clinical trial). Unlike the FDA, which may be prevented from considering off-label uses of approved products, review teams for military R&D would be required under many circumstances to consider such uses.

Under the Prescription Drug Users Fee Act, drug manufacturers cover the costs of the FDA's review process. Great effort is made to ensure the independence of the review process from any sponsor influence—and to protect the confidentiality of the data that reviewers receive. The cost of reviewing a new drug is approximately \$1 million, or about 0.1 percent of the approximate investment in recent years in an approved product, and hence a modest cost of doing business. Producing and summarizing the reviewed data entail activities that manufacturers would, largely, perform in any case, and that thus add minimal costs. The FDA's data needs are known early enough to affect the design of the clinical trials, so as not to slow things up. The review process itself can be accelerated when the need arises.

There is reason to believe that the quality of pharmaceutical research is improved by receiving the FDA's input during trial design and its technical review at the end. The FDA's evidentiary needs are sufficiently standardized for firms so that the needed expertise is widely available (from inside firms or from contractors).

To fulfill its responsibilities, DARPA has (among other things) assigned an internal privacy ombudsman to work closely with the DOD Privacy Office, and has created an independent privacy review panel to assess existing and emerging privacy laws, regulations, technologies, and norms and to analyze their potential effects. The panel is composed of leading scholars and policy and technology experts in the privacy field. In February 2011, the panel met with DARPA to discuss “the implications of privacy laws and policies on DARPA programs” and “to help DARPA create an internal privacy accountability process.”⁹ It is the intent that the panel's experts will consult with individual DARPA program managers to help them address privacy concerns that arise early in a program's life cycle and to ensure that each program's privacy implications are understood.

⁹ Ibid.

By imposing uniform standards, the FDA helps to level the playing field across products. It may create barriers to entry for smaller firms, unless they can team with entities having the needed risk analysis and management capabilities. The ensuing regulatory decisions are sufficiently predictable that manufacturers can often look at preliminary results from testing a product and decide whether to continue its development.

To make its decision-making process more predictable and transparent, the FDA has recently committed to producing a standard summary of the rationale for its approval decisions. (When products are not approved, no public statement is issued, allowing manufacturers to revise, or drop, projects while revealing minimal details.) That summary distinguishes between *evidence* and *reasons* for the decision. The former involves scientific results, including associated uncertainties. The latter contains the scientific opinions of expert reviewers about the implications of that evidence for the regulatory decision—recognizing that scientists' perspectives may be valuable, even if someone else makes the approval decision.

The summary includes analyses of risks and benefits, as well as the “unmet medical need” that captures the case for innovative treatments—which may be approved even if their risk-benefit profile is no better than that of existing products. For many products, the summary concludes with a risk evaluation and mitigation strategy, with recommendations for additional measures that could increase a product's benefits (e.g., by ensuring patient compliance), reduce its risks (e.g., by requiring pregnancy tests), or improve its evidentiary base (e.g., by having a patient registry or by conducting a postmarketing clinical trial, the details of which must be approved by the FDA as a condition of licensing).

¹ For more information on CDER, see <http://www.fda.gov/Drugs/ResourcesForYou/Consumers/ucm143462.htm>.

A second DARPA effort has been to create an advisory committee for the Living Foundries program. As noted in Chapter 2, that committee is modeled on the privacy panel described above, and its purpose is to advise program staff on the inherent ethical and societal issues that might be raised by DARPA's investment in synthetic biology R&D. In practice, the advisory committee (AC) has several responsibilities:

- It helps to shape broad agency announcements and requests for proposals;
- It reviews all incoming proposals and flags potential areas of concern in advance;
- It tracks research as it is conducted and flags emerging issues;
- It assesses how results should be released and publicized; and
- It assesses potential applications of research.

The AC has a number of different modes of doing its work. In 2012, it held an initial day-long meeting to orient DARPA program officials to ethical, legal, and societal issues related to synthetic biology. The AC will also engage with program managers directly, one-on-one, and in retreats with research performers. Feedback will be provided from the AC to the DARPA director through the program manager and directly to research performers. AC members are encouraged to discuss their work with anyone they choose, whether in or out of DARPA.

There are no predetermined processes in place for how to handle problematic ELSI concerns that are identified through the AC. It is not expected by DARPA that one process will be applicable to all issues, and significant variations from case to case and situation to situation seem likely.

DARPA has also established a working group in cooperation with the National Science Foundation to address the ethical, legal, and societal implications of personally identifiable information during the R&D activities it supports. This activity is strongly influenced by the unique national security concerns associated with operational security and the need to protect sources and methods.

7.3 CONSIDERATIONS FOR MECHANISMS USED TO ADDRESS ETHICAL, LEGAL, AND SOCIETAL ISSUES IN THE CONTEXT OF MILITARY R&D

All of the mechanisms described above speak to some of the ethical, legal, and societal issues in some S&T research and development efforts to some degree. How, if at all, any of these mechanisms might be useful for addressing ethical, legal, and societal issues associated with R&D in a military context is the question that this section explores.

Toward characterizing the attributes of a process for addressing ELSI concerns related to R&D with military relevance, the above discussion is a point of departure. Abstracting from this discussion, the following attributes seem relevant:

- *Awareness.* Most of the mechanisms described above are predicated on the awareness of the scientists and engineers engaged in an R&D effort. These individuals have a significant stake in how problematic ELSI concerns are resolved, because they may have to revisit and modify or curtail some of their technical efforts to overcome or resolve the issues. Communication and analysis of ethical, legal, and societal issues is a key part of this process. Such communication enlightens and also serves as a statement of values by the entity conducting the analysis.

- *Accountability and responsibility.* Mechanisms such as IRBs, chief privacy officers, and the formal LOAC review of weapons prior to procurement acknowledge the need for accountability in discussions of ELSI-related matters. These efforts combine program responsibilities with functional responsibilities.¹⁰ Personnel working on an R&D effort thus have loyalties to the project (they are committed to making the project work), and they also have responsibilities for exercising and deploying their skill sets as well as they can. In large organizations, personnel are accountable both to the project managers and to their functional management. In small organizations, project management and functional management may be combined in the same person(s).

- *Expertise.* Some of the mechanisms described above (e.g., IRBs, advisory boards, interdisciplinary ELSI research, research ethics consultation services) are predicated on the idea that addressing ethical, legal, and societal issues requires deep and serious expertise both from the scientific disciplines involved and from specialists in ethics, law, and the social sciences. Furthermore, such expertise must be available both to program officials (who decide on the scope and nature of the support that they will provide to any given R&D project) and to project personnel (who will execute the project, presumably within the parameters specified by program officials).

- *Access to relevant scientific and technical information.* One of the fundamental rationales for interdisciplinary work is that knowledge from one discipline can prompt and facilitate insight and analysis by another—and barriers to passing such information between researchers inhibits such analysis. ELSI research and discussions of ELSI concerns are no exceptions to this rationale. Analysis of ethical, legal, and societal issues can make greater progress when scientific and technical information passes freely between ELSI researchers and the R&D researchers, and the same is true for the ELSI information.

- *Time.* All of the mechanisms above call for the expenditure of some amount of time. In some cases, the calendar time needed for invocation of any of these mechanisms can be reduced by operating the mechanism in parallel with the scientific work. But in those instances where the mechanism serves as a gateway to future work, there is much potential for delay.

¹⁰ A program or project typically has budget, performance, and schedule goals that project managers are accountable for meeting. That is, a project promises to achieve certain goals (performance) within a certain time frame (schedule) and a certain budget. Functional responsibilities are the skill sets that are necessary to reach these goals. Functional responsibilities include a technical skill set (e.g., engineering), but also may include skill sets related to legal and regulatory matters, human resources, finance, and so on.

- *Variety in perspectives.* A number of the mechanisms described above (e.g., environmental impact statements, research ethics consultation services, advisory groups) are based on the idea that taking input from a broader range of perspectives (especially perspectives that are not necessarily similar to those of the scientific researchers) will surface issues specific to a particular project or program that those involved in the program might not have considered otherwise. In addition to the mechanisms described above, the DOD R&D community has a tradition of red-team analysis to find technical and operational weaknesses in proposed acquisition projects—an approach that could be adapted specifically for raising ELSI concerns underlying a given research direction. Insiders who see that certain ethical issues are being ignored and others who are not associated with or advocates for particular projects are also sources of insight.

- *Comprehensiveness.* The mechanisms discussed above focus on different kinds of ethical, legal, and societal issues—those related to the environment or human subjects or specific technologies, for example. Thus, with the application of any one such mechanism, important ELSI concerns—even those that may have been known in advance or anticipated—may go unaddressed simply because there is no comprehensive mechanism in place for addressing a range of such issues.

- *Cooperation.* The mechanisms described above work best when project and program managers can address ELSI concerns in a cooperative manner early enough to affect the way a project or program is laid out, that is, before addressing ELSI concerns becomes very expensive either in time or financial resources.

Depending on their goals, policy makers will have to decide how far to go with respect to any of these attributes in designing an approach for addressing ethical, legal, and societal issues in the context of military R&D.

In any event, the approach will have to include a process for identifying and assessing ELSI concerns at the outset of an R&D project and also a process for monitoring and assessing the subsequent emergence of such issues throughout the project's timeline. Both in-house expertise and external expertise with ethical, legal, and societal issues in the context of military R&D are necessary for these processes to work well. Appropriate public engagement to identify issues and to build legitimacy for a particular R&D project is necessary as well.

The FDA process described in the section on drug evaluation and approval in Appendix D has some of the elements outlined in the bulleted list of attributes above, and is thus suggestive of a point of departure for a model that fits the conditions of certain kinds of military R&D under

some circumstances. The subject-matter expertise and deciding authorities will be very different, as might some of the ethical and social issues. However, a credible, workable system for evaluation of military R&D would have to have many of the attributes described in the bulleted list above.

It is very important that an approach for addressing ELSI concerns for military R&D take into account the special characteristics of the military environment described in Chapter 1. To defend the nation and its interests, the United States develops some military technologies and applications for use as weapons, and weapons are designed to cause harm, possibly extensive, to people (specifically, combatants) and to property (specifically, property with military purposes). That such development can be ethical is therefore a fundamental premise of such work. Thus, a chosen approach to addressing ethical, legal, and societal issues for military R&D must maintain control over processes for receiving input from individuals who do not share or are not willing to set aside discussion of this premise.

In addition, an approach for addressing ELSI concerns with R&D of military relevance must be capable of accommodating the classified dimensions of military research. Although classification does limit the number of individuals who can participate in any kind of ELSI review, the fact that a program is classified is not ipso facto a valid reason for asserting the impossibility of conducting a useful review. One major reason is that the ELSI dimensions of a project can often be discussed without referring to the parts of a project that involve classified information. A second reason is that a significant breadth of input can be gathered by using cleared individuals not formally associated with a given project.

It is also noteworthy that some of the issues raised by research classified for national security purposes also occur in considering certain kinds of civilian research and development. In particular, many industrial research labs operate with as high a level of secrecy as they can manage for obvious commercial reasons. Thus, under some circumstances, it is possible that experience with handling ELSI considerations in a quasi-classified civilian environment might have some relevance to handling such considerations for classified research.

Finally, urgent military needs sometimes emerge under the pressure of operations (e.g., new adversary weapons or tactics), and R&D may be needed on a time scale that does not allow ELSI concerns to be fully considered or accommodated before the technical work on a specific application is completed. Three observations are relevant here. First, it is not necessary to handle all relevant ELSI concerns as “gateway” issues—and to the extent that they can be handled in parallel, they need not necessarily add calendar time to a project timeline. Second, such time pressures

are usually not relevant to research aimed at advancing foundational or enabling technologies; rather, they emerge primarily in the context of specific applications to address urgent needs. Third, nothing in the discussion above limits consideration of ethical, legal, and societal issues after a new application is deployed for use, and indeed policy makers should be prepared for the possibility that actual operational use of a given application will raise ethical, legal, and societal issues that they will have to address.

The recommendations in Chapter 8 elaborate one version of the approach suggested above.

8

Findings and Recommendations

8.1 SYNTHESIS

Chapter 1 of this report describes the approach of the United States to national security as one that emphasizes technologically derived qualitative advantages over its adversaries and the centrality of technology development to its national security efforts. This emphasis drives the U.S. Department of Defense and a variety of other agencies with national security responsibilities to invest heavily in activities that promote the development of technology with applications to military and other national security needs.

The emergence of new technologies often raises ethical, legal, and societal issues. Sometimes, these issues are new; other times, they are familiar but must be reexamined in the light of a new technological milieu or societal sensitivities that may not have been present when these ethical, legal, and societal concerns first appeared.

Although substantial work has been done over the past few decades to explore ELSI implications of new technologies, such work has been done largely in a civilian context. This report explores the ELSI implications of emerging and readily available technologies (ERA technologies) in a military context, and suggests the possibility that some of the ELSI understandings formulated in the context of civilian applications may need to be modified or extended when cast against a military or other national security backdrop.

Chapters 2 and 3 distinguish conceptually between foundational science and technology and application domains. Foundational science

and technology enable progress and applications in a variety of application domains; an application domain is associated with a set of specific operational military problems, the solutions to which may draw on many different technologies. Chapter 4 describes sources of ELSI insight, including a variety of theoretical and disciplinary approaches to ethics; international law; and insights from social sciences such as anthropology and psychology.

Building on the examples offered in Chapters 2 and 3 and informed by an understanding of sources of ELSI insight outlined in Chapter 4, Chapter 5 develops an analytical framework for systematically identifying and assessing ethical, legal, and societal issues that may arise with ERA technologies for military and national security purposes.

Chapter 6 focuses on the fact that foresight regarding the direction and outcomes of technology development is never entirely complete or accurate, and it describes a variety of approaches that can be used to help compensate for such fallibilities in anticipating ethical, legal, and societal issues associated with ERA technologies.

Chapter 7 identifies a variety of mechanisms that have been used in a civilian context to address ethical, legal, and societal issues and also describes some approaches to addressing such issues in the context of novel technological developments with military applications.

In the review process for this report, a number of reviewers suggested that the framework, findings, and recommendations offered in the report apply across the board to essentially all science and technology research of military significance, and not just those that are emerging and readily available. The committee examined only ERA technologies, and thus declines to assert the relevance of this report so broadly, but the committee would be gratified if the discussion in this report turns out to be relevant to non-ERA technologies as well.

8.2 FINDINGS

Finding 1: Some developments in emerging and readily available technologies in a military context are likely to raise complex ethical, legal, and societal issues, some of which are different from those associated with similar technologies in a civilian context.

The history of science and technology (S&T) shows that S&T developments have always raised ethical, legal, and societal issues to one degree or another. But as noted in Chapter 1, the foundational technologies of interest for this report are associated with a high degree of uncertainty about their future trajectories and what the useful applications of these technologies will turn out to be. A broad range of uncertainty in technol-

ogy development suggests a correspondingly broad range in the ethical, legal, and societal issues that are likely to emerge—and inevitably some of these issues will be thorny and complex.

Previous work on ethical, legal, and societal issues in the civilian S&T context provides a valuable point of departure for any effort to examine such issues in a military context. But essential differences between civilian and military contexts must be taken into account.

For example, new technologies with military application can confound the conceptual basis on which ethical norms are founded. Consider the connection between S&T and principles of “avoiding unnecessary harm.” Ethics is in part about the avoidance of harm, and in a civilian context, science and technology researchers do not ordinarily seek to enable or develop applications that would be harmful to people or damaging to property. But in some military contexts, these are explicitly the goals—and presumptions about avoiding harm in civilian technology development give way to notions of avoiding *unnecessary* harm in the development of certain military technologies.

New science and technology also open new areas in which the concept of harm may operate. The first Hague Convention on the laws of war was formulated in 1899, and at that time, the notion of harm did not—indeed could not—acknowledge notions of harm to an individual’s genome or harm caused by radiation. Today, information technology and cyber weapons offer possibilities for harming individuals and societies without death or destruction; economic harm and social harm are two possible outcomes of cyber conflict. Physical proximity as an indicator of risk for harm (e.g., a civilian’s distance from a military target, such as a munitions factory) is not particularly relevant when cyber weapons are considered.

A related point is that new technologies with military application may well generate ELSI controversy even if the ELSI concerns are in some sense not new. A new technology often provides new ways of accomplishing certain military tasks, and the new ways as well as the tasks themselves may create controversy or need further ELSI-related scrutiny. Over time, a consensus may develop regarding these ethical, legal, and societal issues.

If such a consensus does not develop, the controversy may fade from public view or continue with high public visibility. When a controversial ELSI concern remains unsettled, the (actual or potential) use of a new technology to accomplish military tasks may well re-open the debate, or at least put a new spotlight of public attention on it. From the standpoint of public understanding and accountability, the assertion that the ethical, legal, and societal issues themselves are not new can only be a starting point for exploring the ELSI ramifications of new technologies. In a new

and different context, a new technology may change weightings of different factors that need to be taken into account or even their salience or relevance to the ELSI concerns in question.

As for the “readily available” aspect of ERA technologies, the most significant impact on ethical, legal, and societal issues arises from the fact that more parties with access to such technologies have a greater collective ability to create new applications, and the larger set of applications thus made possible expands the scope of ELSI concerns that could arise. In addition, ERA technology characteristics such as rapid change and low barriers to entry may have ELSI implications in and of themselves.

Finding 2: Sustainable policy—policy whose goals and conduct can be supported over the long run—regarding science and technology requires decision makers to attend to the ELSI aspects of the S&T involved.

Why should ethical, legal, and societal issues be addressed at all? One obvious answer is normative: as a nation, we wish to conduct ourselves and our activities in an ethically defensible manner and for ethically supportable purposes. But a more practical answer is found in the idea that policy makers want the policies that they formulate to be sustainable over the long run. High-quality science is one of the more important and obvious factors that contribute to the success of any particular S&T effort. But inattention to ELSI aspects of an R&D endeavor can undermine even scientifically sound R&D efforts and call into question policy decisions that led to those efforts, regardless of the initial intent underlying those original decisions.

One illustration comes from DARPA’s own history: the Policy Analysis Market. As noted in Chapter 6 (Box 6.1), the goal of that project was to develop a new technique for predicting political events based on a futures market—a technique with some support in the scientific literature. But the undertaking ran afoul of public concerns regarding the ethics of a project that might give individuals incentives to conduct terrorist activities, even if such incentives were in some absolute sense minimal. The methodology—arguably a promising one in the appropriate context—was not as thoroughly explored as it might have been, and the project was canceled.

Finding 3: Public reaction to a given science or technology effort or application is sometimes an important influence on the degree of support it receives.

A public perception that an R&D project is unethical may undermine support for it, even if the project is technically sound. A lack of support

may manifest itself through adverse journalistic and editorial treatment, greater political scrutiny, reduced budgets (especially in a time of constrained finances), additional restrictions on research, and so on. On the other hand, a positive perception regarding the ethics of an R&D project may enhance public support for pursuit of that science or technology, irrespective of the scientific or technical basis for such pursuit.

Finding 4: The ethical, legal, and societal issues of concern that may be associated with a given technology development are very hard to anticipate accurately at the start of that development.

The discussion above implies that decision makers must exercise a kind of due diligence in identifying and assessing ethical, legal, and societal issues associated with the R&D they support

Issues that may arise along a known technological path can emerge at any point in the R&D process and indeed may do so on a very short time scale. The salience of such issues can also be amplified through multiple channels (e.g., social media). On a longer time scale, ethical concerns and issues often change as technology evolves and matures, and as society becomes more familiar with the technology.

In addition, overly optimistic technological forecasts made by interested parties about possible applications of a given S&T base can distort the decision-making calculus and interfere with a fair weighing of the pros and cons of pursuing a given line of research. This distortion may be especially problematic among decision makers who are unable to critically evaluate technological feasibility.

