Blue Horizons IV

Deterrence in the Age of Surprise

John P. Geis II, PhD, Colonel, USAF, Retired
Grant T. Hammond, PhD
Harry A. Foster
Theodore C. Hailes, Colonel, USAF, Retired

January 2014

70

Occasional Paper No. 70
Center for Strategy and Technology
Air War College

Air University
Maxwell Air Force Base

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE
JAN 2014

2. REPORT TYPE

3. DATES COVERED
00-00-2014 to 00-00-2014

4. TITLE AND SUBTITLE
Deterrence in the Age of Surprise

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air War College,Center for Strategy and Technology,325 Chennault Circle,Maxwell AFB,AL,36112

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study examines the implications of exponential technological change on the panoply of threats the US Air Force may have to face in the future and how the Air Force should posture itself to best deter those threats. Specifically, this study ? examines the changes in the array of threats for which be needed in the future, due to the proliferation of disruptive technologies ? explores the relevance of deterrence theory to both existing and new threats, some of which may surpass nuclear weapons in the risk they pose to both the United States and humankind; and ? recommends new ways of applying deterrence theory in order to reduce the risk that new disruptive technologies will be used against the United States or its interests. Building on previous Blue Horizons studies, this work assumes that science and technology growth will continue and will drive proliferation of advanced and potentially dangerous technologies. It posits that the result of rapid advances in nanotechnology, biotechnology, directed energy, space, computers and communications technologies may prove to be particularly dangerous. These developments span the private sector and many nations.1 Globalization in finance, communications, education, industry, trade governance, and myriad other areas is facilitating the rapid spread of new technologies among nations, groups, and individuals.2 Actors in unstable states and terrorists may use these technologies in malevolent ways to directly threaten US national security and that of friends and allies. This threat will take the Air Force back to its roots, which began in intelligence surveillance, and reconnaissance. Of principal concern by the year 2035 are threats in six separate areas nuclear weapons, attacks in cyberspace, directed energy weapons, space systems, nanotechnology, and biotechnology. Each of these poses the risk of catastrophic attack to the United States, its citizens, and its infrastructure. Deterring threats posed by nations, groups, and individuals will require new thinking regarding the application of deterrence theory. Fundamentally deterrence theory suggests that actors are deterred from attacking a target if they believe that the risk or cost of retribution outweighs the gains to be achieved by carrying out the attack. As such, deterrence theory has always contained two primary branches. One is deterrence by retribution? the cost one can impose on the attacker for either carrying out an attack or making the attempt to do so. The other is deterrence by denial?the ability to deny an adversary the opportunity to attack or having sufficient resiliency that little is to be gained even if the attack is successful. Each of these branches can affect the deterrence calculus. This study examines the interplay among the six technology threat areas and how deterrence theory applies. Historically, deterrence theory as it applies to nuclear weaponry has relied

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**86**	

Blue Horizons IV

Deterrence in the Age of Surprise

by

John P. Geis II, PhD, Colonel, USAF, Retired
Grant T. Hammond, PhD
Harry A. Foster
Theodore C. Hailes, Colonel, USAF, Retired

The Occasional Papers series was established by the Center for Strategy and Technology as a forum for research on topics that reflect long-term strategic thinking about technology and its implications for US national security. Copies of no. 70 in this series are available from the Center for Strategy and Technology, Air War College, 325 Chennault Circle, Maxwell AFB, Alabama 36112, or on the CSAT website at http://csat.au.af.mil/. The fax number is (334) 953-6158; phone (334) 953-6150.

Occasional Paper No. 70
Center for Strategy and Technology

Air University
Maxwell Air Force Base, Alabama 36112

Project Editor
Dr. Ernest Rockwell

Cover Art, Book Design, and Illustrations
L. Susan Fair

Composition and Prepress Production
Nedra O. Looney

Print Preparation and Distribution
Diane Clark

AIR FORCE RESEARCH INSTITUTE

AIR UNIVERSITY PRESS

Director and Publisher
Allen G. Peck

Editor in Chief
Oreste M. Johnson

Managing Editor
Demorah Hayes

Design and Production Manager
Cheryl King

Air University Press
155 N. Twining St., Bldg. 693
Maxwell AFB, AL 36112-6026

http://aupress.au.af.mil
http://afri.au.af.mil/

Library of Congress Cataloging-in-Publication Data

Geis, John P.
Blue horizons IV : deterrence in the age of surprise / by John P. Geis II, PhD, Colonel, USAF, Retired ; Grant T. Hammond, PhD ; Harry A. Foster.
pages cm. – (Occasional paper ; no. 70)
Includes bibliographical references and index.
ISBN 978-1-58566-231-9 (alk. paper)
1. United States. Air Force—Operational readiness. 2. United States. Air Force—Organization. 3. Cyberterrorism—Prevention. 4. Biological warfare—Prevention. 5. Deterrence (Strategy) I. Title. II. Title: Deterrence in the age of surprise.
UG633.G45 2013
358.4'030973—dc23
2013046547

Published by Air University Press in January 2014

Disclaimer

The views expressed in this academic research paper are those of the authors and do not reflect the official policy or position of Air University, the US government, or the Department of Defense. In accordance with Air Force Instruction 51-303, Intellectual Property—*Patents, Patent Related Matters, Trademarks and Copyrights,* it is not copyrighted but is the property of the US government.

Contents

Illustrations

About the Authors

Col John P. Geis II, PhD, USAF, retired, is a professor at the Air Force Research Institute and the former director of the Air Force Center for Strategy and Technology (CSAT) at Maxwell AFB, Alabama. He retired from the service in 2011 after more than 27 years in uniform. Dr. Geis has served as an instructor, weapons systems officer, navigator, and fire control officer on such aircraft as the F-111A, F-111E, T-37, AT-38B, T43, and AC-130H. Operationally, he served as a planner for Operation Eldorado Canyon, flew combat missions over Bosnia-Herzegovina, and commanded the joint and combined special operations task force that replaced the USS *Independence* Carrier Battle Group on the Korean Peninsula. In 1996 Colonel Geis coauthored the Alternate Futures Monograph for the chief of staff–directed *Air Force 2025* study. Shortly thereafter, he served as chief, Strategic Planning, Doctrine, and Force Integration Branch at Headquarters Air Force Special Operations Command, leading all long-range planning, doctrine development, and joint force integration for all Air Force special forces. Dr. Geis is a graduate of the Air War College. He is the author or editor of nearly two dozen Air University Press books and monographs. Dr. Geis has a bachelor of science degree in meteorology from the University of Wisconsin, a master's degree in political science from Auburn University, a master's degree in strategic studies from the Air War College, and both a master of arts and a doctorate in political science from the University of Wisconsin.