Ethical, legal, and societal issues may also arise along as-yet-unknown technological paths. If a path is not known, it will be very hard to undertake a meaningful assessment of the ethical, legal, and societal issues associated with that path. As the discussion in Chapter 6 indicates, prognosticators do not have a good track record in forecasting technology outcomes.

This is especially true when the technologies in question are foundational and worthy of basic research. Although nearly all such research supported by the government in a military context inevitably has an arguable (if speculative) nexus with military applications, proposals to the DOD for basic research do not generally mention specific applications (military or otherwise) that such research might support. But funding agencies make decisions about specific proposals based on the likelihood that such research will in fact advance the science in which they are interested, and these agencies are interested in developing the science base to (eventually) support a variety of as-yet-unknown applications useful to DOD missions.

To increase the likelihood that relevant ELSI concerns will be revealed, responsible parties would do well to consult a diversity of sources with different intellectual and political perspectives.

Finding 5: Any approach to promote consideration of ethical, legal, and societal issues in R&D of military significance will have to address how such plans are implemented at both the program and the project levels.

Policies and plans intended to promote consideration of ethical, legal, and societal issues in R&D do not by themselves ensure that any given implementation of such policies will actually address such issues in the manner intended by the originators of such plans. Implementation is critical to the success of any policy or plan, and controversy and concern can easily be fueled by inadequate attention to detail and implementational oversights as well as by the inadequacy or absence of a high-level plan to address relevant issues.

For example, it is not without precedent in large organizations that well-intentioned policies promulgated by senior management are ultimately implemented as bureaucratic checklists and mindless procedures that emphasize the letter of the policies rather than their spirit. The intent of this committee's findings and recommendations is not to impose undue compliance requirements on program managers or agencies, but rather to help well-meaning program managers in these agencies to do their jobs more effectively and to help ensure that basic American ethical values (such as those embodied in the U.S. Constitution's Bill of Rights) are not compromised. The use of common sense, judgment, and understanding of the fundamental intent of policies to address ethical, legal, and societal issues—not simply formal compliance—is the goal and is an important foundation for developing an ELSI-sensitive culture. Accordingly, the committee believes that policies originated by an agency's senior management to address ethical, legal, and societal issues systematically should have a light footprint when they are implemented by program managers.

The committee also suspects that if an agency's culture routinely addresses ELSI concerns, the additional work required to address ELSI matters on any individual project will be small. That is, the cost of putting into place the necessary processes and procedures to address the first R&D projects to be assessed for ELSI significance is likely to be at least partially amortizable over succeeding projects subject to the same processes and procedures, and a new project addressing approximately the same problem domains might require only incremental work.

The committee recognizes that having to grapple with ELSI issues may well complicate the conduct of a given S&T research project in the

short term. After all, R&D generally requires a great deal of attention focused on the science and nothing but the science. On the other hand, in the long term, addressing such issues may well be necessary for sustaining support for projects.

Consideration of ethical issues may also improve the quality of the research by pointing to other overlooked problems in the research or opportunities for improvement in the science or technology to be pursued. For example, an ethical objection to some proposed research may be based on possible harm to people resulting from that research. A scientific exploration of the mechanisms underlying that possible harm may generate additional information that could help put such fears to rest as well as make the overall research more complete from a science point of view. Indeed, critics who raise ethical objections often do so in part because they have a different perspective and ask questions different from those asked by advocates of such research.

The history of the FDA approval process for drugs to treat AIDS is an example. In the late 1980s, a variety of AIDS advocacy groups argued that the timeline for delivering promising drugs for AIDS treatment was simply too long, and that on ELSI grounds, that timeline should be accelerated. Their arguments were ultimately successful, and the FDA adopted an approval standard for certain drugs based on a risk-benefit calculus rather than on the traditional criteria of being shown to be “safe and effective.”¹

8.3 RECOMMENDATIONS

Chapters 1 through 5 point out ways in which developments in ERA technologies in a military context may end up raising significant ethical, legal, and societal issues. Such issues can raise a variety of problems, both when these technologies are used as intended and in their unintended applications. The results may include public outrage, negative political effects, or problems with internal morale, not to mention negative consequences for society as a whole.

8.3.1 Recommendations for Agencies

Agencies sponsoring research have an obligation to the people they serve at least to assess and to consider the possible negative effects of that research on individuals and society. Advance consideration of those issues should be an important task for agencies that fund such research.

¹ Harold Edgar and David Rothman, “New Rules for New Drugs: The Challenge of AIDS to the Regulatory Process,” *Milbank Quarterly* 68(Supplement 1): 111-142, 1990.

Agencies also have a self-interest in assessing these implications. Research that raises complex ethical and social issues can harm the sponsoring agency—and that can be true whether or not the research actually leads to ELSI-related problems, or even whether or not that research is even carried out. Ethical and social issues are much more than public relations problems, but they also definitely are public relations problems. Even if an agency were concerned solely with its own future, and not with the broader consequences of its actions, it would still have to worry about the ethical and social implications of its work.

As a result, both for the public interest and in its own self-interest, any agency funding research that is likely to raise complex ethical, legal, and societal issues should have in place processes to identify, assess, and monitor those issues. Any such processes will require the agency to create the capacity to operate the processes. Exactly what processes and what capabilities a particular agency needs will depend on the agency and its research. Nevertheless, there are some common features of any useful institutional response to these kinds of challenges.

For example, the committee believes that a mix of centralized management attention to ethical, legal, and societal issues and continuing responsibility for ELSI concerns distributed among program managers will be needed. But nothing in this notion necessarily implies that extra layers of management for formal review of ethical, legal, and societal issues should be required. Instead, the committee was guided by the principle that review processes should be as lightweight as possible, consistent with focusing necessary agency attention on ELSI concerns.

To implement useful mechanisms for addressing ELSI concerns in the context of military R&D, agencies supporting research of potential military value need to take action. The findings above help to shape the committee's four recommendations to agencies that support R&D on emerging and readily available technologies of military significance and that are interested in addressing ethical, legal, and societal issues inherent in their R&D portfolios. (In the recommendations below, the term "interested agency" is used to mean agencies interested in addressing ELSI concerns inherent in their R&D portfolios. In this context, an "agency" could also include a coordination office for R&D efforts across multiple agencies, such as the Networking and Information Technology Research and Development (NITRD) coordination office.)

Recommendation 1: The senior leaders of interested agencies that support R&D on emerging and readily available technologies of military significance should be engaged with ethical, legal, and societal issues in an ongoing manner and declare publicly that they are concerned with such issues. Such a public declaration should

include a designation of functional accountability for ethical, legal, and societal issues within their agencies.

An agency's senior leadership has a critical ongoing role to play in ensuring that ELSI concerns are an important consideration for the R&D it supports. High-level support from senior agency leadership is required if an agency is to seriously address ethical, legal, and societal issues associated with the research it funds. Such support must be visible and sustained over time: in its absence, little will happen. An agency's senior leadership sets the tone by publicly communicating to the organization and its stakeholders its values and their rationale. In general, a public declaration would include a statement about the importance of addressing ethical, legal, and societal issues, the willingness of the agency to learn from outside perspectives, and the intent of the ELSI-related processes. In the long run, these are key elements in creating an institutional culture that is sensitive to ELSI concerns.

Furthermore, statements of public support need to be repeated periodically, to remind experienced program managers of the importance that the agency places on the subject and to introduce new program managers to the idea of doing so. Presenting such statements at events involving the research community (e.g., professional meetings, proposers' days) as well will help to inform researchers of an agency's ELSI concerns.

The recommendations that follow provide an approach for dealing with these kinds of issues, but recommendations are not self-implementing. Even the adoption of some form of this committee's recommendations would not necessarily mean that they had been implemented, let alone implemented effectively. Organizations implement measures effectively when the people who make up those organizations believe that the measures are important. It is crucial, therefore, that an agency understand why the assessment of ethical, legal, and societal issues is important, from the top of the agency down through its ranks.

Of course, public declarations are by themselves insufficient to drive an agency's program managers to attend to ELSI concerns that may be inherent in the R&D projects they support. The fact that the agency's leadership thinks something is important may ensure that the staff will pay it lip service. To get more than lip service will often require more than a mandate from above.

To maximize the likelihood that ethical, legal, and societal issues will be addressed, an agency's senior leadership should designate a point of functional accountability for this responsibility. The rationale for ensuring such accountability arises from the complexity of an agency's operating environment. In the private sector, high-consequence businesses are characterized by an environment where hundreds of people engaged

in an effort make thousands of decisions, and one person making one mistake that goes undetected and uncorrected can cause unacceptable outcomes, such as loss of human life or enormous financial losses.

The primary responsibility for preventing such outcomes rests with the team executing the program. However, management often assigns functional organizations to provide oversight as a secondary line of defense against unacceptable outcomes. Functional managers also have ultimate responsibility as points of contact for anyone within their agencies with concerns about functional matters—in principle, anyone with a financial concern can bring that concern to the attention of the chief financial officer, anyone with a legal concern can bring that concern to the attention of the general counsel, and so on.

Internal functional organizations such as “Engineering,” “Quality Assurance,” and “Mission Success” assign people to the project team who report both up the reporting chain of the project line management and to the relevant functional manager, e.g., the VP of Engineering or the VP for Quality. Sometimes this approach is referred to as “two to hire, one to fire.” To assign someone to a project, both the project manager and the functional manager must agree on the selection. Either can remove the individual if reporting accountabilities are not met.

These individuals with two reporting lines have dual accountabilities. First, they are accountable for supporting the project team in achieving cost/schedule and financial objectives, and also accountable in their functional reporting chain to ensure that programs do not take unacceptable risks in their functional areas. For example, those from Engineering ensure that the engineering is done properly, using the established processes and tools approved by the functional organization. They are expected to “blow the whistle” to their functional management line if questionable engineering or quality practices are used by the project team, and they also serve as points of contact if project staff come across problematic issues to which the line program management is not responsive.

The functional management line is responsible for ensuring that the people it deploys to projects are accountable and satisfy their responsibilities. In safety and reliability engineering, for example, most lapses result from people not doing what the organization is relying on them to do. The result can sometimes be a multibillion-dollar disaster in which someone on the project team made a mistake (e.g., a typing error in input data to a launch vehicle) that was not caught by the several layers of project people and functionally deployed people who were accountable for checking and correcting such mistakes and who each failed to be accountable and to satisfy their responsibilities.

Risks from unaddressed ELSI concerns may, or may not, be less consequential. The concept of holding functional people accountable is

the same, and the intent is that when those accountabilities clearly include appropriate consideration of ethical, legal, and societal issues arising from research, such issues are more likely to be considered. But the committee notes that there are many ways to create and maintain such accountability, and does not think that any one way is necessarily best.

Last, an agency should subject all R&D projects carried out using agency resources to a screening to identify plausible ethical, legal, and societal issues that they might entail. This implies that agency staff must not be allowed to carry out R&D projects “off the books,” that is, to conduct projects without the knowledge of the senior agency management responsible for attending to ELSI concerns.

Recommendation 2: Interested agencies that support R&D on emerging and readily available technologies of military significance should develop and deploy five specific processes to enable these agencies to consider ethical, legal, and societal issues associated with their research portfolios: (a) initial screening of all proposed R&D projects for ELSI concerns, (b) review of projects that do raise such concerns, (c) monitoring of projects as they proceed for the emergence of unanticipated ELSI concerns and to make periodic midcourse corrections to the research when necessary, (d) engagement with various segments of the public as needed, and (e) periodic review of ELSI-related processes in the agency.

2.a—Initial screening of proposed R&D projects

Before supporting a project in a particular area of S&T research, agencies should conduct a preliminary assessment to identify ethical, legal, and societal issues that the research might raise. Both the sponsoring agency and project managers would have responsibilities for identifying if not resolving ethical issues that they believe might attend to the effort in question. The agency should require those seeking research funding to identify in their proposals the plausible ELSI concerns that they believe their research might raise. Using such information as a starting point, the funding agency should then make its own assessment about the existence and extent of such issues. Note that this initial assessment should be carried out for all R&D projects (both classified and unclassified).

At this stage, the goal is to identify whether the proposed research would raise significant ELSI concerns that require further consideration.

In most cases, the result of an initial screening will be “no, the project raises no new issues that have not been thoroughly explored before,” and assessment of the proposed research will proceed without any necessary further consideration of ethical, legal, and societal issues. This procedure

is not intended to assess the significance of the issues or the agency's response to them. It is intended solely to differentiate between research proposals that are explicitly determined to raise no new ELSI concerns and those that do—those in the former category should not be subject to further ELSI review in this phase.

How this identification process should be performed would surely vary with the setting. Depending on the size of the agency, the number of research proposals it handles, and the nature of that research (research on cosmology, for example, may raise fewer ethical and societal issues than research on specific weapons applications), the identification process might be performed by one employee as a part-time effort or may require a committee. It might be formal; it might be informal. The point is that it has to be done—and those who do it must have both enough knowledge of the underlying technology and enough familiarity with the kinds of ELSI concerns that are likely to arise to ensure that they can make sufficiently accurate decisions.

A systematic methodology is useful for identifying ethical, legal, and societal issues related to R&D. One such methodology is the framework described in Chapter 5, which can serve at least as a point of departure. Of course, no human decisions are completely accurate. The history described in Chapter 6 suggests that despite the best efforts of analysts to identify ethical issues that might arise in the course of an R&D effort, those efforts will be at best only partially successful, and that ethical issues are likely to arise or become important that were not predicted despite initial best efforts to do so.

A false positive, involving the identification of an ELSI concern that a proposal in fact does not raise, may be corrected in the next step, namely, the assessment process discussed in Recommendation 2.b. A false negative, involving the failure to identify an ELSI concern that a project in fact does raise, would need correction only if the research proposal is actually funded; the monitoring process discussed below in Recommendation 2.c is intended to help catch those false negatives.

2.b—Reviewing proposals that raise ELSI concerns

Once an agency has identified research proposals or projects that may raise complex ethical, legal, and societal issues, it needs to decide how to proceed. That requires some closer scrutiny of those issues, including asking how likely they are to arise, how serious they are likely to be, and whether there are ways to mitigate them.

This is, in essence, a risk assessment exercise, one that looks at the ELSI risks posed by the research in question. If and when such issues are identified, program managers should have the opportunity to take action

in response to such issues. (Of course, program managers are themselves subject to higher authorities, and the latter may take action as well.) Possible responses include not pursuing a given R&D effort, pursuing it more slowly, pursuing it in a modified form that mitigates the ethical or societal concerns, pursuing the original effort but also pursuing research to better understand the ethical or societal impacts, and so on. The responses should not be limited simply to a decision to proceed or not to proceed.

The method by which an agency conducts assessments of proposed R&D may vary. In some cases, several people may need to be involved in order to provide different perspectives—for example, someone from the agency's communication group or its legal counsel might, in some cases, make useful contributions to understanding the ethical and societal implications of the research. In some cases it may also be useful to bring in voices from outside the agency, such as experts in the technology, experts in the particular ethical, legal, and societal issues, or representatives of the groups that might be affected by the issues. All such possibilities are based on the idea that engagement with a variety of different intellectual and political perspectives increases the likelihood that relevant ELSI concerns will be revealed. Furthermore, because consideration of ethical, legal, and societal issues is fraught with fundamental questions of inclusivity and trust (e.g., whose opinions and ethical standards should be taken into consideration?), casting a broad net may forestall downstream politically powerful complaints about a lack of inclusivity.

It should be expected that the initial assessment of a proposed R&D project will not be correct in all aspects. If so, what is the value of an initial assessment if that assessment cannot be expected to predict the ethical, legal, and societal issues that are likely to arise? It is often said that no battle plan survives first contact with the enemy, but no commander believes that this undeniable reality obviates the need for planning battles. The very effort of planning assembles resources that are likely to be helpful in a battle, even if how and when such resources are used may be very different from what the original plan specified. In addition, the initial assessment is a concrete point of departure for evolving an approach to handling ELSI issues as circumstances change. Similar observations hold for an initial assessment of ethical, legal, and societal issues related to R&D on ERA technologies.

The process described here seems likely to call for a committee, but other methods may well be possible or better in some circumstances. The key is to have people with relevant knowledge look at the implications and decide what should be done. The answer may be “nothing” because the issues involved are seen, on closer examination, to be minor or non-existent. It may be to flag the research for decision by higher authorities in the agency. Or it could be anything in between.

One hard question about the process of proposal review for ELSI concerns is how it should interact with the process of making decisions on research projects or proposals. Should it take place before a funding decision, as part of the decision, or after the (initial) decision? Again, the committee believes that different models will be appropriate for different agencies and/or different research portfolios and volumes of research, even within a single agency. It is important, though, that the assessment be able to feed back into the research proposal, because one result of the assessment process may be a recommendation that the research be modified to mitigate some of the ethical and societal concerns identified.

2.c–Monitoring R&D projects for the emergence of ethical, legal, and societal issues and making midcourse corrections when necessary

Perfect prediction of significant ELSI concerns is virtually impossible, especially in an area as fraught with uncertainty as research on emerging and readily available technologies. Projects that seemed to raise substantial ethical, legal, and societal issues may turn out to raise none; projects that seemed to have no ethical or societal implications may turn out to have hugely important consequences.

A process for monitoring the course of R&D projects is thus essential to help agencies to adjust to such changing realities. If the perceived ELSI concerns change significantly during the course of a project (that is, if and when new issues are identified, if and when previous attempts to address already-identified issues prove inadequate, or if and when public perceptions change even if the issues themselves have not), programmatic or project responses are developed and the program or project plan can be modified accordingly. This is an adaptive approach that plans and relies on continual (or at least frequent) midcourse changes in response to such feedback.

An agency needs to be able to adjust to these changing realities. A twofold monitoring strategy would allow that kind of flexibility.

First, for projects for which the assessment process discussed in Recommendation 2.b did identify issues that required attention, that process should be repeated periodically during the life of the research. Such periodic assessment will enable an agency to see whether the research project needs fewer, more, or different methods to deal with those issues. It would also allow a decision as to whether the research, as it has developed, has surfaced ethical, legal, and societal issues that require that the research be examined, or examined again, at higher levels of the agency.

A monitoring process could, in principle, be similar to the initial screening process, with the important proviso that the baseline be updated to take into account what has been learned since the last look

at the project. To catch ethical, legal, and societal issues that may have appeared in the interim, the monitoring process should touch all projects in the agency's R&D portfolio, so that projects that were previously determined to not raise ELSI concerns can be reexamined. But the intent of this requirement is not to reopen a debate over a project as initially characterized but rather to see if new issues have arisen in the period of time since the last examination—and in most cases, a project originally determined to not raise ethical, legal, and societal issues will retain that status upon reexamination despite progress in the project. It may also be the case that projects originally determined to raise ELSI concerns have evolved in such a way that it becomes clear that they do not.

Second, for some projects, the review advocated in Recommendation 2.b will conclude that no ethical or societal issues require consideration or modification. Such projects should be reexamined periodically to see whether that situation has changed.

On either path, if the perceived ELSI concerns associated with an R&D project change significantly, the interested agency will have to adapt to those changes. When new issues are identified (or previous attempts to address already-identified issues prove inadequate) and programmatic or project responses are developed, the program or project plan can be modified accordingly. That is, an adaptive approach relies on continual (or at least frequent) midcourse changes in response to feedback.

How, if at all, should a follow-on assessment differ structurally from an initial assessment? On one hand, involving the same person or persons provides an important degree of continuity and reduces the burden of getting up to speed on any given project. On the other hand, involving others who were not involved in the initial assessment provides new perspectives that may be valuable and more likely to reveal new issues. A mix of those familiar and unfamiliar with a given project helps to resolve the tension between these two propositions, but a mix implies that at least two people must consider each project—a fact that entails a higher degree of overhead. Agencies must decide how to manage these tensions, and the outcome may well vary by agency.