Dr. Grant T. Hammond is a deputy director of the USAF Center for Strategy and Technology (CSAT) and a professor of international security at the Air War College. Dr. Hammond received his bachelor of arts from Harvard and a master of arts and doctorate from the School of Advanced International Studies of the Johns Hopkins University. Prior to coming to the Air War College, Dr. Hammond was chairman of the International Studies Department at Rhodes College and executive officer at the Center for International Affairs at Harvard University. He left CSAT and the Air War College in 2007 to be dean and deputy commandant of the NATO Defense College in Rome, Italy, returning to CSAT in late 2010. Dr. Hammond has written three books—*Countertrade Offsets and Barter in International Political Economy* (New York: St. Martin's Press, 1990); *Plowshares into Swords: Arms Races in International Politics, 1840–1991* (Columbia: University of South Carolina Press, 1993); and *The Mind of War: John Boyd and American Security* (Washington, DC: Smithsonian Institution Press, 2001)—and has authored numerous book chapters, articles, and briefings. He has addressed all of the US armed services command and staff colleges and war colleges as well as military and civilian audiences in Belgium, Germany, Italy, Jordan, Morocco, the Netherlands, Romania, Singapore, Sweden, and the United Kingdom.

Harry A. Foster is a deputy director of the Center for Strategy and Technology. Prior to joining CSAT, he served as the chief of strategy for US Air Forces Central Command at Al Udeid AB, Qatar. While a student at the Air War College at Maxwell AFB, Alabama, in 2008, he coauthored the executive summaries for two USAF Blue Horizons studies. A combat-experienced instructor pilot in three aircraft (F-16, B-2, and B-1), he has commanded an operations support squadron and served in the Air Staff's Checkmate Division. He holds graduate degrees from Marine Command and Staff College at Quantico, Virginia, where he was a distinguished graduate; the School of Advanced Air and Space Studies at Maxwell Air Force Base, Alabama; the Harvard Kennedy School at Cambridge, Massachusetts; and the Air War College, where he graduated with highest distinction.

Col Theodore C. Hailes, USAF, retired, is the Force Transformation Chair at Air University and a founding member of the Center for Strategy and Technology. In addition to his work in technology, he is also on the faculty of the Air War College, teaching courses on national security decision making, international security studies, and regional studies field seminars. He retired from the Air Force in 1996, completing a 30-year tour. During that time he flew F-4, 0-2A, F-5, and F-15 aircraft, accumulating over 4,000 hours, of which 500 were in combat. He served in Vietnam as a forward air controller with the 2nd Brigade, 101st Airborne Division, and finished his fighter career as squadron commander of the 22 TFS and then as director of operations of the Northeast Air Defense Sector. He served in two staff tours: the Pentagon from 1979 to 1983, where he worked in international programs and was executive officer for AF/A8, and the Air War College from 1990 to 1996, where he was a department chairman and associate dean of faculty. He returned to the Air War College faculty in a civilian capacity in 1997 and has worked there since. His military educational background includes Squadron Office School (resident, 1972), Air Command and Staff College (seminar, 1981), and Air War College (resident, 1987). His civilian education includes a bachelor of arts in history from Denison University and a master of science in international relations from Troy University. His principal areas of interest in the academic world have been in international relations and the strategic implication of accelerating technological change.

Abstract

This study examines the implications of exponential technological change on the panoply of threats the US Air Force may have to face in the future and how the Air Force should posture itself to best deter those threats. Specifically, this study

- examines the changes in the array of threats for which deterrence will be needed in the future, due to the proliferation of disruptive technologies;
- explores the relevance of deterrence theory to both existing and new threats, some of which may surpass nuclear weapons in the risk they pose to both the United States and humankind; and
- recommends new ways of applying deterrence theory in order to reduce the risk that new disruptive technologies will be used against the United States or its interests.

Building on previous Blue Horizons studies, this work assumes that science and technology growth will continue and will drive proliferation of advanced and potentially dangerous technologies. It posits that the result of rapid advances in nanotechnology, biotechnology, directed energy, space, computers, and communications technologies may prove to be particularly dangerous. These developments span the private sector and many nations.[1]

Globalization in finance, communications, education, industry, trade, governance, and myriad other areas is facilitating the rapid spread of new technologies among nations, groups, and individuals.[2] Actors in unstable states and terrorists may use these technologies in malevolent ways to directly threaten US national security and that of friends and allies. This threat will take the Air Force back to its roots, which began in intelligence, surveillance, and reconnaissance.

Of principal concern by the year 2035 are threats in six separate areas: nuclear weapons, attacks in cyberspace, directed energy weapons, space systems, nanotechnology, and biotechnology. Each of these poses the risk of catastrophic attack to the United States, its citizens, and its infrastructure.

Deterring threats posed by nations, groups, and individuals will require new thinking regarding the application of deterrence theory. Fundamentally, deterrence theory suggests that actors are deterred from attacking a target if they believe that the risk or cost of retribution outweighs the gains to be achieved by carrying out the attack. As such, deterrence theory has always contained two primary branches. One is deterrence by retribution—the cost one can impose on the attacker for either carrying out an attack or making the attempt to do so. The other is deterrence by denial—the ability to deny an adversary the opportunity to attack or having sufficient resiliency that little is to be gained even if the attack is successful. Each of these

branches can affect the deterrence calculus. This study examines the interplay among the six technology threat areas and how deterrence theory applies.

Historically, deterrence theory as it applies to nuclear weaponry has relied almost exclusively on deterrence by retribution. This was necessary, as by treaty each side in the Cold War had more weapons than the other had interceptors to protect from those weapons. The result was an implicit assumption that avoiding a devastating attack was impossible. As a result, deterrence with respect to nuclear weapons has historically relied on a credible threat of a massive retaliatory response, the costs of which would be so great—outweighing the gains to be won—that no rational adversary would ever initiate such an attack. This philosophy was known as mutually assured destruction. However, this historical thinking focuses on only one-half of the deterrence equation, and this is inappropriate in dealing with the newer threats.

This study finds that deterrence by denial has significant leverage in relation to the newly emerging technological threats. Unlike nuclear weapons, it is possible to deny an adversary the capability, opportunity, and the ability to create significant effects using most new technologies if the appropriate steps are taken in advance. In short, it is possible to significantly mitigate the gains to be achieved by attacking and thus change the deterrent calculus in the mind of a prospective adversary. As a result, deterrence by denial now needs to be considered as an integral part of deterrence strategy by the United States and, by extension, its Air Force.

Scope of the Study

Entitled *Deterrence in the Age of Surprise*, this study examines the impact of exponential technological change on potentially catastrophic threats to the United States and its interests and makes recommendations on how the Air Force should best posture itself to aid the United States in deterring these new threats. This study's research team, with more than 650 years of combined airpower and military experience, examined the context of the future strategic environment and researched threats across six technology areas in-depth: nuclear weapons, biotechnology, nanotechnology, directed energy technologies, space systems, and cyberspace systems. They evaluated the nature and extent of the potential threats posed in each of these areas and examined the relevance and application of existing deterrence theory to these new threats. From this analysis of deterrence theory, the study makes policy recommendations that will enhance the likelihood that the United States will be able to deter future attacks across this wide range of technologies from nation-states, groups, and individuals.

This study employs the Delphi study method pioneered by RAND, highlighting the real dangers posed by adversary nations, groups, and individuals possessing advanced technologies. It concludes that groups and individuals will continue to gain access to new capabilities and technologies that once were considered the exclusive domain of nation-states. These technologies will enable these groups to overcome the tyranny of distance and make it easier to discover, act, surprise, and target almost any place on Earth. The study concludes that deterrence of individuals will be more difficult than that of groups or nation-states but that with the most dangerous of new technologies, the greatest likelihood of catastrophic attack is likely to be posed by groups. It reconfirms that more than three-fourths of all technology research and development is now conducted outside the United States, making it increasingly difficult for the Department of Defense to control technology proliferation.

Conclusions

The chapters that follow detail the data, findings, analysis, and conclusions of the research team. Vetted by senior scientists from the national laboratories and the Air Force Research Laboratory, the contents have been peer-reviewed by technical experts around the world. Based on an in-depth analysis of the six major technology areas, the research team reached the following conclusions and makes the following recommendations.

National critical infrastructure is vulnerable to attack in space (communications) via cyberspace and directed energy weapons. This holds the potential to cause permanent damage to parts of the infrastructure, rendering it inoperative for periods ranging from months to years. Additional efforts to guard this infrastructure are required.

While nanotechnology is often thought of as a technology that makes all other things better, it holds the promise and threat of being able to pack large amounts of energy into small spaces. From a battery or space-lift perspective, it offers the ability to solve some of our most important technological challenges. From a weapons perspective, it may enable the miniaturization of bombs that can destroy civilian airliners. This poses risks to the nation's transportation infrastructure, upon which all commerce depends.

Nuclear weapons are unlikely to disappear in the next 20–30 years, and proliferation is likely to continue. In addition to the current nine nuclear states, others, particularly Iran, appear interested in acquiring this technology. Ensuring that weapons remain under the control of the governments that created them will be a key challenge in the future.

The most dangerous technology is nano-enabled biotechnology. While the nexus of these two sciences has already produced extremely effective medicines for certain types of cancer and will likely cure other diseases in time, the same technologies that can cure disease can also be perverted to cause it. With the "Rosetta Stone" for the human genome only a handful of years away, the world is entering an era when it is possible to design a perfectly lethal virus for which no immunity exists. By 2030 this capability could reside in the hands of a master's degree holder in microbiology.

Deterring nation-states, groups, and individuals from using these technologies in ways that would cause catastrophic harm to society is of national importance. While it is more than merely an Air Force problem, the Air Force has a major role to play in providing the nation the necessary capabilities to make successful deterrence more likely.

The Air Force's roots began with observers in balloons overlooking battle lines in World War I, conducting surveillance and reconnaissance of the adversary, and using this information to guide military operations on the ground below. This same fundamental core competency, now called "information superiority," is able to monitor potential adversaries, attribute their activities, and strike them as needed. This is extremely important in successfully deterring an adversary strike. As it did in the two world wars, the Air Force must again pioneer new methods of conducting intelligence, surveillance, and reconnaissance of our adversaries, making certain that they know that no attack will go unnoticed, unattributed, or undetected.

Secondly, the Air Force needs to make itself more resilient in the face of potential adversary attack. In a process this study refers to as immunization, the Air Force needs to assess the risks it is currently taking in relation to these new technology threats regarding its interdependence with other services and the national critical infrastructure for key functions. Once these risks are mapped, research and development will be required to mitigate the risks to make the Air Force and, by extension, the United States less vulnerable to an adversary attack.

The study concludes that if the United States can make it more likely that an adversary will be accurately attributed (ideally before an attack is launched) and can make it less likely that significant damage would occur in such an attack due to greater system resiliency, then adversaries will find launching an attack a risky option with little payoff. In short, they are more likely to be deterred. By increasing the likelihood that future adversaries will find themselves deterred, this will decrease the likelihood that such an attack would ever take place. Greater detail on what these threats are, how they could be implemented, and what steps the Air Force can take to begin the process of readying itself for the future is contained in the pages that follow.

Preface

In 1996 the Air Force initiated a major study under the direction of Gen Ronald Fogleman, the Air Force chief of staff (CSAF). That study, *Air Force 2025*, looked 30 years into the future and made enormous contributions toward directing Air Force research and procurement.

In 2007 Gen T. Michael Mosley, CSAF, directed that a continuous series of future-oriented study efforts be undertaken, using Air University (AU) as the "Air Force's think tank." This study, *Blue Horizons*, was commissioned by the CSAF to provide "a new look at the future." Specifically, the CSAF asked the research team to provide "a common understanding of future strategic and technological trends for Air Force leaders to make better decisions." The chief also sought to "confirm AU as [the Air Force's] in-house think tank" and to improve the relevance of Air Force education to the decision-making processes in Washington, DC.[3]

Under the leadership of the Center for Strategy and Technology, a team of 46 officers from the Air Force and the sister services participated in the study during their one-year master's degree professional military education program. They examined the question "How should the Air Force best posture itself to deter threats by traditional and new weapons of mass destruction or disruption with an eye toward the mid-2030s?"

The authors collectively led the effort and spent the year researching and traveling to identify the range of challenges posed by accelerating exponential technological change and how these changes will modify the types of weapons that may have catastrophic effects in the next 20–30 years. They then examined deterrence theory to determine if this theory would still apply to the new weapons types. In this study, the authors recommend a new way to apply deterrence theory to counter the wide range of threats that could significantly damage the United States and its interests in the years to come.

Notes

[1] T. Michael Moseley and the Air Force Center for Strategy and Technology, *Blue Horizons 2007: Horizons 21 Project Report* (Washington, DC: Headquarters US Air Force, 2008).

[2] Thomas L. Friedman, *The World Is Flat* (New York: Farrar, Straus, and Giroux, 2005).

[3] Gen John D. W. Corley, vice chief of staff, United States Air Force, "Strategic Studies (Blue Horizons) Special Interest Item," memorandum, 17 May 2006.

Chapter 1

Introduction

This study is the fourth in the Blue Horizons series. This series explores topics of interest to the chief of staff and senior leadership of the Air Force and recommends solutions to strategic challenges created by emerging technologies.

In the spring of 2009, the Air Force Center for Strategy and Technology (CSAT) began discussions with the Air Staff regarding the findings of the first two Blue Horizons studies.[1] In these discussions, then–Lt Gen Raymond Johns, the deputy chief of staff for plans and programs, raised concerns that a new examination of how deterrence would operate in the future was necessary. The topic of study for 2010 was derived from these discussions and the memoranda that followed.