These first three subrecommendations lay out the elements of a process for identifying, assessing, and monitoring ethical, legal, and societal issues that may arise from research. Box 8.1 provides an example.

2.d—Engaging with various segments of the public as needed

With the stipulation that engagement with various segments of the public does not necessarily mean coming to consensus with them, an agency's ELSI deliberations will often benefit from such external engagement. For example, public concerns about a given R&D project are often

Box 8.1 One Example of How to Implement Subrecommendations 2.a, 2.b, and 2.c

Subrecommendations 2.a, 2.b, and 2.c lay out the elements of a process for identifying, assessing, and monitoring ethical, legal, and societal issues that may arise from research. What follows is a concrete example of one way that a flexible and minimally bureaucratic process might be implemented. This is not the only possible method of implementation and it will not be, in all circumstances, the best, but it does provide an example of the committee's thinking. The example is based on an agency funding extramural research projects, but it could also be applied to other kinds of research support.

All researchers applying for funding support would be required to answer a question (or questions) in the application about the ethical, legal, and societal issues that they see as being raised by their research. As part of the review of the research proposal, someone within the agency would examine all proposals to identify which ones appear likely to raise significant ELSI concerns. Depending on the size and breadth of the research portfolio at the agency and its internal organization, that examination might be conducted by one person or several. Rarely if ever would the full-time effort of one employee be required.

The person in charge of the examination process would have the benefit of the applicant's self-assessment, but would not be bound by it. The screening process would result in one of two decisions. It might conclude that there were no significant ELSI concerns in this research. In that case, the proposal would be released to the more general funding process. Alternatively, the examination could conclude that the proposal did raise potentially significant issues. In that case, the proposal would be sent to the assessment process.

formulated in ELSI terms rather than in technical terms. As indicated above, policy makers must be prepared for the emergence of unforeseen outcomes of technology development and thus must have structures in place that will detect such outcomes and focus attention on them in a timely way. When unforeseen outcomes do emerge, policy makers must be prepared to communicate with the public using proven techniques (as described in Chapter 4 of this report). A developed strategy for public communication is also useful when anticipated ELSI concerns become public. Government actions in the United States ultimately depend, legally and practically, on the consent of the governed. Building public understanding of an agency's actions, the reasons for those actions, and the precautions the agency has taken will normally be the best strategy, for democracy and for the agency.

In addition, members of these various publics (examples include communities of expertise that may be relevant to an R&D project who are not formally associated with it, including technical experts, experts on risk

The assessment process could be done by a committee, made up of designated agency personnel, but with the power to ask for participation by other agency employees or even by outside experts when relevant. Early in the process the committee should ask itself whether its membership has the appropriate expertise. This committee would be charged with assessing the likelihood and significance of the ethical, legal, and societal issues that the research proposal raises. It would be empowered to conclude that the issues were not sufficiently important to require action, to recommend actions to mitigate the effects of those issues, to recommend against funding the research, or to refer the issues to higher authorities within the agency. It could also combine some of these actions, or take others as appropriate.

For research proposals that were funded, the funding agency might require an annual review for ethical, legal, and societal issues. Researchers might also be encouraged to bring to the attention of program managers new ELSI concerns if they become aware of them during the course of their work. Proposals that initially were not seen as raising such issues, either during the screening or after the assessment process, could be sent back through the screening process. The screening process, once again, could conclude that the research still did not raise any ethical or societal issues that required consideration; could conclude that the issues were modest enough to require only staff review; or could send the project to the assessment committee for possible action.

If the research proposal had initially reached the assessment committee, and its review raised significant issues regarding proposed research, then the assessment committee would review the research, its progress, and the ethical, legal, and societal issues it raises each year. It could then recommend changes as necessary.

assessment and communication, and those with ELSI expertise broadly defined) may have points of view that were not well represented in an agency's internal deliberations about a given R&D project. Engagement with these publics may well yield information that may have been overlooked or underweighted in these deliberations. Ongoing engagement throughout the course of a project may reveal the impending appearance of initially unanticipated ethical, legal, and societal issues, and thus provide early warning to program managers and enable a more rapid response if and when these new issues do appear. Finally, the mere fact of consultation and engagement with a wide range of stakeholders helps to defuse later claims that one perspective or another was ignored or never taken into account.

For example, the ethical perspectives of potential users of a given application may be relevant. If an application (as presented to a potential user) offends the user's ethical sensibilities, the likelihood that the user will actually use the application is obviously diminished. (Although it is

true that U.S. military users could be ordered to use a given application in any case, the same does not hold true for U.S. coalition allies, who might benefit from the capabilities afforded by a new application.)

Finally, a relevant stakeholder that interested agencies should engage is the community of researchers themselves. An agency that is considering substantive changes in its requirements for proposals and that wants researchers to attend to ethical, legal, and societal issues as part of the R&D it supports has some responsibility to engage with and inform the research community about what it means to do so. What is the rationale for these changes? How, if at all, will research projects have to change? What, if anything, does “attending to ethical, legal, and societal issues” mean in the context of decisions about specific proposals? The particulars of how best to proceed with such explanations almost certainly depend on the specific agency involved.

For R&D projects that are classified, public engagement is obviously constrained to a certain extent. Nevertheless, even if such projects can be discussed only with the cleared subsets of the various stakeholder groups, the result will still be more robust and defensible than if the project had not been discussed at all.

2.e–Periodically reviewing ELSI-related processes in an agency

As noted above, well-meaning policy statements are sometimes translated into excessively bureaucratic requirements when they have been implemented “on the ground.” To ensure that ELSI-related processes do not place undue burdens on researchers or on program managers in an agency, these processes should themselves be reviewed periodically to ensure that they are consistent with the intent of high-level policy statements regarding the handling of ethical, legal, and societal issues in the agency. If the agency finds that the promulgated policies and implementations are both consistent with the senior leadership’s intent and helpful to the agency, it has the option of advocating through appropriate chains of command similar efforts to other agencies that fund S&T research.

Recommendation 3: Interested agencies supporting R&D on emerging and readily available technologies of military significance should undertake an effort to educate and sensitize program managers to ethical, legal, and societal issues.

One critical element of effective implementation is education. As a general rule, program managers are not selected for their jobs on the basis of their knowledge of ELSI concerns that a given R&D effort might raise. Indeed, such individuals generally lack any formal training at all in such

matters, and it is unreasonable to expect these individuals to attend to (or even notice) ethical, legal, and societal issues in any systematic manner in the absence of such training. For work with military relevance, however, program managers are sometimes current or former military personnel, all of whom have had some training in and exposure to the laws of war.

In an agency that funds or oversees research likely to raise complex ethical, legal, and societal issues, the relevant staff should be educated in the problems that can arise, and have arisen, for similar agencies when those issues are ignored. The fate of the Total Information Awareness program and its intended proponents, as well as negative effects it had for DARPA overall, could be one useful object lesson.

If funding agencies are to screen, assess, and monitor research proposals and projects for possibly significant ethical, legal, and societal issues, they will need people with the ability to recognize those issues. Like all fields, the fields that assess ELSI concerns arising with various technologies have their own vocabularies. At the very least, the agency personnel dealing with these issues will have to understand, at some level, the relevant “language.” At the same time, those with ELSI responsibilities and/or expertise must have some understanding of the underlying research in order to identify issues that may or may not emerge.

One crucial, and easily overlooked, aspect of building internal expertise is building history. If an agency has no institutional memory of what ethical, legal, and societal issues it has faced, how it dealt with those issues, and what the consequences were, its ability to learn from that past is diminished. This diminished capability will be a particular problem for agencies that have frequent turnover. An interested agency needs to make it a priority to collect—and to use—information about how it has dealt with these issues. The agency party invested with functional accountability for ELSI concerns (as mentioned in Recommendation 1) might be in a good position to collect and organize that kind of information.

Once again, the committee does not believe there is one perfect method for building that expertise. Depending on the agency, it might make sense to hire employees who are trained in ethical, legal, and societal issues arising from technology. In other settings, it may make the most sense to provide existing agency employees with additional training to help them understand these issues. Without making a specific recommendation to use this particular mechanism, the committee notes that the Defense Acquisition University, an educational institution within the Department of Defense that seeks to educate professionals in the fundamentals of defense acquisition, could be a vehicle through which agency employees might be sensitized to ethical, legal, and societal issues.

In most cases, the committee expects that funding agencies will need to have several people involved in making decisions concerning ethical,

legal, and societal issues in research proposals and projects. One, or a few, might require extensive training, whereas for others involved in the assessment or monitoring process, more limited training may be sufficient. For example, in an agency with one person screening proposals or projects for ELSI concerns, that person might need substantial training. The other people involved at the assessment stage, though, might be sufficiently trained through a series of a few lectures or seminars, possibly even delivered online or in videos.

Recommendation 4: Interested agencies supporting R&D on emerging and readily available technologies of military significance should build external expertise in ethical, legal, and societal issues to help address such issues.

The need for some training or expertise in identifying and assessing ethical, legal, and societal issues may also exist within the research projects funded by an agency. One possible intervention that agencies could suggest for projects raising such issues could be that the project itself should include people who have had, or would receive, some training in dealing with those issues. For example, institutions that apply for funding from the National Science Foundation are required to specify how they will provide training and oversight in the responsible and ethical conduct of research to undergraduate students, graduate students, and postdoctoral researchers participating in the proposed research project.² Similar mechanisms might be used to promote awareness of ethical, legal, and societal issues in the next generation of researchers.

However, not all expertise should be, or can be, internal to an agency. Agencies should seek advice from external experts, because properly addressing some ELSI concerns will require a depth of knowledge that cannot realistically be expected of program managers or scientists. If such expertise is not immediately available, it should be cultivated. Such cultivation would have both immediate and longer-term benefits. It would help the agency directly by providing that expertise, but, in the longer run, it could also build knowledge, expertise, and even trust outside the agency about what it does about ethical, legal, and societal issues, and why.

In addition, outside advisors can help to reduce conflicts of interest and to ensure honest, objective feedback. Agency employees may be pressured or otherwise reluctant to be as forthcoming or straightforward as needed. Of course, even outside advisors are prone to the same vulnerabilities, if they are worried that harsh criticism means they will not be

² See, for example, <http://www.nsf.gov/bfa/dias/policy/rcr.jsp>.

retained in the future. But as outsiders, they presumably have less at risk than do agency employees.

Many methods exist for involving outside experts. They could be consulted on individual cases, on a consultant or contractual basis. At the other extreme, an agency might want to set up an advisory committee for agency leadership to consider ethical issues associated with ERA technologies in a national security context. An agency could bring in outside experts full-time for limited terms of 1 or 2 years, or could hold a quarterly lecture or seminar series.

There are some other ways that an agency might try to build a knowledgeable and useful relationship with outside experts. It might, for example, fund research into the ELSI implications of some of its work. The ELSI program at the National Human Genome Research Institute has done that for more than two decades. An agency might also host an occasional conference at the agency on the ethical, legal, and societal issues raised by the agency's research. Many approaches are possible; what is important is that an agency focuses on the goal of getting help from outside experts who understand ELSI concerns but also understand, to some extent, the agency and its mission. Such expertise may be rare, in which case new training grants on ethical, legal, and societal issues in S&T with regard to specific agency culture, procedures, and mission might be indicated.

8.3.2 Recommendation for Research-Performing Institutions and Individual Researchers

Recommendation 5: Research-performing institutions should provide assistance for researchers attending to ethical, legal, and societal issues in their work on emerging and readily available technologies of military significance.

Recommendations 1 through 4 address government agencies that fund research on ERA technologies of military significance. To the extent that these recommendations are adopted, researchers supported by these agencies may need assistance in identifying and responding to ethical, legal, and societal issues—indeed, many researchers are likely to not have previously considered at all or in any systematic manner ELSI concerns that might be associated with their research.

Depending on the research field, investigators can be expected to be more or less familiar with ethical, legal, and societal issues. In all cases, the starting point for efforts at assistance should be the assumption that researchers will want to do the right thing. In addition, all researchers should have access to assistance in anticipating the consequences of complex, uncertain research programs, and that assistance should be available

early enough in the research planning process to enable researchers to accommodate and benefit from it.

The committee believes that research-performing institutions should provide ELSI-related assistance to researchers working under their aegis in much the same way that they provide other functional support, such as legal, contracting, and various kinds of administrative support.

Research-performing institutions have processes and standards for addressing certain ELSI concerns in certain research contexts, such as protections for human subjects or environmental safety and health. When research on ERA technologies of military significance involves such issues, these processes and standards may be relevant. In cases where existing requirements and procedures are not applicable, research-performing institutions should encourage researchers to use their creativity and provide additional institutional assistance to examine ethical, legal, and societal issues and determine how best to proceed, rather than stipulating bureaucratic requirements for compliance with a single uniform policy.

Finally, certain research-performing institutions (e.g., universities) are likely to have access to in-house ELSI-related resources, such as academic researchers who specialize in ELSI-related matters. In such cases, these institutions may be able to play a useful matchmaking role in linking with sources of expertise scientific researchers who wish to address potential ethical, legal, and societal issues.

Providing assistance of this nature will help researchers to respond to any ethical, legal, and societal issues of concern to agencies that might fund their research.

In addition, many institutions performing research on ERA technologies with military significance already have in place policies and procedures to address a variety of ethical, legal, and societal issues that arise in some S&T research. For example, institutional review boards for research involving human subjects are quite common. Leveraging policies and procedures already in place to address ELSI concerns associated with certain kinds of research will help to minimize unnecessary overhead in institutions performing research on ERA technologies with military significance, and where policies and procedures already exist to address ethical, legal, and societal issues that are common to both military and civilian-oriented research, new ones should not be created to address them.

8.4 CONCLUDING OBSERVATIONS

Although ethical, legal, and societal issues have always accompanied the development of technology for military purposes, ERA technologies present special challenges because of the difficulties in anticipating how they might be researched and ultimately used. Fortunately, previous

efforts to address ethical, legal, and societal issues associated with S&T in a civilian context provide a useful base of knowledge for addressing such issues in a military context. Thus, addressing ELSI concerns in a military R&D context should not be regarded as an entirely new intellectual enterprise. That said, civilian-oriented ELSI mechanisms cannot be used in a military context without taking into account the special and unique aspects of that context.

Apparent in DARPA's charge to the committee is a concern about what it means to undertake R&D in an ethical manner. The committee applauds this concern, recognizes the difficulties posed by this concern, and hopes that its report is a first step forward in helping DARPA—and indeed all agencies that support military R&D—address these very important and human issues.

Appendixes

A

Committee Members and Staff

A.1 COMMITTEE MEMBERS

William F. Ballhaus, Jr., *Co-Chair*, is the retired president and chief executive officer of the Aerospace Corporation, an organization dedicated to the objective application of science and technology toward the solution of critical issues in the nation's space program. Ballhaus joined Aerospace in 2000 after an 11-year career with Lockheed Martin Corporation. At Lockheed Martin he served as corporate officer and vice president, engineering and technology, where he was responsible for advancing the company's scientific and engineering capabilities and for overseeing research and engineering functions. Prior to his tenure with Lockheed Martin, Ballhaus served as president of two Martin Marietta businesses, Aero and Naval Systems (1993-1994) and Civil Space and Communications (1990-1993). Before joining Martin Marietta, Ballhaus served as director of the NASA Ames Research Center (1984-1989). He also served as acting associate administrator for aeronautics and space technology at NASA Headquarters (1988-1989). He serves on the boards of Draper Laboratory and OSI Systems. He is a member of the National Academy of Engineering and completed two 3-year terms as a member of the NAE Council in 2007. He is an honorary fellow of the AIAA and served as its president in 1988-1989. He is a fellow of the Royal Aeronautical Society and the American Astronautical Society, and is a member of the International Academy of Astronautics. He serves on the Jet Propulsion Laboratory Advisory Council, and he served on the Defense Science Board, the NOAA Science Advisory Board, the Air Force Scientific Advisory Board

(co-chair, 1996-1999), and the NASA Advisory Council. He served as chair of the board of the Space Foundation. He is a graduate of the University of California, Berkeley, where he earned a Ph.D. in engineering and his bachelor's and master's degrees in mechanical engineering.

Jean-Lou Chameau, Co-Chair, took office as president of King Abdullah University of Science & Technology (KAUST) in Saudi Arabia on July 1, 2013. Chameau is president emeritus of the California Institute of Technology—Caltech—which he led for 7 years prior to joining KAUST. After receiving his engineering degree in France at the École Nationale Supérieure des Arts et Métiers and earning his Ph.D. in civil engineering from Stanford University, he had a distinguished career as a professor and administrator at Purdue University and the Georgia Institute of Technology (Georgia Tech). He then served as president of Golder Associates, a geotechnical consulting company, before returning to Georgia Tech as Georgia Research Alliance Eminent Scholar and vice provost for research. He became dean of its college of engineering, the largest in the United States, and then provost and vice president for academic affairs. Throughout his career, he has been committed to fostering excellence in science and technology, as well as promoting a multidisciplinary approach to research and education. He encouraged the development of programs in such areas as energy, medical science, and the environment, which can provide the dramatic scientific advances and new technologies society is seeking. He also promoted industry-university partnerships and the involvement of universities in economic development, including the development of new businesses and emphasis on advancing entrepreneurial and international opportunities for faculty and students. He has served on a number of public and industry boards, including the Council on Competitiveness, John Wiley & Sons, MTS, Safran, and the Academic Research Council of Singapore. He has received numerous awards for his contributions as an educator and university leader. He is a member of both the French Académie des Technologies and the U.S. National Academy of Engineering.

Marcus Feldman is currently a professor of biology in the Department of Biological Sciences at Stanford University. With L.L. Cavalli-Sforza in 1973, he originated the quantitative theory of cultural evolution, initiating a research program in cultural transmission and gene-culture coevolution. The efforts started the subdiscipline of cultural anthropology, also known as coevolution, gene-culture evolution, cultural transmission theory, and dual inheritance theory. The landmark work that ensued used models from population genetics to investigate the spread of culturally transmitted units. When *Cultural Transmission and Evolution: A Quantitative*

Approach was published in 1981, it inspired new research into the correlation of patterns of genetic and cultural dispersion. His own research into human molecular evolution for the Morrison Institute for Population and Resource Studies has investigated issues concerning the history of today's modern humans. Feldman is now working on three books—on gene-culture co-evolutionary theory, niche construction in evolutionary biology, and the sex-ratio issue in China—and also serves as academic director of Bridging the Rift, a project to develop collaborations between Israeli and Jordanian scientists. In addition to his teaching, research, writing, and directing, he is managing editor of *Theoretical Population Biology* and associate editor of *Genetics*, *Human Genetics*, *Annals of Human Genetics*, *Annals of Human Biology*, and *Complexity*. He is a former editor of *The American Naturalist*. Feldman is a member of the American Society of Human Genetics and a fellow of the American Academy of Arts & Sciences and of the California Academy of Sciences. The Hebrew University of Jerusalem has awarded him an honorary doctorate of philosophy, and Beijing Normal University and Xi'an Jiaotong University have each appointed him honorary professor. He earned his bachelor of science degree in 1964 at the University of Western Australia, and then 2 years later, his master of science in mathematics from Monash University in Australia. He earned his Ph.D. in biomathematics from Stanford University in 1969, after which he returned to Australia, where he had accepted a teaching position at La Trobe University in Melbourne.

Bran Ferren is the co-founder and chief creative officer of Applied Minds and is a designer of movie and theater special effects. Ferren is the former president of research and development of Walt Disney Imagineering, as well as the co-founder of Associates and Ferren, a visual effects company that supplied visual effects for *Star Trek V*, *Altered States*, *Little Shop of Horrors*, and *The Manhattan Project*. Ferren is also a member of a number of government advisory panels relating to national security and technology.

Baruch Fischhoff is Howard Heinz University Professor in the Departments of Social and Decision Sciences and of Engineering and Public Policy at Carnegie Mellon University, where he heads the decision sciences major. A graduate of the Detroit Public Schools, he holds a B.S. in mathematics and psychology from Wayne State University and an M.A. and a Ph.D. in psychology from the Hebrew University of Jerusalem. He is a member of the Institute of Medicine of the National Academies and is a past president of the Society for Judgment and Decision Making and of the Society for Risk Analysis. He chaired the Food and Drug Administration Risk Communication Advisory Committee and the National Research Council Committee on Behavioral and Social Science Research to

Improve Intelligence Analysis for National Security. He has been a member of the Eugene, Oregon, Commission on the Rights of Women, and of the Department of Homeland Security Science and Technology Advisory Committee. He has also been a member of the Environmental Protection Agency Scientific Advisory Board and was a chair of the Advisory Board's Homeland Security Advisory Committee. He has written or edited several books: *Acceptable Risk* (1981), *A Two-State Solution in the Middle East: Prospects and Possibilities* (1993), *Preference Elicitation* (1999), *Risk Communication: The Mental Models Approach* (2001), *Intelligence Analysis: Behavioral and Social Science Foundations* (2011), *Risk: A Very Short Introduction* (2011), *Communicating Risks and Benefits: An Evidence-Based User's Guide* (2011), *Judgment and Decision Making* (2011), *Risk Analysis and Human Behavior* (2011), and *Counting Civilian Casualties* (2013).

Michael Gazzaniga is the director for the SAGE Center for the Study of Mind at the University of California, Santa Barbara. He oversees an extensive and broad research program investigating how the brain enables the mind. Over the course of several decades, a major focus of his research has been an extensive study of patients who have undergone split-brain surgery that has revealed lateralization of functions across the cerebral hemispheres. In addition to his position in Santa Barbara, Gazzaniga is also the co-director of the Summer Institute in Cognitive Neuroscience, president of the Cognitive Neuroscience Institute, and the founding director of the MacArthur Law and Neuroscience Project. After completing his undergraduate degree at Dartmouth College, Gazzaniga earned a Ph.D. in psychobiology at the California Institute of Technology.

Henry Greely is a professor of law and co-director of the Program in Genomics, Ethics, and Society at Stanford University. A leading expert on the legal, ethical, and social issues surrounding health law and the biosciences, Greely specializes in the implications of new biomedical technologies, especially those related to neuroscience, genetics, and stem cell research. He frequently serves as an advisor on California, national, and international policy issues. He is chair of California's Human Stem Cell Research Advisory Committee and served from 2007 to 2010 as co-director of the Law and Neuroscience Project, funded by the MacArthur Foundation. Active in university leadership, Greely chairs the steering committee for the Stanford Center for Biomedical Ethics and directs both the law school's Center for Law and the Biosciences and the Stanford Interdisciplinary Group on Neuroscience and Society. Greely serves on the Scientific Leadership Council for the university's interdisciplinary Bio-X program. Before joining the Stanford Law School faculty in 1985, Greely was a partner at Tuttle & Taylor, and he served as a staff assistant

to the secretary of the U.S. Department of Energy, and as special assistant to the general counsel of the U.S. Department of Defense. He served as a law clerk to Justice Potter Stewart of the U.S. Supreme Court and to Judge John Minor Wisdom of the Court of Appeals for the Fifth Circuit. He received his J.D. from Yale Law School.

Michael Imperiale is a professor in the Department of Microbiology and Immunology at the University of Michigan Medical School. He joined the department in 1984 as the Arthur F. Thurnau Assistant Professor of Microbiology and Immunology and was subsequently promoted to associate professor in 1990 and professor in 1996. He is currently the Arthur F. Thurnau Professor of Microbiology and Immunology as well as associate chair of the department. In 2010 Imperiale was elected as a fellow of the American Academy of Microbiology, and in 2011 as a fellow of the AAAS. Before joining the University of Michigan, Imperiale carried out research training as a postdoctoral fellow at the Rockefeller University, where he first became interested in DNA tumor viruses, studying gene regulation in the human pathogen, adenovirus. Currently, Imperiale's research interests focus on the study of how DNA tumor viruses interact with the host cell, including how they traffic within the cell and how they persist. Imperiale is a member of the National Science Advisory Board for Biosecurity, a position he has held since 2005. He received his undergraduate and graduate training at Columbia University, receiving a B.A. in 1976, an M.A. in 1978, and a Ph.D. in 1981, all in biological sciences.

Robert H. Latiff is a private consultant, providing advice on advanced technology matters to corporate and government clients and universities. He retired from the U.S. Air Force as a major general in 2006. Latiff is an adjunct faculty member with the John J. Reilly Center for Science, Technology, and Values at the University of Notre Dame and a research professor at George Mason University. Immediately after his retirement from the Air Force Latiff was chief technology officer for Science Applications International Corporation's space and geospatial intelligence business. His last active duty assignment was at the National Reconnaissance Office, where he was director, advanced systems and technology, and deputy director for systems engineering. Latiff has also served as the vice commander, USAF Electronic Systems Center; commander of the NORAD Cheyenne Mountain Operations Center; and program director for the E-8 JSTARS surveillance aircraft. While in the U.S. Army, he served in both the infantry branch and the ordnance corps, where he commanded a tactical nuclear weapons unit, and he was also an assistant professor of engineering at the U.S. Military Academy at West Point. Latiff received his commission from the Army ROTC program at the University of Notre

Dame and later transferred to the Air Force. He received his Ph.D. and his M.S. in materials science and his B.S. in physics from the University of Notre Dame and is a graduate of the National Security Fellows Program at Harvard's JFK School of Government. Latiff is a recipient of the National Intelligence Distinguished Service Medal and the Air Force Distinguished Service Medal. He is a member and former chair of the National Research Council's National Materials and Manufacturing Board and is a member of the Air Force Studies Board.

James Moor is the Daniel P. Stone Professor of Intellectual and Moral Philosophy at Dartmouth College. He does research in computer ethics, philosophy of artificial intelligence, philosophy of the mind, philosophy of science, and logic. He is the editor of the book *The Turing Test: The Elusive Standard of Artificial Intelligence* (Kluwer, 2004) and for many years was the editor-in-chief of the philosophical journal *Minds and Machines*. He has served as the president of the International Society for Ethics and Information Technology (INSEIT). In 2003 he received the Association for Computing Machinery SIGCAS Making a Difference Award, and in 2006 he received the American Philosophical Association Barwise Prize for lifetime achievement in philosophy and computing.

Jonathan Moreno is the David and Lyn Silfen University Professor of Ethics at the University of Pennsylvania. Moreno is an elected member of the Institute of Medicine and has served as a senior staff member for three presidential advisory commissions. He was an Andrew W. Mellon postdoctoral fellow, holds an honorary doctorate from Hofstra University, and is a recipient of the Benjamin Rush Medal from the College of William and Mary Law School. His book *The Body Politic: The Battle Over Science in America* was named a Best Book of 2011 by *Kirkus Reviews*. He is also the author of *Mind Wars: Brain Science and the Military in the 21st Century* (2012). He is a member of the Governing Board of the International Neuroethics Society, a faculty affiliate of the Kennedy Institute of Ethics at Georgetown University, a fellow of the Hastings Center and the New York Academy of Medicine, and a past president of the American Society for Bioethics and Humanities.

Joel Moses is Institute Professor as well as a professor of computer science and engineering and engineering systems at MIT. Between 1974 and 1998 he served as MIT's provost, dean of engineering, head of the Department of Electrical Engineering and Computer Science (EECS), associate head of EECS, and associate director of the Laboratory for Computer Science. Moses served as the Engineering System Division's acting director from December 2005 through November 2007. He was acting director of the Center for Technology, Policy and Industrial Development from 2006

to 2010. Moses is a member of the National Academy of Engineering and is a fellow of the American Academy of Arts and Sciences, the American Association for the Advancement of Science, the Association for Computing Machinery, and the Institute of Electrical and Electronics Engineers. He led the development of the Macsyma system for algebraic formula manipulation and is the co-developer of the knowledge-based systems concept in artificial intelligence. His current interests include the complexity and flexibility of engineering systems and artificial intelligence. He holds a Ph.D. in mathematics, which he received from MIT in 1967.

Kenneth Oye is an associate professor of political science and engineering at MIT. After serving two terms as director of the MIT Center for International Studies (1992-2000), he is now forming a political economy and technology policy program within the center. He has taught on the faculties of the Kennedy School at Harvard University, the University of California, Princeton University, and Swarthmore College. He has published six books and numerous short studies in international relations, political economy, and science and technology policy. His books include *Economic Discrimination and Political Exchange*, *Cooperation Under Anarchy*, and a four-volume series on Carter, Reagan, and Bush administration foreign policies. His articles examine international export financing issues, regulatory diversity and trade, and a range of science and technology issues. He is now completing books on environmental regulation and trade and on uses of compensation in political economy. He has launched two projects that apply theories of political economy to problems of science and technology policy. With Lawrence McCray, he is studying knowledge assessment in areas marked by controversy over scientific issues. With Alliance for Global Sustainability and Finnish Environmental Institute support, he is examining the effects of environmental, health, and safety regulations on the competitive position of firms. Oye has served as a consultant to the U.S. Trade Policy Coordinating Committee on export financing issues (2002-2003), as a member of the Advisory Committee to the U.S. Export-Import Bank (1999-2001), as director of the Seminar XXI program (1994-2000), as an editor of the journal *World Politics* (1983-1987), as a trustee of the World Peace Foundation (1997-present), and as a member of the Council on Foreign Relations. He has been a co-principal investigator on a MacArthur Foundation Joint Harvard-MIT Transnational Security Program and on research projects on economic and environmental issues funded by the Alliance for Global Sustainability, the Center for Global Partnership, NEDO, MISTRA, and the Institute for International Economics. He holds a B.A. in economics and political science with highest honors from Swarthmore College and a Ph.D. in political science with the Chase Dissertation Prize from Harvard University.

Elizabeth Rindskopf Parker is the dean and a professor of law at the University of the Pacific, McGeorge School of Law. A noted expert on national security law and terrorism, Parker served 11 years in key federal government positions, most notably as general counsel for the National Security Agency; principal deputy legal adviser, Department of State; and general counsel for the CIA. In private practice, she has advised clients on public policy and international trade issues, particularly in the areas of encryption and advanced technology. She began her career as a Reginald Heber Smith Fellow at Emory University School of Law and later served as the director, New Haven Legal Assistance Association, Inc. Early in her career she was active in litigating civil rights and civil liberties matters, with two successful arguments before the U.S. Supreme Court while a cooperating attorney for the NAACP Legal Defense and Education Fund. Immediately before her arrival at McGeorge, she served as general counsel for the 26-campus University of Wisconsin system. A member of the American Bar Foundation and the Council on Foreign Relations, Parker is a frequent speaker and lecturer. Her academic background includes teaching as a visiting professor at Case Western Reserve Law School and Cleveland-Marshall State School of Law. Currently, Parker serves on two committees of the National Research Council, holds a presidential appointment to the Public Interest Declassification Board, and is a board member of the Sacramento Region Community Foundation. Parker received her B.A. and J.D. from the University of Michigan.

Sarah Sewall teaches international affairs and directs the Program for Human Rights and National Security at the John F. Kennedy School of Government at Harvard University. She is a member of the U.S. Department of Defense's Defense Policy Board Advisory Committee. Sewall is also the founder and faculty director of the Mass Atrocity Response Operations (MARO) Project and for 3 years was faculty director of the Carr Center for Human Rights Policy. She led the Obama Transition's National Security Agency Review process in 2008. During the Clinton Administration, Sewall served as the inaugural deputy assistant secretary of defense for peacekeeping and humanitarian assistance. From 1983 to 1996, she was senior foreign policy advisor to Senate Majority Leader George J. Mitchell, serving on the Democratic Policy Committee and the Senate Arms Control Observer Group. Before joining Harvard, Sewall was at the American Academy of Arts and Sciences, where she edited *The United States and the International Criminal Court* (2002). Her more recent publications include a comprehensive DOD study on efforts to mitigate civilian casualties, *Parameters of Partnership: U.S. Civil-Military Relations in the 21st Century* (2009), and the introduction to the *U.S. Army and Marine Corps Counterinsurgency Manual* (2007). She attended Harvard College and was a Rhodes Scholar at Oxford University.

Alfred Spector is the vice president of research and special initiatives at Google, Inc. He was recently vice president of strategy and technology and CTO of IBM's Software Business. Prior to that he was vice president of services and software at IBM Research. He was also founder and CEO of Transarc Corporation, a pioneer in distributed transaction processing and wide-area file systems, and was an associate professor of computer science at Carnegie Mellon University. While at CMU he did fundamental work in a number of areas, including the Andrew File System that changed the face of distributed computing. Spector received his Ph.D. in computer science from Stanford University and his A.B. in applied mathematics from Harvard University. He is a member of the National Academy of Engineering, a fellow of the IEEE and the ACM, and the recipient of the 2001 IEEE Computer Society's Tsutomu Kanai Award for work in scalable architectures and distributed systems.

John H. Tilelli, Jr., is the chairman and chief executive officer of Cypress International, Inc. He is a retired United States Army four-star general who served as vice chief of staff of the United States Army from 1994 to 1995; commanding general, United States Army Forces Command from 1995 to 1996; and commander-in-chief, United Nations Command, Republic of Korea/United States Combined Forces /United States Forces Korea from 1996 to 1999. Tilelli retired from the army on January 31, 2000. He graduated from Pennsylvania Military College, now Widener University, with a degree in economics in 1963 and was commissioned as an armor officer. He earned a master's degree in administration from Lehigh University in 1972 and graduated from the Army War College in 1983. He was awarded honorary doctoral degrees by Widener University and the University of Maryland. Tilelli served two combat tours in Vietnam, commanded the 1st Cavalry Division during Operation Desert Shield and Operation Desert Storm, and served four times in Germany. Upon his retirement from the United States Army Tilelli was appointed president and CEO of the USO Worldwide Operations.

Stephen J.A. Ward is professor and director of the George S. Turnbull Center of the University of Oregon in Portland. Previously he was director at the Center for Journalism Ethics at the University of Wisconsin-Madison, and before that he was director of the Graduate School of Journalism at the University of British Columbia in Vancouver, Canada. He is the author of the award-winning *The Invention of Journalism Ethics: The Path to Objectivity and Beyond* (2005). In addition, he is the author of *Global Journalism Ethics* (2010) and co-editor of *Media Ethics Beyond Borders: A Global Perspective* (2009). Ward is associate editor of the *Journal of Mass Media Ethics*. His articles and reviews have appeared in such journals as *Journalism Studies*; *Ecquid Novi: African Journalism Studies*; *Harvard Inter-*

national Journal of Press/Politics; and the *Journal of Mass Media Ethics*. He serves on many editorial and advisory boards for ethics organizations and for journals on media ethics and science. His research interests include the history of journalism ethics, ethical theory, global media ethics, and science journalism. Ward was a reporter, war correspondent, and newsroom manager for 14 years. He covered conflicts in Yugoslavia, Bosnia, and Northern Ireland. He then became the British Columbia bureau chief for the Canadian Press news agency in Vancouver. Ward has a Ph.D. in philosophy from the University of Waterloo, Ontario.

A.2 STAFF

Herbert S. Lin, Study Director, is chief scientist at the Computer Science and Telecommunications Board, National Research Council of the National Academies, where he has been the study director of major projects on public policy and information technology. These studies include a 1996 study on national cryptography policy (*Cryptography's Role in Securing the Information Society*), a 1991 study on the future of computer science (*Computing the Future*), a 1999 study of Defense Department systems for command, control, communications, computing, and intelligence (*Realizing the Potential of C4I: Fundamental Challenges*), a 2000 study on workforce issues in high technology (*Building a Workforce for the Information Economy*), a 2002 study on protecting kids from Internet pornography and sexual exploitation (*Youth, Pornography, and the Internet*), a 2004 study on aspects of the FBI's information technology modernization program (*A Review of the FBI's Trilogy IT Modernization Program*), a 2005 study on electronic voting (*Asking the Right Questions About Electronic Voting*), a 2005 study on computational biology (*Catalyzing Inquiry at the Interface of Computing and Biology*), a 2007 study on privacy and information technology (*Engaging Privacy and Information Technology in a Digital Age*), a 2007 study on cybersecurity research (*Toward a Safer and More Secure Cyberspace*), a 2008 study on health care information technology (*Computational Technology for Effective Health Care*), a 2009 study on offensive information warfare (*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*), and a 2010 study on cyberdeterrence (*Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options*). Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT. Avocationally, he is a long-time folk and swing dancer and a poor magician. Apart from his CSTB work, he is published in cognitive science, science education, biophysics,

and arms control and defense policy. He also consults on K-12 math and science education.

Rachelle Hollander directs the Center for Engineering, Ethics, and Society (CEES) at the National Academy of Engineering (NAE), which manages the NAE Online Ethics Center (www.onlineethics.org), a widely used resource for engineering and research ethics education. She is a principal investigator on several National Science Foundation (NSF)-funded projects and several subcontracts. For many years Hollander directed science and engineering ethics activities at NSF, where she was instrumental in the development of the fields of research ethics and professional responsibility, engineering ethics, and ethics and risk management. She has written articles on applied ethics in numerous fields and on science policy and citizen participation. Hollander is a fellow of the American Association for the Advancement of Science (AAAS) and a member of the Governing Board of the Association for Practical and Professional Ethics (APPE). In 2006, Hollander received the Olmsted Award “for innovative contributions to the liberal arts within engineering education” from the American Society of Engineering Education’s Liberal Education Division. She received her doctorate in philosophy in 1979 from the University of Maryland, College Park.

Frazier Benya is a program officer in the National Academy of Engineering’s Center for Engineering, Ethics, and Society (CEES). She manages the projects run by CEES and assists with the Online Ethics Center for Engineering and Research Web site. Her work at the NAE has focused on three areas in particular: education on climate change, engineered systems, and society; energy ethics education in science and engineering; and ethical and social issues with advancing military technologies. She received her Ph.D. in the history of science, technology, and medicine from the University of Minnesota in 2012 and her M.A. in bioethics, also from the University of Minnesota, in 2011. Her Ph.D. thesis focused on the history of bioethics and scientific social responsibility during the 1960s and 1970s that led to the creation of the first federal bioethics commission in 1974. Her M.A. work analyzed different types of institutional methodologies for considering the social implications of science with a focus on those that integrate scientific research with ethics research in the United States and Canada. During graduate school she worked on a project to create an online bioethics resource Web site, EthicShare.org, which indexed resources from multiple databases.

Jo L. Husbands is a scholar/senior project director with the Board on Life Sciences of the National Research Council, where she manages studies

and projects to help mitigate the risks of the misuse of scientific research for biological weapons or bioterrorism. She represents the U.S. National Academy of Sciences (NAS), on the Biosecurity Working Group of IAP: The Global Network of Science Academies, which also includes the academies of Australia, China, Cuba, Egypt, India, Nigeria, Poland (chair), Russia, and the United Kingdom. From 1991 to 2005 she was director of the NAS Committee on International Security and Arms Control (CISAC) and its Working Group on Biological Weapons Control. Husbands is currently an adjunct professor in the Security Studies Program at Georgetown University. Before joining the National Academies, she worked for several Washington, D.C.-based nongovernmental organizations focused on international security. She is a member of the Temporary Working Group on Education and Outreach in Science and Technology of the Organization for the Prohibition of Chemical Weapons and is a member of the Global Agenda Council on Nuclear, Chemical, and Biological Weapons of the World Economic Forum. She is also a fellow of the International Union of Pure and Applied Chemistry. She holds a Ph.D. in political science from the University of Minnesota and a master's in international public policy (international economics) from the Johns Hopkins University School of Advanced International Studies.