This study examines the question "How should the Air Force best posture itself to assist the nation in deterring nation-states, groups, and individuals from attacking the United States in space or cyberspace, or by using nuclear, nanotechnological, biotechnological, or directed energy weapons from now to the year 2035?" This monograph discusses what has become known as "the future deterrence study" inside the Air Force, including the methods of examination used, the findings surrounding these emerging technologies, and the conclusions as to how the Air Force best postures itself to deter the "threats of the responsibly imaginable."[2]

Methodology

The *Blue Horizons IV* study draws upon extensive background research; site visits to the US Air Force and National Laboratories; interviews with scientists, researchers, policy analysts, senior officials in agencies across the "whole of government"; and engineers building the technologies that will help shape the future strategic environment.[3] The team of 35 researchers and five faculty members from two colleges began with a search across science and technology, education and training, governmental policy, organizational culture, national strategies, and military studies literatures.[4] The research team was deliberately selected for its breadth of expertise across all relevant military specialties. The team composition is represented in figure 1.

These researchers visited three of the major national laboratories.[5] In addition the team visited seven of the 10 Air Force Research Laboratory directorates, including Space Vehicles, Directed Energy, Materials Sciences, Human Factors Engineering, Propulsion, Air Vehicles, and Sensors. In each, senior scientists made presentations, and the researchers had time to discuss and interview these scientists regarding current projects, including those that were in the conceptualization stages. This research helped define the range of technologies likely to be available in the field in the 2030–35 time frame for which this study was commissioned.

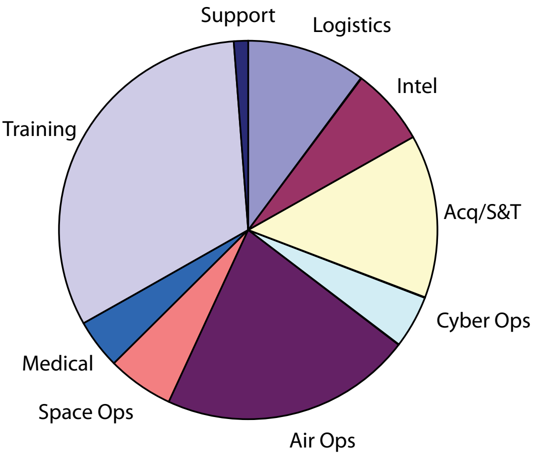
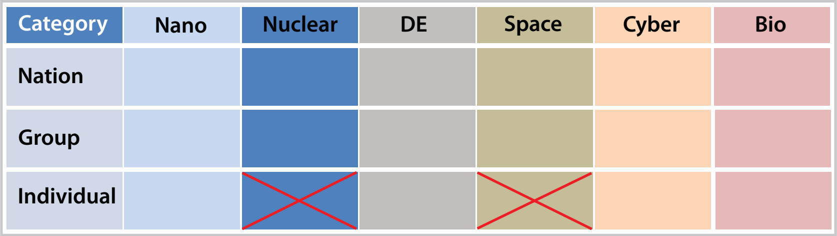


Figure 1. Research team composition by specialty

Once equipped with this understanding of the future threat environment, the research team embarked on research specific to the technological threat across six technology areas and across three types of actors. Specifically, the team examined nanotechnology, nuclear weapons, directed energy technologies, space systems, cyberspace as a domain and as a set of systems, and biotechnology. The team researched these six technological areas as they pertained to potential threats from three actor types: nation-states, groups, and individuals. This created a matrix of 18 squares that required detailed examination (fig. 2). Two of the 18 boxes were eliminated early in the study. Nuclear weapon threats from single individuals were ruled implausible on two grounds. First, it is improbable for a single person to produce such a weapon. Similarly, space attack by a single individual was deemed unlikely in the study time frame, as the team concluded that the infrastructure and materials needed to successfully carry out such an attack would exceed the capacity of a single individual.



Category	Nano	Nuclear	DE	Space	Cyber	Bio
Nation						
Group						
Individual		✗		✗		

Figure 2. Study design—matrix of technologies versus actors

The team, initially divided into subgroups to conduct the specific research above, was later recombined to conduct a more holistic look at the challenges presented across the matrix. The team built a structural model of deterrence and then embarked on a formal Delphi study, followed by an informal version of the Delphi method to evaluate risks and opportunities to deter across the various boxes of the matrix.[6] The formal Delphi study lasted three rounds before convergence was found on the values and the Delphi study was terminated. The informal Delphi discussions took place across five rounds of approximately three hours duration each. The former generated 3,528 data points for quantitative analysis; the latter helped add a qualitative understanding to the meaning.

In the end, the team concluded that the greatest future risks lie not in the area of nuclear weapons, though threats there do remain, but rather in areas of biotechnology and cyberspace. The team also found that while the body of literature on deterrence theory remains valid for future threats, the areas of focus to put the theory into practice will change in the years ahead.

Overview

This paper begins with a discussion of conclusions reached in previous Blue Horizons studies that are applicable to deterring threats emanating from new and emerging technologies. Here, the paper briefly discusses the rapidly changing nature of technology, its proliferation, and the developmental challenges associated with having only a small percentage of global research and development within the nation's military portfolio. It then delves into the nature of the threats across the six technological areas that CSAT was asked to examine. The paper discusses the types of attacks that will be possible over the next 20 years and what the effects could be upon the national critical infrastructure and the population; furthermore, it enables the reader to understand the breadth and depth of the challenges faced.

The paper then introduces a structural model of deterrence. Based on the writings of many of the preeminent deterrence theorists of the past 60 years, this model dissects the concept of deterrence into its component parts and offers a useful analytic tool to determine how best to address each of the threats discussed. Through the lens of Air Force history, the paper recommends two main areas of emphasis for the Air Force as that service seeks to better posture itself to deter threats across these technological realms or domains. It concludes with a specific set of recommendations that were presented to the Air Force chief of staff, while highlighting a few areas where further research or actions are required. While the Air Force can make a major difference, it is not the only agency that has a role in this process, and action by other governmental agencies is also required to create an optimum deterrent posture. Thus, the conclusion of the paper also addresses issues that other departments must attend to in order to aid successful deterrence initiatives.

Background

In the first year of the Blue Horizons program, entitled *Horizons 21*, CSAT examined a broad range of emerging technologies. The researchers found that advancements were happening across the entire range of sciences at an exponential rate. They concluded then that the capabilities available to actors in the international arena will continue to expand at an ever-increasing rate. Driven by motives of profit, social pressures for ever-more-capable goods, as well as scientific curiosity and military necessity, continued exponential technological change is real and inevitable.