Anne-Marie Mazza joined the National Academies in 1995. She has served as senior program officer with both the Committee on Science, Engineering and Public Policy and the Government-University-Industry Research Roundtable. In 1999 she was named the first director of the Science, Technology, and Law Program, a position she continues to hold. Between October 1999 and October 2000, she divided her time between the STL Program and the White House Office of Science and Technology Policy, where she served as a senior policy analyst. She holds a B.A. in economics, an M.A. in history and public policy, and a Ph.D. in public policy from the George Washington University.

Eric Whitaker is a senior program assistant at the Computer Science and Telecommunications Board of the National Research Council. Prior to joining the CSTB, he was a realtor with Long and Foster Real Estate, Inc., in the Washington, D.C., metropolitan area. Before that, he spent several years with the Public Broadcasting Service in Alexandria, Virginia, as an associate in the Corporate Support Department. He has a B.A. in communication from Hampton University.

B

Meeting Agendas and Participants

The Committee on Ethical and Societal Implications of Advances in Militarily Significant Technologies That Are Rapidly Changing and Increasingly Globally Accessible held five open meetings starting in August 2011. These meetings included information-gathering sessions open to the public, as well as closed segments for committee deliberation. The committee heard from numerous presenters at these meetings. They include the following by meeting date and session.

MEETING 1

Tuesday, August 30, 2011

- | | |
|---------------------|--|
| 10:45 AM - 11:15 AM | Discussion of Charge with DARPA
Norman Whitaker, DARPA |
| 11:15 AM - 12:45 PM | Military Ethics and Law
Shannon French, Case Western University
(video) <ul style="list-style-type: none">• How and to what extent, if any, do military ethics differ from the law of armed conflict?
Ward Thomas, College of the Holy Cross <ul style="list-style-type: none">• How have norms of military conflict evolved with the introduction of new technologies? |

	Judith Miller, former Department of Defense general counsel
	<ul style="list-style-type: none"> • How do ethical/legal considerations enter into DOD acquisition decisions?
12:45 PM - 1:30 PM	Lunch
1:30 PM - 3:15 PM	<p>Military Futures: Emerging Contexts Peter Schwartz, Global Business Network</p> <ul style="list-style-type: none"> • What are the emerging/re-emerging contexts and trends in the global environment that are shaping military missions? <p>Consider:</p> <ul style="list-style-type: none"> —Non-state actors in conflict (e.g., insurgencies, terrorism); —Access to resources (food, energy, water) —Climate disruption —Ethnic/religious tensions and conflict —Economic pressures —Demographic changes —Social connectedness —Changes in regional military capacities and relationships —Technology “push” —Dual-use technologies and research
3:15 PM - 3:30 PM	Break
3:30 PM - 5:15 PM	<p>Future Military Missions Scott Wallace, U.S. Army (ret.), Tradoc</p> <ul style="list-style-type: none"> • What military missions are emerging in response to these trends? <p>Consider, for example:</p> <ul style="list-style-type: none"> —Peacekeeping, conflict reduction, humanitarian operations; nation-building —DOD support as authorized by law for domestic agencies within the continental United States —Traditional military activities, for example with respect to near-peer competitors
5:15 PM	Adjourn

Wednesday, August 31, 2011

- 8:30 AM - 10:15 AM Technologies for Meeting Emerging Military Missions
 George Lucas, U.S. Naval Academy
 Patrick Lin, California Polytechnic State University, San Luis Obispo, California
- How do the emerging/re-emerging contexts and military missions described earlier shape ethical, legal, and societal questions about military technology?
- Consider, for example, such questions as they relate to:
- Constraints on technologies intended to help protect troops, civilian populations, or particular subgroups; to support humanitarian missions or other peacekeeping operations
 - Technologies that kill vis-à-vis those that maim or that negatively or positively affect mental or psychological processes
 - Concerns regarding blowback from emerging technologies
 - Technologies that enable military operations at long range or that remove the “human-in-the-loop” from decision making (e.g., drones, cyber, robots)
 - Technologies for surveillance (including surveillance of populations as well as of military deployments and movements)
- 10:15 AM - 10:30 AM Break
- 10:30 AM - 12:30 PM Prior ELSI Efforts—Biomedical/Engineering Ethics
 R. Alta Charo, University of Wisconsin Law School
- Basic approach of and relevant history from biomedical ethics
- Joseph Herkert, Arizona State University
- Basic approach of and relevant history from engineering ethics; ethics of emerging technologies

MEETING 2**Wednesday, November 2, 2011**

8:00 AM - 8:30 AM	Breakfast
8:30 AM - 8:40 AM	Welcome and Housekeeping
8:40 AM - 10:35 AM	Technology Panel 1—Information Technology Technology and Applications—Peter Lee, Microsoft Research Ethics—Keith Miller, University of Illinois, Springfield Ethics and Societal Issues—Gloria Mark, University of California, Irvine Ethics of Research—Simson Garfinkel, Naval Postgraduate School
10:35 AM - 10:50 AM	Break
10:50 AM - 12:45 PM	Technology Panel 2—Neuroscience Basic Science—Scott Grafton, University of California, Santa Barbara Applications—Craig Stark, University of California, Irvine Ethics—Martha Farah, University of Pennsylvania (via video link)
12:45 PM - 1:30 PM	Lunch
1:30 PM - 3:25 PM	Technology Panel 3—Prosthetics Technology (arm)—Stuart Harshbarger, Contineo Robotics Technology (eye)—Daniel Palanker, Stanford University Technology (neurology)—Gerald Loeb, University of Southern California (via phone) Ethics—Nicholas Agar, Victoria University of Wellington, New Zealand (via Skype) Ethics—James Hughes, Trinity College
3:25 PM - 3:40 PM	Break

3:40 PM - 5:35 PM	Technology Panel 4—Synthetic Biology Fundamentals—George Church, Harvard University (via video link) Applications—Drew Endy, Stanford University Ethics—Nita A. Farahany, Vanderbilt University
5:35 PM - 6:15 PM	Reception with Speakers
6:15 PM - 7:45 PM	Dinner

Thursday, November 3, 2011

8:00 AM - 8:30 AM	Breakfast
8:30 AM - 10:15 AM	Crosscutting Synthesis and Discussion Judith Reppy, Cornell University George Khushf, University of South Carolina
10:15 AM - 10:30 AM	Adjourn

Questions for Technology Panels

Basic Science

What is the maturity of the underlying science for creating national security applications with significant operational value? What hard problems need to be resolved to enable such applications?

Applications

Assuming the hard scientific/technical problems described above can be resolved, what are the scope and nature of such national security applications?

How important are the potential national security applications for the future of the technology/field/etc. as opposed to, for example, potential commercial drivers of development?

Ethical and Societal Issues

How, if at all, do researchers in the field identify and address ethical issues that might apply to their research? What mechanisms exist to address latent ethical issues that are not noticed by researchers? (Leave out issues related to scientific misconduct.)

What ethical and societal issues arise if the national security applications described above can be successfully deployed?

What ethical and societal issues arise in the course of conducting basic and/or applied research oriented toward national security applications? How can or should attention to these issues affect directions and outcomes of basic and applied research oriented toward national security applications?

How, if at all, have the ethical and societal issues evolved as the technology has matured?

MEETING 3

Thursday, January 12, 2012

- | | |
|--------------------|--|
| 8:00 AM - 8:30 AM | Breakfast |
| 8:30 AM - 8:45 AM | Housekeeping |
| 8:45 AM - 10:45 AM | <p>Emerging Technologies and ELSI
Deborah Johnson, University of Virginia
Sheila Jasanoff, Harvard University, Kennedy
School of Government
David Rejeski, Woodrow Wilson Center
Malcolm Dando, University of Bradford
(respondent)</p> <ul style="list-style-type: none"> • How have various technology fields addressed ELSI concerns? • How and in what ways have these approaches been successful and unsuccessful? • How, if at all, have these fields managed uncertainties (prospectively) and inaccuracies (retroactively) in forecasts about what the future would bring? (Uncertainties and inaccuracies are intended to cover all domains in which they might be relevant—ELSI concerns, scientific or technical developments, national security applications.) • How, if at all, are the lessons learned from past and current approaches to ELSI issues being changed by: |

- A military/national security orientation or application of emerging technologies?
 —High degrees of accessibility to these technologies by nonmajor nation-states and/or subnational actors?
- 10:45 AM - 11:00 AM Break
- 11:00 AM - 12:45 PM Mechanisms Used by Government Agencies to Address ELSI Concerns (panel 1 of 2, panel 2 for April meeting)
 Kelly Moore, National Science Foundation
 Jean McEwen, National Human Genome Research Institute
 Valery Gordon, National Institutes of Health
 Fred Cate, Indiana University School of Law
 Ray Colladay, DARPA (retired)
- What are some of the mechanisms (e.g., regulations, rules, institutions) that agencies have used to address ELSI concerns? What prompts agencies to put these mechanisms in place?
 - What has been the impact on the course of scientific/technological research and progress when these mechanisms have been used?
 - How has the research community responded to such mechanisms?
 - How and in what ways, if any, could such mechanisms be usefully applied to the conduct of research with applications for national security?
- 12:45 PM - 1:30 PM Lunch
- 1:30 PM - 3:15 PM Technology Panel—Cyber Warfare
 Mark Seiden, Yahoo!
 Randall Dipert, University of Buffalo
 Neil Rowe, Naval Postgraduate School
- See attached questions (same as for November meeting)
- 3:15 PM - 3:30 PM Break

3:30 PM - 5:30 PM Technology Panel—Robotics and Automated Weapons
 Ron Arkin, Georgia Institute of Technology
 Peter Singer, Brookings Institution
 Jürgen Altmann, Technische Universität Dortmund, Germany

- See attached questions (same as for November meeting)

5:30 PM - 6:00 PM Reception

6:00 PM - 8:00 PM Dinner

Friday, January 13, 2012

8:00 AM - 8:30 AM Breakfast

8:30 AM - 10:30 AM Risk Assessment (panel 1 of 2, panel 2 for April meeting)

Paul Fischbeck, Carnegie Mellon University

- How to elicit expert judgments about the performance of deeply uncertain systems

Denise Caruso, Carnegie Mellon University

- How to responsibly conduct R&D in the context of emerging scientific understanding and complexity

Peter Hancock, University of Central Florida

- How to anticipate human use and misuse of new technologies

10:30 AM - 10:45 AM Break

10:45 AM - 11:45 AM Committee Discussion—Identification of Major Ideas

This session will focus on identifying the major ideas that committee members believe are important for inclusion in the report. To increase the efficiency of the idea extraction process, we'll use a procedure often used in industry to engage committee members in parallel.

We start with large sheets of butcher paper on the wall, each with the title of a chapter from the draft report (see attachment). An additional sheet is labeled “miscellaneous and other.” Each committee member will have a 3 × 5 sticky note pad; during this session, committee members write their ideas on these sticky notes, one idea per sheet. They then post their ideas on the relevant sheet of paper. Reading other ideas on the sheet often inspires people to think of yet other ideas, which they are free to post as appropriate. Sometimes committee members think of the same ideas—that becomes clear as multiple notes appear with the same idea. Over lunch, staff will examine the ideas that have been posted and will attempt to synthesize commonalities for presentation to the group at the start of the afternoon session.

11:45 AM - 12:45 PM	Lunch
12:45 PM - 3:15 PM	Committee Discussion
3:15 PM	Adjourn

Questions for Technology Panels

Basic Science

What is the maturity of the underlying science for creating national security applications with significant operational value? What hard problems need to be resolved to enable such applications?

Applications

Assuming the hard scientific/technical problems described above can be resolved, what are the scope and the nature of such national security applications?

How important are the potential national security applications for the future of the technology/field/etc., as opposed to, for example, potential commercial drivers of development?

Ethical and Societal Issues

How, if at all, do researchers in the field identify and address ethical issues that might apply to their research? What mechanisms exist to address latent ethical issues that are not noticed by researchers? (Leave out issues related to scientific misconduct.)

What mechanisms exist for consideration, correction, or redress of untoward consequences?

What ethical and societal issues arise if the national security applications described above can be successfully deployed?

What ethical and societal issues arise in the course of conducting basic and/or applied research oriented toward national security applications? How can or should attention to these issues affect directions and outcomes of basic and applied research oriented toward national security applications?

How, if at all, have the ethical and societal issues evolved as the technology has matured?

MEETING 4

Thursday, April 12, 2012

8:00 AM - 8:30 AM	Breakfast
8:30 AM - 8:45 AM	Welcome
8:45 AM - 10:45 AM	<p>Embedding Ethics in Research and Development Heather Douglas, University of Waterloo, Canada Alex John London, Carnegie Mellon University Nils-Eric Sahlin, Lund University, Sweden</p> <ul style="list-style-type: none"> • At what point (or points) in the R&D effort is societal and ethical expertise best brought to bear? Why? • A commonly stated desire of scientists is to ensure that societal and ethical review does not “unduly” affect the pace and nature of scientific progress. What does “unduly” mean? By what standards might one recognize a societal or ethical review that unduly affects a given R&D project?

- How and to what extent, if at all, do the kinds of societal and ethical expertise depend on the specific nature of the R&D being performed?
- What is necessary to facilitate respectful and honest communication between those with societal and ethical expertise and working scientists and technologists?
- How can expertise about societal and ethical matters be brought to bear on a given R&D effort?
- How can those charged with having such expertise and applying expertise to an R&D effort be kept from “going native” and being compromised?

10:45 AM - 11:00 AM Break

11:00 AM - 12:45 PM Risk Assessment

Paul Fischbeck, Carnegie Mellon University

Wandi de Bruin, Carnegie Mellon University

Arthur (Skip) Lupia, University of Michigan

Adam Finkel, Carnegie Mellon University

- What information do various publics need in order to judge social and ethical issues of emerging military technologies fairly?
- What organizational procedures should the sponsors of those technologies follow, in order to meet those information needs?
- What analytical methods are best suited to produce that information, considering the novelty, complexity, uncertainty, etc., of those technologies?
- What are the potential barriers to public understanding of that information, assuming that it is produced?
- How can we ensure that effective communications are created, tested, and disseminated in a timely fashion?
- What are examples of successful and unsuccessful programs for addressing these challenges?

- What additional research is most needed to provide a scientific foundation for risk analysis and communication, for emerging military technologies?

12:45 PM - 1:30 PM Lunch

1:30 PM - 3:15 PM Mechanisms, Panel 2
 William Brinkman, U.S. Department of Energy, Office of Science
 Carmen Maher, U.S. Food and Drug Administration, Office of the Chief Scientist
 Diana Hoyt, NASA, Office of the Chief Technologist
 Edward Knipling, U.S. Department of Agriculture (USDA)

- What are some of the mechanisms (e.g., regulations, rules, institutions) that agencies have used to address ELSI concerns? What prompts agencies to put these mechanisms in place?
- What has been the impact on the course of scientific/technological research and progress when these mechanisms have been used?
- How has the research community responded to such mechanisms?
- How and in what ways, if any, could such mechanisms be usefully applied to the conduct of research with applications for national security?

3:15 PM - 3:30 PM Break

3:30 PM - 5:30 PM Non-U.S. Perspectives on Ethics in Science and Technology
 Qiu Renzong, Chinese Academy of Social Science, China
 Frans Brom, Utrecht University, The Netherlands
 Steven Lee, Hobart and William Smith Colleges
 Montgomery McFate, U.S. Naval War College

The purpose of this panel is to consider the following question:

With respect to issues of ethics regarding science and technology as they may be applied to armed conflict, how do the perspectives of different nations, religious traditions, and cultures compare to those of the United States?

It is recognized that the ethics of science and technology and the ethics of war and armed conflict are fundamentally different areas. Accordingly,

- Professors Qiu Renzong and Frans Brom are requested to address ethics in science and technology from the Asian and European perspectives, respectively, and to speculate, if they wish, on the implications of Asian and European perspectives on ethics in science and technology as they might apply to military matters.
- Professors Steven Lee and Montgomery McFate are requested to compare different religious (Lee) and cultural (McFate) perspectives on armed conflict and war to U.S. perspectives that are based largely on “just-war” theory, and to speculate, if they wish, on the implications of these differences for how the United States might use new military technologies.

5:30 PM - 6:00 PM

Reception

6:00 PM - 8:00 PM

Dinner (with speakers)

Homework:

- Make comments regarding the report summary on sticky notes for placement in the morning.

- Each committee member will have a 3 × 5 sticky note pad to be used for recording thoughts on the material to be discussed on Friday (see Friday agenda below). Please record one thought per note sheet, and organize them by the topics below.
- If your comments don't fit into the categories listed below, record them anyway for the "miscellaneous" category.
- Also, please think about comments on two topics from Thursday's sessions:
 - How do non-U.S. perspectives affect our report? (from Thursday)
 - Embedding ethics into R&D (from Thursday)

Both will be discussed on Friday.

Friday, April 13, 2012

ALL FRIDAY SESSIONS ARE CLOSED.

MEETING 5

Monday, June 4, 2012

8:00 AM - 8:30 AM	Breakfast
8:30 AM - 10:00 AM	Nuclear Ethics George Perkovich, Nuclear Policy Program, Carnegie Endowment for International Peace (via videolink)
10:00 AM - 10:15 AM	Break
10:15 AM - 12:15 PM	Nonlethal Weapons David Fidler, Center for Applied Cybersecurity Research, Indiana State University Neil Davison, International Committee of the Red Cross (via videolink)

12:15 PM - 1:15 PM	Lunch
1:15 PM - 5:30 PM	Closed Session
5:30 PM - 8:00 PM	Reception and Dinner

Tuesday, June 5, 2012

ALL TUESDAY SESSIONS ARE CLOSED.

C

Research and Development Organizations Within the Department of Defense

The Department of Defense (DOD) supports extramural research and development on military technologies of interest and conducts in-house research as well. The DOD also supports a variety of medical research activities that are not mentioned in this appendix.

C.1 DOD-WIDE RESEARCH AND DEVELOPMENT

The Defense Advanced Research Projects Agency (DARPA) supports but does not itself conduct R&D for all branches of the DOD.¹ DARPA's mission is to maintain the technological superiority of the U.S. military and to prevent technological surprise from harming U.S. national security. DARPA research ranges from supporting scientific investigations in laboratories to building full-scale prototypes of military systems. DARPA also supports research in biology, medicine, computer science, chemistry, physics, engineering, mathematics, neuroscience, the social and behavioral sciences, and more.

DARPA is organized into six offices:²

- The Adaptive Execution Office (AEO) prepares and coordinates field trials of advanced technology developed by DARPA. At any moment,

¹ "Organizational Chart: Defense Advanced Research Projects Agency," available at <http://www.defense.gov/orgchart/#96>.

² "Our Work," available at http://www.darpa.mil/our_work/.

DARPA has technologies in all stages of development, ranging from nascent ideas to systems ready for fielding. Working with combatant commands and Service partners, AEO establishes relationships that enable the rapid insertion of these technologies into military operations and exercises to address requirements and enhance warfighting capabilities.

- Defense Sciences Office (DSO) programs bridge the gap from fundamental science to applications by identifying and pursuing the most promising ideas within the science and engineering research communities and transforming these ideas into new DOD capabilities. At the time of this writing, DSO was focusing on five program areas: physical science, neuroscience, materials, mathematics, and biology.

- The Information Innovation Office (I2O) seeks to ensure U.S. technological superiority in all areas where information can provide a decisive military advantage, including the conventional defense mission areas (e.g., intelligence, surveillance, reconnaissance, command, control, communications, computing, networking, decision making, planning, training, mission rehearsal, and operations support) and emergent information-enabled technologies and application domains (e.g., social science; human, social, cultural, and behavioral modeling; social networking and crowd-based development paradigms; natural-language processing, knowledge management, and machine learning and reasoning; medical/biological informatics; and information assurance and cyber-security). I2O programs currently focus on three areas:

- Technology-assisted understanding of adversary capabilities, intentions, and activities as well as local human, social, cultural, and behavioral factors.

- Warfighter empowerment in command and control over the physical elements of combat (e.g., weapons systems; intelligence, surveillance, and reconnaissance assets; and communications resources) through advanced computing technologies to improve military decision making, planning, training, mission rehearsal, and operations support.

- Connection of friendly forces in the face of adversary attacks on friendly network and computational resources.

- The Microsystems Technology Office (MTO) seeks to improve the capabilities and potential of commercial off-the-shelf technologies available to all players for the benefit of U.S. warfighters and to develop methods for countering threats (both incidental and intentional) that arise from sustained advances in cheap and readily available technologies. MTO also develops high-risk, high-reward technologies outside and beyond the scope of commercial industry to secure the DOD's technological superi-

ority. Today, MTO focuses on biological platforms; computing; electronic warfare; manufacturing; photonics; position, navigation, and timing; and thermal management.

- The Strategic Technology Office (STO) undertakes research and development of innovative technologies to support the DOD mission in current and emerging strategic areas including finding difficult targets; communications, electronic warfare, and networks; shaping the environment; and foundational strategic technologies.

- The Tactical Technology Office (TTO) pursues high-risk, high-pay-off tactical technology and development of rapid, mobile, and responsive combat capability for advanced weapons, platforms, and space systems. The TTO seeks revolutionary improvement (order-of-magnitude improvement rather than incremental improvement) in existing capabilities and technologies and systems that facilitate “game-changing” tactics, techniques, and procedures across the entire spectrum of armed conflict. In addition, the TTO invests in research and technologies that enable strategic advantage over technological surprise in advanced weapons, platforms, and space systems.

Box C.1 provides a sampling of recent DARPA programs.

DARPA also supports R&D on technology useful to the intelligence community, although it is not the only source of technology for that community.³

C.2 SERVICE-SPECIFIC RESEARCH AND DEVELOPMENT

In addition to the DOD-wide R&D supported by DARPA, the military services support extramural R&D and conduct in-house R&D on technologies relevant to their service needs. The Army Research Office, the Office of Naval Research, and the Air Force Office of Scientific Research support extramural work, while the Naval Research Laboratory, the Army Research Laboratory, and the Air Force Research Laboratory are responsible for in-house R&D. Box C.2 illustrates some of the in-house projects conducted by these organizations.

³ As an example, the intelligence community was intimately involved in the development of remotely piloted vehicles for surveillance, later versions of which were equipped with lethal weapons.

Box C.1 A Sampling of Recent DARPA Programs

Information Innovation Office

Cyber Defense (Cyber Genome); see [http://www.darpa.mil/Our_Work/I2O/Programs/Cyber_Defense_\(Cyber_Genome\).aspx](http://www.darpa.mil/Our_Work/I2O/Programs/Cyber_Defense_(Cyber_Genome).aspx).

The Cyber Defense Program is

developing the core computing and networking technologies required to protect DOD's information, information infrastructure, and mission-critical information systems. This effort includes new cyber-forensic techniques to automate the discovery, identification, and characterization of malware variants and thereby accelerate the development of effective responses. Such responses could include dynamic quarantine techniques that employ static and dynamic code analysis for program understanding. The Cyber Defense Program is also developing network traffic monitoring techniques with performance and scalability that are orders of magnitude better than those seen with conventional approaches. The technologies being developed by the Cyber Defense Program will provide cost-effective cyber security and survivability solutions that enable DOD information systems to operate correctly and continuously even when they are attacked.

Adaptive Execution Office

Crosshairs; see http://www.darpa.mil/Our_Work/AEO/Programs/CROSSHAIRS.aspx. (At the time of this writing, this Web page is no longer available; however, an archived version of the page can be found at https://web.archive.org/web/20130722165614/http://www.darpa.mil/Our_Work/AEO/Programs/CROSSHAIRS.aspx.)

The Crosshairs program seeks to develop

a vehicle mounted threat detection and countermeasure system that will detect, locate, and engage shooters, as well as defeat a variety of threats including bullets, rocket propelled grenades, anti-tank guided missiles, and direct fired mortars, while stationary and moving. Threat identification and localization will be accomplished in sufficient time to enable both automatic and man-in-the-loop responses. The weapon station will be equipped with visual and infrared cameras for collecting forensic and judicial evidence and for rapid dissemination of combatant location information for effective concealment and counterfire.

Defense Sciences Office

Cognitive Technology Threat Warning System (CT2WS); see [http://www.darpa.mil/Our_Work/DSO/Programs/Cognitive_Technology_Threat_Warning_System_\(CT2WS\).aspx](http://www.darpa.mil/Our_Work/DSO/Programs/Cognitive_Technology_Threat_Warning_System_(CT2WS).aspx). (At the time of this writing, this Web page is no longer available; however, an archived version of the page can be found at [https://web.archive.org/web/20130221145010/http://www.darpa.mil/Our_Work/DSO/Programs/Cognitive_Technology_Threat_Warning_System_\(CT2WS\).aspx](https://web.archive.org/web/20130221145010/http://www.darpa.mil/Our_Work/DSO/Programs/Cognitive_Technology_Threat_Warning_System_(CT2WS).aspx).)

continued

Box C.1 Continued

Recognizing the warfighter's need to see and identify threats at long distance, the Cognitive Technology Threat Warning System program sought to assemble different technologies into

soldier-portable visual threat detection devices. These systems will provide greater visual information about a warfighter's surroundings while providing tools to initiate an early response when threats emerge. The program will integrate areas of technology such as flat-field, wide-angle optics, large-pixel-count digital imaging, and cognitive visual processing algorithms. Other features include ultralow-power analog/digital hybrid signal processing, operator neural signature detection processing, and operator interface systems. Success in this effort will result in a composite software/human-in-the-loop system capable of high-fidelity detection with extremely low false alarm rates without adding to already significant warfighter combat loads.

Microsystems Technology Office

Living Foundries; see http://www.darpa.mil/Our_Work/MTO/Programs/Living_Foundries.aspx.

The Living Foundries program seeks to create an engineering framework for biology, speeding the biological design-build-test cycle and expanding the complexity of systems that can be engineered. The program aims to develop new tools, technologies, and methodologies to decouple biological design from fabrication, yield design rules and tools, and manage biological complexity through abstraction and standardization.

Box C.2 Illustrative Service Laboratory Activities

Air Force Research Laboratory

Counter-electronics High-powered Microwave Advanced Missile Project (CHAMP); see https://www.fbo.gov/index?print_preview=1&s=opportunity&mode=form&id=9fae0cfe0f33a0dc38d99b95a8b31eed&tab=core&tabmode=list.

In 2008, AFRL was seeking to develop and demonstrate the capability and operational utility of a high-power microwave (HPM) aerial demonstrator. According to the solicitation, the objective of this effort was as follows:

to develop, test, and demonstrate a multi-shot and multi-target HPM aerial demonstrator capable of degrading, damaging, or destroying electronic systems. For this effort, the contractor shall develop a compact HPM payload for integration into an aerial platform. The contractor shall produce five aerial demonstrators. One aerial platform without the HPM source shall be developed for a flight test to demonstrate delivery, controllability, and fusing. The remaining four aerial platforms with the integrated HPM source shall be developed for flight testing, demonstration, and HPM effects tests. Of the four HPM prototypes one shall be used for ground tests, two shall be used for flight tests, and the remaining one shall be used as a back-up for the flight test.

CHAMP, which renders electronic targets useless, is a nonkinetic alternative to traditional explosive weapons that use the energy of motion to defeat a target. CHAMP allows for selective high-frequency radio wave strikes against numerous targets during a single mission. "This technology marks a new era in modern-day warfare," said Keith Coleman, CHAMP program manager for Boeing Phantom Works. "In the near future, this technology may be used to render an enemy's electronic and data systems useless even before the first troops or aircraft arrive."¹

Space Fence

Space Fence is envisioned as the following:

a system of up to two land-based radars, with the first located at Kwajalein Atoll in the Marshall Islands, to track objects entering Earth's orbit. According to program officials, it will form the foundation of improved space situational awareness by expanding the ability to detect, track, identify, and characterize orbiting objects such as commercial and military satellites, smaller objects, maneuvering satellites, break-up events, and lower-inclination objects.

"Space situational awareness is a continual concern and challenge for U.S. and ally nations," said Ken Francois, Space Fence program manager. "The Space Fence program will increase the capability to provide predictability in reducing the chance of a collision or attack."²

continued

Box C.2 Continued

Army Research Laboratory

MyWIDA (My Weather Impacts Decision Aid); see <http://www.arl.army.mil/www/default.cfm?page=1416>.

MyWIDA is

a knowledge-based expert system that employs a database of rules for meteorological critical values and impacts. Its Web services and associated applications automate the prediction and display of these weather impacts. MyWIDA's collection of rules and associated system critical values aids the commander in selecting an appropriate platform, system, and subsystem; personnel, including soldier performance; or sensor, collectively referred to here as assets, under given or forecast weather conditions, providing qualitative weather impacts for the selected assets.

Development of Quantum Computing Technology; see <http://www.arl.army.mil/www/pages/8/QCTBAA2010%20Final.pdf>.

ARO proposals for quantum computing include research areas such as:

- Robust solid-state qubits and related technologies, specifically work to advance the development of single- and few-qubit solid-state devices, and to advance related supporting technologies;
- Short- to medium-range quantum information transfer in solid-state systems (both on-chip and off-chip transfer) without large overhead costs (e.g., without doing a large number of swap gates); and
- Efficient verification/validation of quantum computing components. Possible topics include, but are not limited to, advances in or alternatives to quantum tomography; methods for extracting fidelity of gate or computation success; and methods or procedures for verifying complex quantum computations that cannot be classically simulated.

Naval Research Laboratory

Miniature Microbial Fuel Cells; see http://www.nrl.navy.mil/techtransfer/fs.php?fs_id=ENE01.

Miniature microbial fuel cells (MFCs) can be used as follows:

for harvesting energy from aerobic aqueous environments. An MFC is powered by passive nutrient diffusion instead of energy-draining pumps used in other MFCs, thereby increasing the net energy output. The NRL design sequesters electrochemically active microbes in the cell, rather than relying on environmentally available bacteria. This allows the NRL MFC to be placed in a wide range of aerobic aqueous environments, not only in the bacteria's natural habitat at the sediment/water interface. Unlike other MFCs, which require relatively costly proton exchange membranes to maintain separation between protons and electrons, the NRL MFC uses inexpensive nanoporous membranes made from polycarbonate or other materials to confine the microbes. The resulting MFC designs are capable of generating microwatts to milliwatts, depending upon size (75 μL to 5 mL) and operating conditions (cathode catalyst, nutrients available, etc.). Many of the designs can be connected easily in series or in parallel for additional power generation. With the addition of a booster circuit, these MFCs can be used as a long-term power supply for underwater autonomous sensors and LEDs.

Electromagnetic Railgun; see <http://www.onr.navy.mil/en/Science-Technology/Departments/Code-35/All-Programs/air-warfare-352/Electromagnetic-Railgun.aspx>.

The Office of Naval Research expressed interest in electromagnetic railguns in 2005. According to the public Web page cited above,

The Electromagnetic Railgun Innovative Naval Prototype (INP) was initiated in 2005. The Phase I goal of 32 megajoule muzzle energy proof-of-concept demonstration has been achieved. A future weapon system at this energy level would be capable of launching a 100-nautical-mile projectile. This launch energy has the advantage of being able to stress many components to evaluate full-scale mechanical and electromagnetic forces. Phase I was focused on the development of launcher technology with adequate service life, development of reliable pulsed-power technology, and component risk reduction for the projectile. Phase II, which started in 2012, will advance the technology for transition to an acquisition program. Phase II technology efforts will concentrate on demonstrating a 10-rounds-per-minute firing rate. Thermal management techniques required for sustained firing rates will be developed for both the launcher system and the pulsed-power system. The railgun is a true warfighter game-changer. Wide-area coverage, exceptionally quick response, and very deep magazines will extend the reach and lethality of ships armed with this technology.

¹ See http://www.boeing.com/Features/2012/10/bds_champ_10_22_12.html.

² See <http://www.afmc.af.mil/news/story.asp?id=123330647>.

D

Established Institutional Mechanisms for Addressing Ethical, Legal, and Societal Issues

D.1 DOD LAW-OF-ARMED-CONFLICT REVIEW AND TREATY COMPLIANCE

The 1977 Additional Protocol I of the Geneva Conventions of August 12, 1949 (to which the United States is a signatory) states in Article 36 that with respect to “development, acquisition or adoption of a new weapon, means or method of warfare, [a signatory] is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable.”¹ Thus, weapons acquired by the Department of Defense are subject to a review that determines whether the normal or expected use of the weapon is consistent with the law of armed conflict (LOAC).² (According to Parks, the “normal and expected use” of a weapon is associated

¹ International Committee of the Red Cross (ICRC), *Additional Protocol I to the Geneva Conventions on the Protection of Victims of International Armed Conflicts*, June 8, 1977, available at <http://www.icrc.org/ihl.nsf/b466ed681ddfcfd241256739003e6368/f095453e41336b76c12563cd00432aa1!OpenDocument>.

² The legal authority for this review is derived from a variety of DOD regulations: U.S. Department of Defense Directive 5000.1, “Defense Acquisition,” March 15, 1996 (hereinafter DODD 5000.1); U.S. Department of the Army, Army Regulations 27-53, “Review of Legality of Weapons Under International Law,” January 1, 1979 (hereinafter AR 27-53); U.S. Department of the Navy, Secretary of the Navy Instructions 5711.8A, “Review of Legality of Weapons Under International Law,” January 29, 1988; U.S. Department of the Air Force, Air Force Instruction 51-402, “Weapons Review,” May 13, 1994 (hereinafter AFI 51-402).

with the “means and method of warfare.”³) Notably, the review is “not required to foresee or analyze all possible misuses of a weapon, for almost any weapon can be misused in ways that would be prohibited.”

In accordance with Additional Protocol I (AP I), the LOAC review is confined to “weapons, means or method of warfare”; thus, research or development work that is not intended to result in a weapon being procured is not included. In addition, AP I does not define what is covered by the term “weapon.” The U.S. military services (Army, Navy, Air Force) do have regulations that specify what is covered and thus what is subject to LOAC review:

- *Army.*⁴ Weapons are defined as “all conventional arms, munitions, materiel, instruments, mechanisms, or devices which have an intended effect of injuring, destroying, or disabling enemy personnel, materiel or property.” Weapons systems refer to the weapon itself and those components required for its operation, but the definition is limited to those components having a direct injurious or damaging effect on individuals or property (including all munitions such as projectiles, small arms, mines, explosives), and that are injury- or casualty-producing.

- *Navy.*⁵ Weapons or weapon systems for the purpose of the legal review are defined as “all arms, munitions, materiel, instruments, mechanisms, devices and those components required for their operation, that are intended to have an effect of injuring, damaging, destroying, or disabling personnel or property, [including] non-lethal weapons. For [the] purpose of the legal review, weapons do not include launch or delivery platforms, such as, but not limited to, ships or aircraft, but rather the weapons or weapon systems contained on those platforms.”

- *Air Force.*⁶ Weapons are defined as “devices designed to kill, injure or disable people, or to damage or destroy property. Weapons do not include devices developed and used for training and practice; aircraft, intercontinental ballistic missiles, and other launch platforms; or electronic warfare devices.”

³W. Hays Parks, “Conventional Weapons and Weapons Reviews,” *Yearbook of International Humanitarian Law* 8:55-142, 2005.

⁴AR 27-53, January 1, 1979; see Federation of American Scientists, available at <http://www.fas.org/irp/DODdir/army/ar27-53.pdf>.

⁵U.S. Department of the Navy, Secretary of the Navy Instructions 5000.2C, “Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System,” November 19, 2004, p. 23, para. 2.6.

⁶AFI 51-402, May 13, 1994.

Parks points to various issues in these definitions.⁷ For example, he notes the difference between a weapon and a weapons system, and points out that in essence these regulations exclude from review parts of a system that do not cause injury. While he accounts for the possibility that devices for electronic warfare (e.g., jammers) might be included, he also notes that the Air Force definition specifically excludes these devices from LOAC review.

AP I does not specify when in the life cycle of a weapon a review must be conducted. Parks indicates only that the LOAC review takes place “early” in the acquisition process. At the time of the writing of the present report (summer 2013), there is no written guidance known to the committee specifying precisely when in the acquisition process such a review must take place.

Parks, who has personally conducted many LOAC reviews of weapons to be acquired, argues that the process has been successful and effective. In his words,

program managers generally have a good sense of and respect for the laws of war, and are cognizant of areas that may raise legal issues. This [familiarity] prompts requests for legal reviews early in the research, development and acquisition process, particularly where the office responsible for conducting the legal review has taken the necessary steps to identify itself and the requirement to engineering, research, development and acquisition commands, and establish an effective working relationship.

He indicates the importance of speaking at professional meetings of weapons development and acquisition experts to inform attendees of the review program, to explain the rationale behind the program, and to indicate the steps or procedures to be taken. In addition, he stresses the need to convince program managers that the review is intended to assist rather than hinder the acquisition process, even though there may be individual instances in which weapons or munitions may be found legally unacceptable.

Finally, Parks notes that to the best of his knowledge, there has never been a delay in providing weapons reviews “as a result of the nature of the [DOD] legal review process”; delays have occurred only when the requester has “failed to provide adequate information for the conduct of the legal review.”

The committee notes that this legal review necessarily takes place after the point at which a specific weapon is available to review; it does

⁷ W. Hays Parks, “Conventional Weapons and Weapons Reviews,” *Yearbook of International Humanitarian Law* 8:55-142, 2005.

not apply to research and development efforts. Moreover, the review is—by assumption—narrow. It examines the weapon only in the context of its stated concept of operations (that is, how the weapon is expected to be used). It is also limited to LOAC issues, with broader ethical or societal issues not within scope.

Similar processes attach to efforts that might implicate obligations stemming from treaties that constrain or restrict research or development in some way.

D.2 CODES OF ETHICS AND SOCIAL RESPONSIBILITY IN MEDICINE, ENGINEERING, AND SCIENCE

Medicine, engineering, and science are fields that generally hold practitioners accountable for considering at least some of the ethical ramifications of their medical, technical, or scientific work. In some cases, these ramifications include those related to matters such as safety and the protection of human subjects; in others, they include those related to the impact of such work on the broader society at large.

Professional standards and codes of ethics may be implied or implicit rather than codified or formalized, and may incorporate standards for behavior (what must a responsible practitioner do in providing services to clients) as well as a sense of social responsibility (e.g., a responsibility for practitioners to provide services and expertise to society in addition to those they provide to their clients; a responsibility to protect a vulnerable public from harm).

Brian Rappert identifies three broad categories of codes:⁸

- *Aspirational codes* (often designated as “codes of ethics”) set out ideals that practitioners should uphold, such as standards of research integrity, honesty, or objectivity. . . .
- *Educational/advisory codes* (often designated as “codes of conduct”) go further than merely setting aspirations by providing guidelines suggesting how to act appropriately. . . .
- *Enforceable codes* (often designated as “codes of practice”) seek to further codify what is regarded as acceptable behavior. Rather than inspiring or educating in the hope of securing certain outcomes, enforceable codes are embedded within wider systems of professional or legal regulation.

⁸ Brian Rappert, “Towards a Life Science Code: Countering the Threats from Biological Weapons,” Bradford Briefing Paper No. 13, September 2004, available at <http://www.brad.ac.uk/acad/sbtwc>.

In general, these standards and codes of ethics serve three important functions:

- They make clear to practitioners that they do have affirmative responsibilities to consider ethical and societal issues that go beyond the narrow scope of their clients' stated needs.
- They make clear to society that practitioners recognize an obligation to society to consider such ethical and societal issues.
- They provide standing for practitioners to resist pressures to proceed in technical directions that may be harmful to society at large and provide, when necessary, a justification for supporting social considerations ahead of financial, management, or technical goals in decisions.