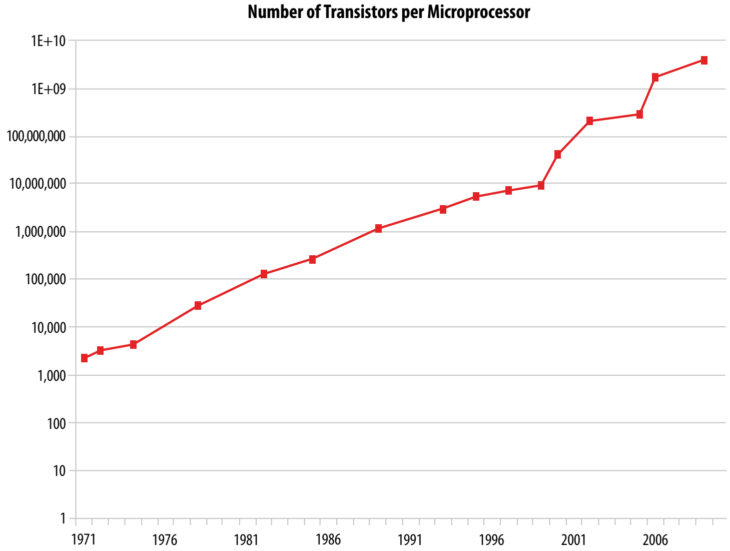


Figure 3. Number of transistors per microprocessor. Graph compiled by authors using data from Intel Corporation. (Intel Corporation, "The Evolution of a Revolution," Intel Developer Forum, n.d., accessed 17 December 2012, http://download.intel.com/pressroom/kits/IntelProcessorHistory.pdf.)

One of the principal early findings, validated in earlier studies, is that many of the key technologies that will require deterrence in the future continue to evolve at an exponential rate. The research team again discovered what is often called the "J Curve." Figure 3 shows the number of transistors per microprocessor on a base 10 logarithmic graph. Each horizontal line represents a 10-fold increase over the line below. On this graph, technological change looks like a straight line. When this or similar technologies are plotted on linear axes, as in figure 4, the curve takes on the appearance of the letter "J," from which this curve gets its name. As with the number of transistors on a microprocessor and the number of Internet hosts, the team revalidated that information, biology, pulsed power, nanotechnology, and other technical sciences are all racing ahead at ever-increasing speeds.

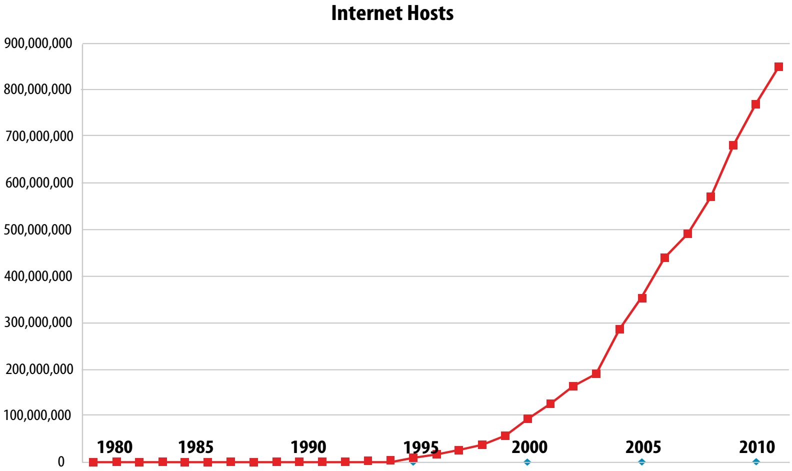


Figure 4. The J-Curve and exponential change. Data from Internet Systems Consortium (Internet Systems Consortium, "Internet Host Count History," n.d., accessed 17 November 2011, http://www.isc.org/solutions/survey/history.)

The rapidly changing nature of technology suggests that the world and the associated technological challenges it faces are changing in unprecedented ways.[7] It is not only the scope of technology change that is unprecedented but also its speed. This century will likely see 1,000 times the technological change of the last century, with each decade containing upwards of 70 times more technological development than occurred in the period from the dawn of time up until the year 2000.[8] This combination of great scope and speed of technological change means that the world of the 2030s will not merely be an extension of today. In many respects it will be fundamentally different. As a result, the greatest threats the world may face likewise represent a significant departure from past thinking.

CSAT's recent research also shows that the United States and its military have an ever-decreasing say in the types of technology being developed. Seventy percent of all research funding happens outside the United States. Further, even among the 30 percent that happens within US borders, 70 percent of those technological developments are privately funded and are solutions or breakthroughs over which the military has no influence or sway.[9] Less than 4 percent of modern technological research is within the purview of the Department of Defense—a radical departure from 50 years ago, when that number was nearly 50 percent.

Feeding this development is the collaboration enabled by the Internet. Specific CSAT research across a multiplicity of disciplines, including computing, alternative energy, nanotechnology, and cyberspace, continues to tell this same story. The scientific breakthroughs and technological applications are both increasingly civilian developed and commercially and globally distributed, and like the number of transistors on a single microprocessor chip (fig. 3), these advancements are continuing at an exponential rate.[10] Moreover, the "half-life" of scientific secrets and their technological applications into militarily critical technologies are shrinking rapidly, and they are available to an ever-larger panoply of actors, both state and nonstate.

The result as we look to the far future is that the technological dominance the United States has historically enjoyed may no longer be possible. By some measures of innovation, such as the number of major scientific articles published in peer-reviewed journals, China is already passing the United States. While the United States continues to enjoy the best laboratory infrastructure in the world, we are declining in our productivity as others are rapidly improving in their ability to innovate. We are in danger of losing the technological race, and our education systems across the United States are setting the nation up to lose even more profoundly in the future.[11]

In the words of Thomas Friedman, these forces are flattening our world. Technologies formerly in the hands of only the wealthy states are now being developed in what were once called "developing countries."[12] This has allowed groups and individuals to acquire advanced technologies that were once the purview only of nation-states. Now computer systems superior to the supercomputers of the 1980s reside in the cell phones of people living in developing countries.[13] Based on a continuation of Moore's law, computers in the next 30 years will become more than 1 billion times more powerful and less expensive than those of today.[14] As a result of this flattening of our world and decreasing cost of technology, warfare is changing.

Historically, wars of high consequence have been relatively rare—sometimes happening only once or twice per century. These were the wars where catastrophic damage could occur or the existence of a state or empire could be threatened. Conflicts with less serious results have been more frequent. In short, warfare has never strayed far from the orange line in figure 5. Today, however, the power once in the hands of states is diffusing to the individual, meaning that attacks and battles of high probability may soon also be events of high consequence. Worse, these conflicts may become more common. This would allow warfare to move into the upper-right quadrant of this strategic planning space—a place it has never been before. This means the future may be different from our past in significant ways.

The number of actors who occupy this new space that may threaten the world is also changing. In 1980 the United Nations (UN) membership stood at 154 nation-states. At the time, these were the primary actors in the world. Today UN membership stands at 192, an increase of nearly 25 percent. In addition, the world has also seen a rise in groups, including nongovernmental organizations, intergovernmental organizations, and terrorist organizations, many of which are able to affect outcomes on at least a regional basis. One such group, al-Qaeda, started the longest war in US history. By 2008 these groups numbered at least 13,425 and may have been as many as 40,000.[15] This represents a three-orders-of-magnitude jump in the number of salient actors.

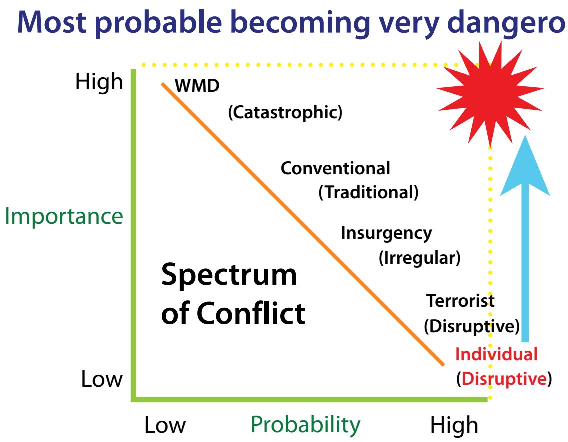


Figure 5. Warfare is changing. (T. Michael Moseley et al., *Blue Horizons 2007: Horizons 21 Study Report* [Maxwell AFB, AL: Air University Center for Strategy and Technology, 2007], 21.)

As technology becomes even less expensive, as automation increases, and as the ability of single individuals to create major effects is enhanced, the number of actors will grow still further. We are in a world where computers can pass the Turing test, meaning that they can not only assist individuals in carrying out tasks but also carry out these tasks by themselves.[16] As machines empower individuals and potentially even become capable of creating significant impacts on society themselves, the number of potential actors undergoes yet another quantum increase. By this measure, the world of 2030 has not hundreds of actors or even tens of thousands. It will have billions. The human race is likely to number between 8 and 9 billion by 2035, and this number itself may pale in comparison to the number of autonomous machines that may be roaming the planet by that time.[17] In short, the number of actors capable of making a major impact on the world stage will increase by another five or six orders of magnitude in the next 30 years—nearly a 100,000-fold increase. Today, we refer to the threats we face as "hybrid." Whatever this future threat is, and there may be no good name for it, it is vastly more complex than anything experienced to date.

The cause of the increase in the number of potential actors and of their increased potential capability is illustrated in economic theory. Matt Ridley argues that the rapid evolution of human capabilities represents a significant research puzzle, as no other species has managed to adapt and conquer its environment so completely or quickly. As recently as 45,000 years ago—a blink of an eye in Darwinian evolutionary time—humans were mostly cave-dwelling, solitary creatures. The discovery and rapid adoption of early tools enabled man to live off the land and provided an incentive for larger communities to form. It also enabled specialization, as the tools enabled farmers to produce enough food for the community, allowing others to specialize in making improved tools or other crafts. Even in this nascent stage of civilization, living together fostered knowledge sharing, causing technology to increase exponentially. Over time, this has led to the increased specialization of employment and the growth of these early communities into the megacities in which many of us live. The critical point made is that the concentration of people escalated the interplay of knowledge that leads to increasing innovation. Ridley argues that the advent of the Internet is exponentially increasing the rate of innovation and now allows information sharing on a planetary scale, which will continue to increase our inventiveness as a species, produce wealth, and result in continued cultural change. In short, the story of the advancement of humanity is the spread of specialization and exchange, with our prosperity being derived from becoming more narrow in what we make and more diverse in what we purchase.[18]

Ridley is an economist, and from an economic perspective this argument is a story of good news. From the standpoint of biology, however, it has a darker side. As innovation increases at an exponential rate, our ability to contain and control new concepts and technology is threatened.[19] It would be an act of hubris to believe that we humans are somehow immune from this outcome.

Notes

1. T. Michael Moseley et al., *Blue Horizons 2007: Horizons 21 Study Report* (Maxwell AFB, AL: Air University Center for Strategy and Technology, 2007); and John P. Geis II et al., *Blue Horizons II: Future Capabilities and Technologies for the Air Force in 2030* (Maxwell AFB, AL: Air University Press, 2009).

2. This phrase is often used by Dennis Bushnell, the chief scientist of NASA's Langley Research Center, to title some of his presentations.

3. The Center for Strategy and Technology (CSAT) has collaborative research relationships with all 10 research directorates of the Air Force Research Laboratory, Sandia National Laboratory, Los Alamos National Laboratory, Lawrence Livermore National Laboratory, and NASA. As needed, CSAT reaches out to scientists and engineers from industry, the academy, and additional laboratories to complete its research. Specific debts of gratitude are owed to the following individuals who contributed to this study and who were willing to be named: John Mearsheimer (University of Chicago); Robert Pape (University of Chicago); Jacek Kugler (Claremont Graduate University); Gen Mike Hayden, USAF, retired; Gen John Shaud, USAF, retired; Dennis Bushnell, NASA Langley Research Center; Peter S. Hamilton, Sandia National Laboratories; Larry A. Schoof, Sandia National Laboratories; Lt Col Joel Almosara, USAF; Col David P. Blanks, USAF; Lt Col Darren Buck, USAF; Lt Col Patrick C. Burke, USAF; Col Christopher Kinnan, USAF; Col Thomas Coglitore, USAF; Lt Col Miguel J. Colón, USAF; Cdr Peter R. Falk, US Navy; Col Michael Finn, USAF; Maj Gen Maury Forsyth, USAF; Lt Col John W. Gloystein, USAF; Col Christopher P. Hauth, USAF; Col William P. Jensen, USAF;

Maj Gen Robert Kane, USAF; Mark J. Krause, National Geospatial-Intelligence Agency; Lt Col Douglas J. Mellars, USAF; Lt Gen Allen Peck, USAF, retired; Col Stella T. Smith, USAF; Col Robert S. Spalding, USAF; Lt Col Michael J. Stephens, USAF; Lt Col Edward L. Vaughan, Air National Guard; and Col Ancel B. Yarbrough, USAF. Many others contributed but were too modest to let us list them here.

4. Neither this work nor any source used to compile this work is classified or draws upon classified material.

5. The majority of researchers visited Sandia National Laboratories in Albuquerque, New Mexico, and Los Alamos National Laboratories in Los Alamos, New Mexico. The faculty advisors and principal authors also visited with scientists and researchers at Lawrence Livermore National Laboratories in Livermore, California.

6. Norman Dalkey and Olaf Helmer, "An Experimental Application of the Delphi Method to the Use of Experts," *Management Science* 9, no. 3 (April 1963): 458–67. Dalkey and Helmer discuss the method in depth, as well as its origins in RAND's Project Delphi. In this case the formal Delphi method was used as described in Dalkey and Helmer. This study then used an informal variant of the Delphi method to see if the results were robust to multiple methodological approaches. For more on this method, see Harold A. Linstone and Murray Turoff, *The Delphi Method: Techniques and Applications* (University Heights: New Jersey Institute of Technology, 2002).