Professional standards have often emerged from the process by which a field becomes a profession but have also developed without experts forming a profession. Some experts, like physicians and some engineers, identify themselves as professionals (as further described below).

Historically, a profession by definition is self-regulating, is autonomous, and serves clients. Often it organizes a society for its members that sets rules and standards and represents its members in the larger society.⁹ The self-regulating component often involves standardized education requirements for degrees, licensing, or certification, as well as codes of conduct or ethics that are enforceable. Society grants autonomy to professions in exchange for this self-regulation, a privilege that results in the restriction of the practice of the profession to qualified individuals only, thereby providing some protection to society.¹⁰ Autonomy and self-regulation in turn allow professionals to be the sole experts in a society in one specific area. Over time the historical understanding of a profession has evolved and broadened in common parlance to include fields with

⁹ Michael Davis, "Defining Engineering: How to Do It and Why It Matters," *Journal of Engineering Education* 85 (April 1996):99, 1996, available at http://www.synbioproject.org/process/assets/files/6452/_draft/davis_defining_engineer.pdf.

¹⁰ More specifically, professions traditionally assume responsibilities for self-regulation, including the promulgation of certain standards to which all members are supposed to adhere. These standards are of two kinds: technical standards that establish the minimum conditions for competent practice, and ethical principles that are intended to govern the conduct of members in their practice. In exchange for exercising this responsibility, society implicitly grants professions a degree of autonomy. The privilege of this autonomy in turn creates certain special obligations for the profession's members.

See Advisory Committee on Human Radiation Experiments, *Part I, Ethics of Human Subjects Research: A Historical Perspective*, Final Report, p. 115, Government Printing Office, Washington, D.C., 1995.

experts who have technical or topical expertise and can join voluntary societies with standards of behavior or codes of ethics.

The professional standards and codes of ethics that help practitioners to maintain their professions' standing in society change over time and are continually being renegotiated, as is the understanding of what makes a field a profession.

The historical origins of social responsibility are significant because they frame the manner in which social responsibility is understood in medicine and engineering compared to science. Physicians' and engineers' social responsibility traditionally has been about upholding their professional standards (which include standards of social responsibility), whereas social responsibility in science traditionally has been about upholding the social contract that results in funding and intellectual freedom for scientists.

D.2.1 Medicine and Engineering

The medical profession exemplifies well the understanding of professional social responsibility. Physicians take some version of the Hippocratic Oath upon graduation from medical school. Further, the medical profession sets education standards through the leadership of the American Medical Association and the Association of American Medical Colleges, both nonprofit member organizations, with the latter especially focused on academic medicine, as well as through licensing requirements through state medical boards. Through the American Medical Association, the profession also has a code of ethics that concerns physicians' interactions with each other and with their patients. However, in addition to the professional ethics code, public policy and legal rulings since the 1960s have increasingly regulated the ethical conduct of physicians, especially in regard to research on human subjects.

The medical profession contains society's experts on medicine and thus is allowed a considerable degree of autonomy in medical matters. The field has evolved around serving its clients, the patients. Physicians' social responsibility developed out of their standing as a profession in society and their desire to maintain their authority and autonomy. Second to serving their patients, physicians are expected to inform, warn, and protect the general public in medical issues. An example is the responsibility that physicians have to serve society in epidemics even at the risk of their own health.

The engineering field also developed as a profession characterized by accreditation, licensure, service to clients, and organization into societies. Engineers set their own standards for education through the Accreditation Board for Engineering and Technology (ABET) and for licensing

through the state boards of professional engineers, which are represented by the National Council of Examiners for Engineering and Surveying. In addition, the various specializations in engineering have their own organized societies, such as the American Society of Civil Engineers, the American Society of Mechanical Engineers, and the Institute of Electrical and Electronics Engineers.

However, the engineering fields distinguish between a professional engineer and what is sometimes called a graduate engineer: the professional engineer has to be licensed and must uphold professional standards or risk losing his or her license, whereas the graduate engineer does not. Graduate engineers have earned a degree from an accredited program and do work that draws on their engineering knowledge, but they have no state engineering license.¹¹ In addition to graduate engineers, employees in companies with “engineer” in their job title need not have engineering training that would qualify them for obtaining a license; this is a result of an industrial exemption in the engineering licensure, which allows the use of the term “engineer” but never “professional engineer” in such cases.¹²

Despite the distinction between professional engineers and graduate engineers, both groups are included in the specialized professional engineering societies. Many of these societies have codes of ethics for their members which include a responsibility to “hold paramount the safety, health and welfare of the public in the performance of their professional duties.”¹³ What is known as the paramourcy clause was added in the 1970s to engineering ethics codes and demonstrates how these codes and standards are constantly being renegotiated among the profession and with society. In return for upholding and respecting this social responsibility and the rest of the code of ethics, engineers are granted the privilege of autonomy and authority in engineering matters. This benefit is granted to engineers regardless of their membership in a professional society. So even graduate engineers without membership in a professional society get the benefit of calling themselves engineers and the requisite standing and authority that that title holds in society.

Michael Davis argues that this benefit morally obligates all those

¹¹ National Society of Professional Engineers, “What Is a PE?”, available at <http://www.nspe.org/Licensure/WhatisaPE/index.html>; “Regulation and Licensure in Engineering,” Wikipedia, available at http://en.wikipedia.org/wiki/Professional_Engineer; Washington University in St. Louis, “Professional vs. Non-Professional Degrees,” available at <http://ese.wustl.edu/undergraduateprograms/Pages/ProfessionalvsNon-ProfessionalDegrees.aspx>.

¹² Online Ethics Center, National Academy of Engineering, “Signing Off on Engineering Documents,” available at <http://www.onlineethics.org/cms/4606.aspx>.

¹³ Accreditation Board of Engineering and Technology, “Fundamental Canon 1,” in *Code of Engineering Ethics*, 1977. (Adopted by most U.S. engineering societies.)

who call themselves engineers to follow the standards and codes that help make these benefits possible. One of the most significant benefits is the backing on which to draw when standing up to a management that is placing other priorities, such as profits or expediency, above safety and reliability.

This support that professional engineering societies provide can help to protect engineers in the event they must resort to not approving a project or to whistleblowing. Such support and its limits were demonstrated in a case involving three electrical engineers working on the San Francisco Bay Area Rapid Transit (BART) system in 1971. The engineers discovered an engineering flaw in the design of the project that would have resulted in the doors of the train opening before its arriving in the station. The engineers reported their findings to a member of the BART Board of Directors and their supervisor, but no action was taken to remedy the problem. The board subsequently fired the engineers, whose findings had been reported in the local news media. The case resulted in a lawsuit in which the Institute of Electrical and Electronics Engineers (IEEE) filed a friend-of-the-court brief on the engineers' behalf. The IEEE argued that BART had violated the employment contract with the engineers by firing them for upholding their professional code of ethics. Ultimately the case was settled out of court.

D.2.2 Science

Unlike physicians and engineers, scientists did not professionalize in the United States according to the terms described above. Instead, scientists have remained an independent group of scholars who share knowledge and academic pursuits but do not rely on professional credentials, licenses, or certification to define those who are part of the profession. In addition, scientists as scientists may not serve individual clients per se; many teach, train, and seek funding for their intellectual pursuits. The early national science organizations in the United States, such as the American Association for the Advancement of Science, were devoted from the beginning to promoting scientific research, not to regulating the profession.¹⁴

Yet, despite the lack of formal professionalization in science, the field does share the societal grant of authority and autonomy that the medical and engineering professions have. Scientists are considered experts with the authority to determine the scientific value of research proposals and results. This autonomy and authority were granted to scientists during

¹⁴ Paul Lucier, "The Professional and the Scientist in Nineteenth-Century America," *Isis* 100(4):711, 2009.

the World War II era and thereafter, as the system of federal funding of science was negotiated and established.¹⁵ A social contract indicated that scientists would receive funds from the federal government to perform basic research that might eventually benefit society. Scientists were given the authority to decide which projects to fund and which researchers were qualified and in exchange provided assurances to society that the research would be beneficial.

Ideas of social responsibility in science developed over the postwar period and through the 1970s and 1980s and continue to evolve today. Notions of social responsibility evolved out of scientists' concern over the implications of their research and their desire to maintain the trust of the public and the provision of financial support for scientific research.

Different fields of science developed ideas of social responsibility through different pathways and at different times. These differences and similarities provide valuable lessons on how society and the sciences interpret their relationship in response to the implications of the research they do.

For example, physicists were one of the first groups of scientists to express the view that scientists are to be responsible for the social implications of their research. Their social conscience came to public attention around the time that research was conducted on the atomic bomb during World War II.

During the 1960s and 1970s biological scientists started to discuss their social responsibility as research in genetics, organ transplantation, and cellular biology began to provide an increasing capability for controlling the human body through research on manipulation of DNA and nuclear transplantation (which came to be known as cloning). An example is the previously mentioned 1975 Asilomar conference.¹⁶ Similar expressions of social responsibility also appeared in other fields. For example, the American Anthropological Association developed during the 1970s a statement of principle recognizing the special responsibilities of anthropology as a field of study.¹⁷

¹⁵ Daniel J. Kevles, *The Physicists: The History of a Scientific Community in Modern America*, Harvard University Press, Cambridge, 1995; Daniel J. Kevles, "The National Science Foundation and the Debate over Postwar Research Policy, 1942-1945: A Political Interpretation of Science—The Endless Frontier," *Isis* 68(1; March):5-26, 1977; Steven Shapin, *The Scientific Life: A Moral History of a Late Modern Vocation*, University of Chicago Press, 2008.

¹⁶ Charles Weiner, "Drawing the Line in Genetic Engineering: Self-Regulation and Public Participation," *Perspectives in Biology and Medicine* 44(2):208-220, 2001.

¹⁷ The American Chemical Society, American Institute of Chemists, American Society for Biochemistry and Molecular Biology, Society for Neuroscience, Ecological Society of America, and International Society of Ethnobiology, "Codes of Ethics Collection," Center for the Study of Ethics in the Professions, Illinois Institute of Technology, available at <http://ethics.iit.edu/ecodes/ethics-area/12>.

In large part because scientists did not establish themselves as one profession in the traditional sense and because they did not have clients, the various fields of science did not develop codes of ethics as they organized. The lack of explicit attention to ethical concerns became an issue in the late 1970s and 1980s when a number of scandals over the behavior of scientists brought the lack of ethical standards to the attention of the public and Congress. In response, scientists and policy makers developed expectations and regulations for proper behavior, concerns about which focused on falsification, fabrication, and plagiarism of data and research results starting in the 19th century.¹⁸ Physicians and biomedical researchers earlier in the 1960s and 1970s were also regulated when a growing number of scandals over the use of human subjects were made public and legislators concluded that the medical profession's codes were insufficient to prevent abuses.

Going beyond the regulations, professional scientific bodies adopted the standards expressed in the regulations and outlined other standards for proper behavior. Examples of such standards include those discussed in the report *Responsible Science*,¹⁹ plus the development by numerous scientific societies of codes of ethics. Today, many scientific professional societies have included in their code of ethics stipulations about following federal guidelines. It is important to note, however, that these guidelines are often enforced by being attached to federal research funding laws rather than through professional membership.²⁰

D.2.3 Summary Observation on Codes of Social Responsibility

The distinction between scientists and both engineers and physicians is that scientists' codes of ethics and social responsibility developed out of a need to renew and keep public trust as well as to maintain the social contract, whereas those of engineers and physicians grew along with the desire to maintain professionalization. Today many scientific societies

¹⁸ Paul Lucier, "The Professional and the Scientist in Nineteenth-Century America," *Isis* 100(4):719, 2009.

¹⁹ National Academy of Sciences, National Academy of Engineering, and Institute of Medicine, *Responsible Science*, Volumes 1 and 2, National Academy Press, Washington, D.C., 1992-1993.

²⁰ For example, the Federal Policy for the Protection of Human Subjects or the Common Rule, was published in 1991 and codified in separate regulations by 15 federal departments and agencies. The Common Rule requires that as a condition of receiving certain federal research funding, researchers and institutions must establish institutional review boards and follow the ethical principles for research involving human subjects research first laid out in the Belmont report in order to receive research funding. See <http://www.hhs.gov/ohrp/humansubjects/commonrule/>. The Belmont report can be found at <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>.

have codes of ethics, and some include components that refer to social responsibility in science as well as standards of proper behavior and ethical guidelines for research with humans and animals.²¹

To the extent that scientists and engineers involved in research with potential ethical, legal, and societal implications work in private industry or are funded by grants or contracts, it is possible to tie obligations for ethical behavior or social responsibility directly to the conditions of employment or the funding agreements. These mechanisms give codes of ethics significant potential for enforcement not generally attributed to codes.

D.3 RESEARCH ON ELSI

D.3.1 Federally Supported ELSI Research

National Human Genome Research Institute

For a number of years, the National Human Genome Research Institute (NHGRI) has supported a research program in the ethical, legal, and social implications of genetic and genomic research for individuals, families, and communities.²² The individual research program solicits research projects that anticipate, analyze, and address the ethical, legal, and societal implications of the discovery of new genetic technologies and the availability and use of genetic information resulting from human genetics and genomic research.

In FY 2012, the NHGRI issued a request for applications that explicitly called for scientific proposals with an ELSI research component. That is, qualifying proposals were required to include both a biological science component and an ELSI research component, and work associated with these two components was required to be integrated. In addition, project teams had to have genuine expertise in and experience with dealing with ethical, legal, and societal issues in a genome research context. Successful proposals had to be at least moderately strong in both the science and

²¹ The American Chemical Society, American Institute of Chemists, American Society for Biochemistry and Molecular Biology, Society for Neuroscience, Ecological Society of America, and International Society of Ethnobiology, "Codes of Ethics Collection," Center for the Study of Ethics in the Professions, Illinois Institute of Technology, available at <http://ethics.iit.edu/ecodes/ethics-area/12>; Society for Neuroscience, "SfN Ethics Policy," available at http://www.sfn.org/index.aspx?pagename=guidelinesPolicies_PolicyonEthics; Ecological Society of America, "Code of Ethics," available at <http://www.esa.org/aboutesa/codeethics.php>.

²² National Human Genome Research Institute, "ELSI Research Program," 2012, available at <http://www.genome.gov/10001618#al-1>.

ELSI dimensions; proposals that were strong on the science and poor on ELSI research were not successful. The ELSI component in most cases was or is anticipated to be approximately 20 percent of the total award.

The solicitation in question addressed the utility of genomic information in clinical settings. The science component involved developing methodologies for selecting patients who might benefit from the use of genomic information and techniques for interpreting genomic information in ways that were useful to both clinician and patient. The ELSI component was to address matters such as obtaining informed consent for sequencing in the clinical context, how people understand and use the information, and the implications for the patient of returning information (especially incidental findings) (e.g., Did patients become highly anxious because they learned about their specific genomic conditions?) and for clinicians (e.g., How did clinical workflow have to be modified to accommodate the use of such information?).

Since its inception at the beginning of the Human Genome Project, the NHGRI's ELSI Research program has supported freestanding research on ELSI concerns, primarily through several standing program announcements. However, most of the studies supported under these program announcements were either retrospective (where ELSI insights could not directly influence the scientific research under study) or speculative (where ELSI insights might be entirely disconnected from the active concerns of science researchers). The solicitation described above was developed so that knowledge about ethical, legal, and societal issues could have an impact on how the proposed scientific research was conducted.

The community reaction to these proposal solicitations has been largely positive, according to a presentation to the committee by Jean McEwen, director of the NHGRI ELSI Research program. In her view, the reason is that many researchers realize that ethical, legal, and societal issues will become much more prominent in the future if and when genomically personalized medicine becomes a reality for many patients. On the other hand, a number of otherwise eligible teams (that is, teams that had strong scientific proposals) experienced some difficulty in identifying suitable ELSI experts. This was true even though the NHGRI has been supporting ELSI research in this domain for some 20 years.

National Science Foundation

Since the mid-1970s, the National Science Foundation has supported a research program focused on "improving knowledge of ethical and value

dimensions in science, engineering, and technology.”²³ Currently, the NSF Science, Technology, and Society (STS) program considers research proposals focusing on ethics issues. The 2012 STS program announcement reads as follows:

STS considers proposals for scientific research into the interface between science (including engineering) or technology, and society. STS researchers use diverse methods including social science, historical, and philosophical methods. Successful proposals will be transferrable (i.e., generate results that provide insights for other scientific contexts that are suitably similar). They will produce outcomes that address pertinent problems and issues at the interface of science, technology and society, such as those having to do with practices and assumptions, ethics, values, governance, and policy.²⁴

In the first decade of the 21st century, NSF began a second program with a focus on ethics education for graduate students in science and engineering. Housed in the same division with the STS program, it involves all of the NSF directorates. The 2011 program solicitation stated:

The Ethics Education in Science and Engineering (ESEE) program funds research and educational projects that improve ethics education in all fields of science and engineering that NSF supports, with priority consideration given to interdisciplinary, inter-institutional, and international contexts. Although the primary focus is on improving ethics education for graduate students in NSF-funded fields, the proposed programs may benefit advanced undergraduates as well.²⁵

Each of these NSF programs has received relatively few proposals focused on ethical issues in military research, development, or use of technologies. Thus, NSF has made relatively few awards in this domain.

D.3.2 Centers of ELSI Research

A number of centers for research on the ethical, legal, and societal implications of biomedical and behavioral research have been established, some with government support. For example, the NHGRI, the Department of Energy, and the National Institute of Child Health and Human

²³ National Science Foundation, *Societal Dimensions of Engineering, Science and Technology: Ethics and Values Studies Research on Science and Technology*, Program Announcement, NSF 99-82, 1999, available at <http://www.nsf.gov/pubs/1999/nsf9982/nsf9982.htm>.

²⁴ NSF, *Science, Technology, and Society (STS)*, Program Solicitation, NSF 12-509, 2012, available at <http://www.nsf.gov/pubs/2012/nsf12509/nsf12509.htm>.

²⁵ NSF, *Ethics Education in Science and Engineering (ESEE)*, Program Solicitation, NSF 11-514, 2011, available at <http://www.nsf.gov/pubs/2011/nsf11514/nsf11514.htm#toc>.

Development have collaborated to create interdisciplinary centers of excellence in ELSI research. These centers bring together investigators from multiple disciplines to work on ethical, legal, and societal issues related to advances in genetics and genomics. The centers also nurture the growth of the next generation of ELSI researchers working on genome research.

In a similar vein, the National Nanotechnology Initiative (NNI) mentioned in Chapter 1 seeks to “identify and manage the ethical, legal, and societal implications (ELSI) of research leading to nanotechnology-enabled products and processes.”²⁶ Activities to do so call for “increasing the capacity of Federal agencies to identify and address ELSI issues specific to nanotechnology by fostering the development of a community of expertise on ELSI issues related to nanotechnology,” “building collaborations among the relevant communities . . . to enable prompt consideration of the potential risks and benefits of research breakthroughs and to provide perspectives on new research directions,” and “developing information resources for ethical and legal issues related to intellectual property and ethical implications of nanotechnology-based patents and trade secrets.” To pursue these activities, the NNI has established two independent centers of research on societal implications of nanotechnology research, one at Arizona State University²⁷ and the other at the University of California, Santa Barbara.²⁸

D.4 OVERSIGHT BODIES

D.4.1 Institutional Review Boards

Institutional review boards (IRBs) are a mechanism intended to address ELSI concerns directly related to the safety of human subjects that arise in the conduct of research (usually of a biomedical, social, or behavioral nature). Federal law establishes IRBs at all institutions receiving direct or indirect support from the Department of Health and Human Services (DHHS) and numerous others, and requires that all federally funded research involving human subjects must be approved by the IRB before the research can begin. (Separately, many institutions have biosafety committees, radiation safety committees, and so on.) IRBs must review and renew research approvals annually; they have broad authority

²⁶ See <http://www.nano.gov/goalfourobjectives>.