7. John L. Petersen, "Punctuations," *FUTUREdition* 15, no. 8 (30 April 2012), http://www.arlingtoninstitute.org/fe-archive-volume-15-number-8. Petersen's article will be published as the foreword in Finley Eversole, ed., *Infinite Energy Technologies* (Rochester, VT: Inner Traditions, 2012).

8. Ray Kurzweil, *The Singularity Is Near* (New York: Penguin Books, 2005), 10–50.

9. Moseley, *Blue Horizons 2007*. These numbers have not changed much since 2007, as verified in a 2012 study by Battelle Corporation. See Martin Grueber et al., "2012 Global R&D Funding Forecast," *R&D Magazine*, 16 December 2011, http://www.rdmag.com/articles/2011/12/2012-global-r-d-funding-forecast. Grueber and company point out that US research and development spending will top $420 billion but that only $128 billion will be driven by the government—a total of 29 percent. The United States continues to hold about 30 percent of the global research and development share.

10. Among the examples of this research conducted recently are Christopher Coates, *The Air Force in SILICO: Computational Biology in 2025* (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2007); Shane Courville, *Air Force and the Cyberpsace Mission: Defending the Air Force's Computer Network in the Future* (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2007); Mark S. Danigole, *Biofuels: An Alternative to U.S. Petroleum Dependency* (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2007); and Vincent T. Jovene, *Next Generation Nanotechnology Assembly Fabrication Methods: A Technology Forecast* (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2008).

11. Organisation for Economic Co-operation and Development (OECD). The United States ranks last among OECD countries in reading and is 27th in math (between Russia and Portugal) and 22nd in science (between Iceland and the Slovak Republic).

12. See chapter 2, "The Ten Forces That Flattened the World," in Thomas L. Friedman, *The World Is Flat: A Brief History of the 21st Century* (New York: Farrar, Straus and Giroux, 2007), 51–199.

13. Michio Kaku, *The Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100* (New York: Doubleday, 2011), 21.

14. Moore's law posits that computer processor capabilities will double every 18 months. This yields 20 doublings in a 30-year period or an approximate 1.048-million-fold increase.

15. Estimates of the numbers of these groups vary widely. The lowest estimate the authors encountered in their research was 13,425, which is cited by the United Nations.

Mainstream estimates are in the range of a few tens of thousands, with some upper-end estimates around 60,000. For more data, see *The United Nations Today* (New York: United Nations Department of Public Information, 2008). See also Helmut Anheier, Marlies Glasius, and Mary Kaldor, "Introducing Global Civil Society," *Global Civil Society Yearbook 2001* (Oxford, UK: Oxford University Press, 2001), 2–38.

16. Two computers have already successfully passed a version of the Turing test wherein a computer mimics human behavior so closely that in a blind test observers cannot discern which actor in a lineup is the computer. The first such event was in 2008, when Elbot, a chat bot designed by Fred Roberts, successfully convinced two judges out of three after a five-minute interview that it was a human. Elbot won the Loebner Prize that year. Alan M. Turing, "Computing Machinery and Intelligence," in *Parsing the Turing Test: Philosophical and Methodological Issues in the Quest for the Thinking Computer*, ed. Robert Epstein, Gary Roberts, and Grace Beber (Dordrecht, Netherlands: Springer, 2009), 23–66. The other such computer is Watson. See Ray Kurzweil, "The Significance of Watson," *Kurzweil Accelerating Intelligence* (blog), 13 February 2011, http://www.kurzweilai.net/the-significance-of-watson. It is worth noting that Kurzweil believes that the Loebner threshold for passing the Turing test is too low but that genuine human intelligence will be reached by 2029.

17. US Census Bureau, US Department of Commerce, "U.S. & World Population Clocks," accessed 12 May 2012, http://www.census.gov/main/www/popclock.html.

18. Matt Ridley, "Humans: Why They Triumphed," *Wall Street Journal*, 22 May 2010, http://online.wsj.com/article/SB10001424052748703691804575254533386933138.html; and Matt Ridley, *The Rational Optimist: How Prosperity Evolves* (New York: HarperCollins, 2010).

19. A. Hallam and P. B. Wignall, *Mass Extinctions and Their Aftermath* (Oxford, UK: Oxford University Press, 2002). Based on Hallam and Wignall's calculations, the combined extinction loss from the five major extinction events (End-Ordovician [84 percent], Late Devonian [83 percent], End Permian [95 percent], End Triassic [80 percent], and End Cretaceous [76 percent]) would be 99.994 percent. This figure does not include the background extinction rate of those species that died out between these events, which would raise this figure still higher.

Chapter 2

Threats in the Age of Surprise

As a result of this increasing speed of interaction and data sharing, we have entered an "age of surprise." While it is possible to see the broad outlines of the future and to define the strategic planning space, this speed of change is making the specific details harder to see.[1] Whether we call these details "turbulence" or a form of chaos in complex systems, we have entered a period of inevitable surprises. We can discern the outlines of some in advance.[2] The key is to understand some of these potential surprises and know how to deal with the resultant challenges.

Cyberspace

Much of the critical infrastructure in the United States is dependent on cyberspace. To research exactly how vulnerable this infrastructure is, the Department of Energy created a National Critical Infrastructure Test Range as part of the Idaho National Laboratories. In 2007 a test of the robustness of our electrical grids against cyber attacks was first conducted on the lab's 860-square-mile test range.[3] Dubbed "Aurora," the attack simulated a single cyber attacker tapping into a supervisory control and data acquisition (SCADA) system controlling an electrical power generator similar to those used in the power plants across the United States. The result of the attack was a loss of control of systems critical to generator operation, which caused the generator to be destroyed.[4]

It is important to note that large electrical-generation components like the generator in the Aurora test are typically custom manufactured. Utility companies often have spare wire on hand, but spare generators are rare. The usual time to receive a new generator from the time the order is placed is around 18 months, assuming, of course, that the plant that manufactures them has electricity in the first place. In a large cyber attack, this assumption may be invalid.

This demonstration is disturbing on three grounds. First, it is not unique. Several instances of system malfunctions, arguably because of hacking into these types of systems, have already occurred and have caused damage to various infrastructures. Second, the US Air Force is heavily reliant on the national critical infrastructure, and if it were to incur a massive failure, it is highly likely the Air Force would be unable to carry out its principal core functions. Lastly, very little has been or is being done to mitigate this problem.