²⁷ Arizona State University, “Center for Nanotechnology in Society,” available at <http://cns.asu.edu/>.

²⁸ Center for Nanotechnology in Society, “Nano in Society Conference Features CNS-UCSB Researchers,” 2009, available at <http://www.cns.ucsb.edu/news/nano-society-conference-features-cns-ucsb-researchers>.

to review, require revisions in, or halt research that poses safety risks to human subjects, participants, researchers, and the general public, especially where participants are vulnerable populations such as children, the disabled, and so on.

The IRB system is in its most basic sense a review process that relies on the expertise of researchers and community members to protect the rights of subjects and to weigh the risks and benefits to research subjects. This is often achieved by the IRB members imagining the research through the eyes of a subject and by ensuring that the subject's perspective is considered. At the end of the review, the IRB has the flexibility to suggest or require revisions in a research protocol, which they do more often than disapproving studies outright. Suggesting revisions to a protocol allows the IRB to serve as a collaborator in finding an ethical way for the research to proceed.²⁹

IRBs are usually local bodies whose members are from the same institution where the research under review is to be performed. The historical reasoning for this setup was to create a localized responsibility and to allow some flexibility in response to the unique environments in which the research was being conducted. This structure means that researchers serving on an IRB are often reviewing the work of their colleagues and that members of the IRB are familiar with being on the other side of the situation. This shared group review process means that when an experiment is approved, the researchers and the IRB members share responsibility for conducting research in an ethical manner.³⁰

IRBs have been criticized on several grounds. For example, because IRBs are a localized and flexible review process, different IRBs examining multisite clinical research may come to different conclusions about the same research, which may lead to confusion and frustration among researchers from different institutions.³¹ Another criticism argues that because of the power of IRBs to control the specifics of research protocols through the rejection or acceptance of the research protocol, IRBs may create an adversarial relationship between researchers and ethicists instead of encouraging communication and collaboration.³²

Others worry about the scope of IRB review. Some criticisms suggest

²⁹ Laura Stark, *Behind Closed Doors: IRBs and the Making of Ethical Research*, University of Chicago Press, 2012, pp. 2-19.

³⁰ Stark, *Behind Closed Doors*, 2012.

³¹ An accreditation process has been proposed as one way to overcome these kinds of difficulties; the Association for the Accreditation of Human Research Programs, Inc., is an example.

³² Inmaculada de Melo-Martín, "Developing a Research Ethics Consultation Service to Foster Responsive and Responsible Clinical Research," *Academic Medicine* 82(9):900-904, 2007.

that the scope of IRB review is too limited (e.g., IRB review does not go beyond a few specific areas of scientific research, such as research involving human subjects).³³ IRBs are specifically prohibited from addressing possible societal harms.³⁴ At the same time, other criticisms suggest that IRBs have too much power to “impos[e] increasing burdens on researchers, creat[e] bureaucratic nightmares, and otherwise hinder . . . the progress of research.”³⁵ As argued in a University of Illinois report, “As IRBs expand their responsibilities, terminology that might have been very clear in its original context is strained or ambiguous when applied to new areas, leading to imprecision and unreasonable regulatory burden as well as inappropriate regulation and restriction.”³⁶

Another set of criticisms suggests that IRBs today lack focus. For example, a 2003 National Research Council report³⁷ argued that IRBs are often “overloaded and underfunded and so may not be able to adequately protect participants from harm in high-risk research, such as clinical trials of experimental drugs”; are excessively focused on “documenting consent to participate in research so as to satisfy the letter of federal requirements [rather than on] helping individuals reach an informed, voluntary decision about participation”; and have a tendency to “delay research or impair the integrity of research designs, without necessarily improving participant protection, because the type of review is not commensurate with risk.” Others argue that IRBs focus too much on protecting their respective institutions from lawsuits and bad press.³⁸

D.4.2 Embryonic Stem Cell Research Oversight Committees

In 2004, the National Academies began a project to develop guidelines for responsible and ethical research involving human embryonic

³³ Mildred K. Cho et al., “Strangers at the Benchside: Research Ethics Consultation,” *American Journal of Bioethics* 8(3):4-13, 2008.

³⁴ Code of Federal Regulations, Title 45, Public Welfare, Part 46, Protection of Human Subjects, 2009.

³⁵ See <http://www.apa.org/monitor/feb06/sd.aspx>.

³⁶ C.K. Gunsalus, Edward M. Bruner, Nicholas C. Burbules, Leon Dash, Matthew Finkin, Joseph P. Goldberg, William T. Greenough, Gregory A. Miller, Michael G. Pratt, Masumi Iriye, and Deb Aronson, *The Illinois White Paper: Improving the System for Protecting Human Subjects—Counteracting IRB “Mission Creep,”* Sage Publications, Thousand Oaks, Calif., 2007, available at http://www.primr.org/uploadedFiles/PRIMR_Site_Home/Resource_Center/Articles/11.%20Illinois%20Whitepaper.pdf.

³⁷ National Research Council, *Protecting Participants and Facilitating Social and Behavioral Sciences Research*, The National Academies Press, Washington, D.C., 2003, available at http://www.nap.edu/catalog.php?record_id=10638.

³⁸ Steven J. Breckler, “The IRB Problem,” *Monitor on Psychology* 37(2):21, 2006, available at <http://www.apa.org/monitor/feb06/sd.aspx>.

stem cells. The final report of that project recommended that institutions involved in such research establish an embryonic stem cell research oversight (ESCRO) committee to oversee “all issues related to derivation and use of hES cell lines and to facilitate education of investigators involved in hES cell research”³⁹ Of particular significance is the fact that ESCRO committees were supposed to approve the scientific merit of research proposals involving hES cell lines.

According to the 2005 report, such committees should include representatives of “the public and persons with expertise in developmental biology, stem cell research, molecular biology, assisted reproduction, and ethical and legal issues in hES cell research” with “suitable scientific, medical, and ethical expertise to conduct its own review.” An ESCRO committee was not intended to be explicitly coupled to the IRB mechanism, and its responsibilities went beyond those related to human subject protections. Moreover, much of the research in question did not require IRB review.

Since the 2005 report’s publication, most institutions performing such research have in fact adopted ESCRO committees with the responsibilities described in that report. In addition, the National Institutes of Health has taken on an expanded role in overseeing hES cell research, specifically with respect to determining the particular hES cell lines that are eligible for federal research funding.

In a 2010 report based in part on a 2009 NRC-IOM workshop held to review the status of the 2005 guidelines and their implementation,⁴⁰ the NRC observed that most participants in that workshop thought that ESCRO committees play “valuable roles and function in such a way that their elimination could leave gaps not filled by other oversight bodies (e.g., Institutional Review Boards, Institutional Animal Care and Use Committees, Institutional Biosafety Committees).” In addition, some stakeholders at the workshop suggested that in the future, controversies and concerns over the uses of stem cells were likely to grow relative to controversies and concerns regarding the derivation of new stem cell lines.

³⁹ National Research Council and Institute of Medicine, *Guidelines for Human Embryonic Stem Cell Research*, The National Academies Press, Washington, D.C., 2005, available at https://download.nap.edu/catalog.php?record_id=11278.

⁴⁰ National Research Council and Institute of Medicine, *Final Report of the National Academies’ Human Embryonic Stem Cell Research Advisory Committee and 2010 Amendments to the National Academies’ Guidelines for Human Embryonic Stem Cell Research*, The National Academies Press, Washington, D.C., 2010, available at http://www.nap.edu/catalog.php?record_id=12923.

D.5 ADVISORY BOARDS

Advisory boards and committees are a time-honored way to focus attention on ethical, legal, and societal issues associated with S&T. For example, the Recombinant DNA Advisory Committee (RAC) informs and advises the NIH on issues related to recombinant DNA research and reviews human gene transfer research. Established by the NIH in the 1970s, the RAC serves two functions, one as a forum for “open, public deliberation on the panoply of scientific, ethical, and legal issues raised by recombinant DNA technology and its basic and clinical research applications” and the other to review and publicly discuss on behalf of the NIH “protocols that raise novel or particularly important scientific, safety or ethical considerations.”⁴¹ It does so in part by advising the government on potentially controversial areas of genetics research as well as by reviewing novel genetics research proposals that raise new and challenging ELSI concerns.

Another example of an advisory board concerned with issues related to science and technology is the National Science Advisory Board for Biosecurity (NSABB), whose mandate is to provide “advice, guidance, and leadership regarding biosecurity oversight of . . . biological research with legitimate scientific purpose that may be misused to pose a biologic threat to public health and/or national security.”⁴² In this context, the ELSI concern in question is that the results of work on certain biological research may also have harmful effects on public health and/or national security.

Some boards and committees (such as the two described above) have an enduring presence regarding ethical, legal, and societal issues in a specific domain. Others issue a report on a particular topic and then move on to other areas. An example of the latter is the Presidential Commission for the Study of Bioethical Issues (PCSBI), an advisory panel of the nation’s leaders in medicine, science, ethics, religion, law, and engineering that advises the President on bioethical issues arising from advances in biomedicine and related areas of science and technology. The PCSBI seeks to “identify and promote policies and practices that ensure scientific research, health care delivery, and technological innovation are conducted in a socially and ethically responsible manner.”⁴³

Still another example is the “community acceptance panels” sometimes convened by the National Institute of Justice (NIJ) to gather input

⁴¹ “About Recombinant DNA Advisory Committee (RAC),” available at http://oba.od.nih.gov/rdna_rac/rac_about.html.

⁴² National Institutes of Health, “About NSABB,” available at http://oba.od.nih.gov/biosecurity/about_nsabb.html.

⁴³ For more information about PCSBI, see “Presidential Commission for the Study of Bioethical Issues,” available at www.bioethics.gov.

regarding new research and development initiatives from relevant communities. For example, in 2007, the NIJ convened such a panel to discuss efforts to develop safer, more effective use-of-force options for law enforcement officers. According to the NIJ, the panel, consisting of practitioners from the medical, research, legal, and ethical communities, discussed “chemical options, the risk factors associated with their use, potential delivery mechanisms, the empirical studies available from the relevant community, and legal and ethical issues associated with these agents.”⁴⁴

Advisory boards and committees can and do shed light on important ethical, legal, and societal issues. But by definition and as is true with certain other mechanisms such as ELSI research or research ethics consultation services, they have no actual decision-making authority, and the decision makers to whom they report are free to adopt, disregard, or ignore any or all of the findings, conclusions, or recommendations of these boards and committees. Further, because they often work closely with these decision makers in the course of their deliberations, the extent to which they are truly free to make independent findings, conclusions, or recommendations is sometimes questioned.

D.6 ADDITIONAL MECHANISMS

D.6.1 Research Ethics Consultation Services

Research ethics consultation services (RECS) have been established in a number of research environments to help raise awareness of issues related to the ethics of human subjects research and to assist investigators in resolving these issues.⁴⁵ Using an “ELSI consultants on call” model, RECS provide real-time advice to scientists about how to recognize and address ELSI concerns in ongoing research and at the same time may lead those involved to discuss broader ethical, legal, and societal issues. Advocates of RECS believe that their approach can better encourage communication and collaboration and create a mutually beneficial relationship between researchers and ethicists, in contrast to other mechanisms that may create more adversarial relationships.

Approaches to providing RECS vary. For example, in some cases, the personnel providing RECS are embedded with the research team and are likely regarded as collaborators in research; in other cases, they meet with

⁴⁴ National Institute of Justice, “Community Acceptance Panel—Riot Control Agents,” conference, April 30, 2007, Washington, D.C., available at <http://www.nij.gov/topics/technology/less-lethal/riot-control-agents.htm>.

⁴⁵ Mildred K. Cho et al., “Strangers at the Benchside: Research Ethics Consultation,” *American Journal of Bioethics* 8(3):4-13, 2008.

the research team as needed but are independent and are likely regarded as service providers. RECS can be provided by either individuals or teams, and RECS of various kinds are in use at a number of universities.

Although RECS can and do provide ELSI-related input that might not otherwise be available, they also have certain disadvantages.⁴⁶ For example, training for RECS consultants has not been standardized in any way, which means that the results of consultations may vary greatly. The consulting services model can create financial conflicts of interest, given that RECS consultants could alter the advice they give in order to continue being paid, although different arrangements can be institutionalized to insulate payment mechanisms from the specific advice given.⁴⁷ Embedded consultants may be co-opted by their proximity to and relationships with the researchers, losing their objectivity, whereas independent consultants may not have sufficient knowledge or a sufficient opportunity to influence the research work being performed. When individuals provide RECS, available expertise is limited to that of a single individual, and few individuals are qualified to consult comprehensively. The use of teams can overcome this problem, but cost and scheduling can be problematic.

D.6.2 Chief Privacy Officers

Privacy is widely regarded as a key ELSI concern associated with technology in many contexts. One approach to protecting the privacy of citizens and customers in the public and private sectors, respectively, is the use of chief privacy officers who have overall responsibility for such protection within a government agency or a private organization.

For example, the Department of Homeland Security (DHS) established the position of chief privacy officer (CPO) in 2002 pursuant to the Homeland Security Act of 2002. The CPO, a senior official in the DHS hierarchy, has responsibilities “to ensure privacy and transparency in government are implemented throughout the Department.”⁴⁸ More specifically, the CPO’s responsibilities include assuring that the departmental uses of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information; assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in

⁴⁶ Roberta M. Berry, Jason Borenstein, and Robert J. Butera, “Contentious Problems in Bioscience and Biotechnology: A Pilot Study of an Approach to Ethics Education,” *Science and Engineering Ethics* 19(2; June):653-68, 2013; Cho et al., “Strangers at the Benchside,” 2008.

⁴⁷ Cho et al., “Strangers at the Benchside,” 2008.

⁴⁸ U.S. Department of Homeland Security, “Authorities and Responsibilities of the Chief Privacy Officer,” available at <http://www.dhs.gov/chief-privacy-officers-authorities-and-responsibilities>.

the Privacy Act of 1974; evaluating legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the federal government; and conducting a privacy impact assessment of proposed rules of the DHS on the privacy of personal information, including the type of personal information collected and the number of people affected.

Within DHS, the CPO is not expected to take an adversarial role with respect to departmental programs. Rather, the CPO's role is a cooperative one—working with various departmental programs that may have an impact on citizen privacy to find ways of meeting program objectives without harming privacy.

Many government departments have CPOs. But a CPO is also likely to have other responsibilities, such as oversight and/or implementation of policy regarding the Freedom of Information Act. Perhaps more importantly, CPOs may be seen as serving primarily a public relations role rather than actually creating and enforcing policies that protect privacy.⁴⁹

D.6.3 Environmental Assessments and Environmental Impact Statements

Under the National Environmental Policy Act (NEPA) of 1969,⁵⁰ many federal projects that potentially affect the environment require an environmental assessment (EA) that provides sufficient evidence and analysis for determining whether to prepare an environmental impact statement (EIS) or a finding of no significant impact for any given project. An environmental assessment is typically a short document, at least by comparison with an environmental impact statement. If an EIS is required, an analysis is prepared that systematically addresses environmental dimensions of the project in question. An EIS must articulate the beneficial and harmful environmental impacts of a proposed action as well as alternative courses of action.

Environmental impact statements have been criticized by those who believe that they are too lenient and others who believe they are too onerous. Those who believe that EISs are too lenient argue that they are not impartial analyses but rather analyses undertaken by proponents of a project, and thus those proponents may well place their own self-interests ahead of the public interest. Much of the interested public believes, mis-

⁴⁹ Tischelle George, "Say Hello to Your Friend, the Chief Privacy Officer," *Information Week.com*, May 14, 2001, available at http://www.informationweek.com/837/ethics_cpo.htm.

⁵⁰ Environmental Protection Agency, "Environmental Assessments & Environmental Impact Statements," available at <http://www.epa.gov/reg3esd1/nepa/eis.htm>.

takenly, that EISs can mandate cessation of a project, whereas the EIS is instead a tool to provide decision makers with the information they need to make a fully informed decision. Those who believe that EISs are too onerous argue that EISs can introduce unnecessary and often significant delay into project timelines because the content of EISs can be challenged in court. Further, they argue, the significance of the environmental issues EISs address all too often pales against the economic and/or national significance of the project in question.

Sometimes, those responsible for environmental assessment and decision making also seek to involve the public in providing input to the decision-making process. As stated in a 2008 NRC report,⁵¹ many analysts have argued that broader and more direct participation of both the public and interested or affected groups in the official environmental policy processes will increase the legitimacy and the substantive quality of policy decisions. Melnick argued in 1983 that the National Environmental Policy Act was an important reason for the increasing participation of environmental and other nontraditional groups in administrative decision making.⁵²

Others have argued that public participation is not an unalloyed good, raising issues such as “the accountability and representativeness of self-appointed public participants, the inability of nonexpert communities to understand and process complex scientific relationships, the unlikelihood of reaching a meaningful consensus among conflicting interests, the effects of misdirected pressure to achieve consensus at the expense of achieving other important societal goals, and manipulation of outcomes either by those who frame the questions to be addressed or by those who get a ‘seat at the table.’”⁵³

D.6.4 Drug Evaluation and Approval

The Food and Drug Administration (FDA) has long faced ELSI-related decisions having certain properties similar to those faced by military

⁵¹ National Research Council, *Public Participation in Environmental Assessment and Decision Making*, The National Academies Press, Washington, D.C., 2008, available at http://www.nap.edu/openbook.php?record_id=12434&page=10.

⁵² Thomas Sander, “Environmental Impact Statements and Their Lessons for Social Capital Analysis,” conference, Saguaro III, Indianapolis, Ind., December 7-9, 1997, available at <http://www.hks.harvard.edu/saguaro/pdfs/sandereisandsklessons.pdf>. This paper cites R. Shep Melnick, *Regulation and the Courts: The Case of the Clean Air Act*, Brookings Institution, Washington, D.C., 1983, and James P. Lester, *Environmental Politics and Policy: Theories and Evidence*, Duke University Press, Durham, N.C., 1995.

⁵³ National Research Council, *Public Participation in Environmental Assessment and Decision Making*, 2008.

R&D: innovative products offering unique benefits and risks, proprietary information that must be protected, technical information whose evaluation requires scientific expertise, uncertainty that may be reduced by research conducted before or after product use begins, and time pressure that must be respected.

The FDA has developed procedures for addressing ethical, legal, and societal issues in drug development. These procedures are intended to have the following properties:

- *Expert driven.* Evidence is evaluated by scientists, looking at issues identified by officials charged with representing the public interest.
- *Confidential.* Experts have access to all evidence, under conditions that protect proprietary interests.
- *Advisory.* Experts' assessments inform but do not bind policy makers, who must balance conflicting interests when those arise.
- *Predictable.* A growing legacy of decisions expressed in common terms provides developers with guidance about the eventual acceptability of products.
- *Constructive.* Evaluators communicate with developers early enough to incorporate ethical and social concerns in their designs and data collection.
- *Timely.* Evaluations face tight timelines (accelerated for products of great public interest), with documentation proceeding concurrently with development.
- *Efficient.* Evaluations add relatively little to overall development dollar costs, benefiting from economies of scope as issues (e.g., equity, special populations) recur in different contexts. The major costs are arguably in the time required for data collection.

The developers of individual products are not always happy with the decisions that these evaluations produce. However, the pharmaceutical industry supports the process as one that protects the industry by providing equitable standards for all products, while reducing the risk from undisciplined (or unscrupulous) developers.

Critics of the FDA process have pointed to what they regard as excessive delays in drug approval, capture of the process by pharmaceutical companies at the expense of the public interest, imposition of excessive demands for data on new drugs and devices, and improper censorship of medical claims of efficacy (e.g., those regarding supplements), among other things.