There have been several attacks on critical infrastructure worldwide, many of which predated the Idaho test by years. Among those known to be intentional attacks on SCADA systems for the purpose of causing damage is an attack on the Maroochy Shire's sewage treatment system in Queensland, Australia, in January 2000. During this attack, more than 264,000 gallons of sewage spilled over a period of several weeks, just after a new control system had been installed. Pumps were opening and closing without being commanded to do so. Only after months of investigation and 46 successful attacks was the source of the problem traced to a disgruntled employee who was trying to gain employment as the troubleshooter of misbehaving control systems.[5] In March 1997, a teenager managed to hack into the Bell Atlantic Computer and shut down the air traffic control system in and around Worcester, Massachusetts.[6] In addition, hacking attacks have disrupted natural gas pipelines in the former Soviet Union (1982) and Russia (2000). The 1982 event resulted in an explosion known as a "logic bomb."[7] There are other events that were also likely deliberate, as recent speculation regarding the Stuxnet and Flame malware programs suggests. It is important to realize that SCADA systems offer a path into the internal logic of the critical infrastructure; in fact, attacking these systems is easy enough that even a single hacker can accomplish it.

The Air Force is dependent on these systems. If such outages are sporadic and/or localized, such inconveniences are easily overcome. If, however, the outage is part of a coordinated attack and if it affects the whole nation, then current planning is insufficient. A disabled national critical infrastructure affects not only electrical generation but also, over time, the systems that enable water transport, heating systems, sewage systems, and the financial and banking industries upon which modern economies depend. Distribution of foodstuffs, gasoline, and fresh water all require electricity at some stage, even if it is merely to distribute and pump the gasoline to power the trucks. Similarly, communications are electricity dependent. Without it, cell towers and landlines cannot operate. While most Air Force bases have means to recall their members even if there are no communications, the study team could find no one who could articulate how the Air Force would conduct a deployment without the ability to communicate from one base to another.

The Air Force also depends on these systems to carry out missions other than deployment. Cyberspace is likely the future domain in which most intelligence, surveillance, and reconnaissance (ISR) will be conducted. The rapid increase in the number of cameras and pictures that are both geographically and chronologically referenced, combined with the current ability to fuse these images seamlessly together, will enable a new method of creating real-time, three-dimensional images of almost any major city on Earth.[8] As most of these pictures are available on the Internet, the ability to "play" these three-dimensional views back in time will enable the tracking of many activities of military significance back to their sources. In addition, cyberspace and the pictures that exist therein enable reconnaissance in ways impossible via either air or space. Office-space layouts, interior building configurations, and the locations of telephone junctions and circuit breaker boxes are all pieces of data that can be found in a picture on the Internet. These are pieces of data that one will never see from a satellite image.[9] As a result, ISR in cyberspace may become the principal means of obtaining intelligence data in the future, making the survival of the national critical infrastructure even more important.

Perhaps most disturbing is the lack of a sense of urgency in addressing the problem. While research protocols require anonymity, CSAT has interviewed senior executives in several utility companies across the southeastern United States regarding the protective measures they are taking to stop potential cyberspace attacks. To a person, we received the same answer—"nothing." When we queried these leaders (chief executive officers and chief operating officers) as to why they were not taking action to protect their systems, the answer was also unanimous. Protective action costs money, and such money would have to come from shareholders' dividends. In short the market incentives that currently exist are a powerful disincentive for leaders of the private companies to do anything to protect against the vulnerabilities that have long been known to exist. As a result, significant threats, not only of disruption but also of long-term destruction, exist and will likely remain for some time in cyberspace.

Biotechnology

The second area where the threat is rapidly evolving is biotechnology. The Human Genome Project was completed in 2003.[10] In this project, completed several years early, all the genes in human DNA were identified. Today, it is possible to get your finger pricked and have your genomic code printed out with all the As, Gs, Cs, and Ts. Such a printout would reach about 20 feet in height, and it would likely be meaningless both to you and to your doctor, but today it is possible.[11] The step being worked on now is the "Rosetta stone" to those 20,000–25,000 genetic sequences—the part that determines how these genes produce the roughly 20,000 proteins that make each one of us a unique human being. This is called the Human Proteome Project, and it is well and truly under way.[12]

Once the project is completed, pharmaceutical companies will be able to use these data to develop cures for many, if not all, genetic diseases. Illnesses like cystic fibrosis, muscular dystrophy, and cancer may all be eradicated. Already today, some cancers, particularly those of the blood like leukemia, are being attacked by nanoengineered medicines based on an understanding of the ribonucleic acid structure of the underlying disease. Medicines like imatinib (Gleevec) and dasatinib (Sprycel) are able to bind with the leukemic blood molecules at a submolecular level and keep the leukemic molecules from reproducing.[13] The result for many patients is a long life with the leukemia in remission. More such cures and treatments will follow in the years ahead.

Unfortunately, this same technology that may bring almost miraculous cures cuts both ways. Once the human genetic code is understood well enough to cure a genetic disease, it will also be understood well enough to engineer an illness for which no immunity can be found within the human genetic code. We are told by the leading scientists in our national laboratory system that by the year 2025, such capabilities will be resident in the hands of a well-trained microbiologist, whom they define as a master's degree holder from a major university. Such an individual, with a lab costing as little as $100,000, would be able to engineer such a pathogen inside a one-car garage or a small basement.

Lest this be thought of as only science fiction, such an event—though unintended and contained—has already occurred with mice. In 2000 Australian scientists were attempting to modify the mouse pox virus to produce interleukin-4 in the hopes of stimulating the production of viral antibodies. This experiment had two unexpected results.[14] First, it failed to result in the production of the antibodies sought. Second, the resultant mouse pox strain had extraordinary lethality. Researchers awoke one morning to find every mouse in the laboratory dead, including mice immunized against the disease before the experiment began. The virus was 100 percent lethal, had overcome the immunity conferred by prior vaccination, and had spread to every mouse in the lab.[15] Although this incident was an accident, deliberate genetic modifications to existing viruses could produce the same result in other species, including our own.

Nanotechnology

The field of nanotechnology offers three key advances as we move toward the future. The first is at the nexus of biotechnology and nanotechnology, largely discussed above. The second is in the creation of high-density energetic materials much more powerful than those developed to date. The third deals with the development of nanomaterials that will have specifically engineered properties, such as the ability to cause rapid corrosion, which could become a new class of weapons against systems and materiel.

The term *nanotechnology* is recent to science. Some reasonably recent versions of Webster's dictionary do not even contain a definition for the word.[16] Further, even within the discipline, there is some controversy over its meaning. Some have come to use nanotechnology to refer to any object or technology that is smaller than a micron (1,000 nanometers) in size. This misuse was partly an outgrowth of science fiction and partly of science still catching up to the concept.[17] When this was added to the marketing aspects of being able to label anything made with a coating or substance that contains small parts as being "nanotechnology," the environment became ripe for misuse of the term.

Here, nanotechnology refers to materials and substances that are constructed using processes to arrange particles of under 100 nanometers in size with submolecular precision, for which the important properties of the materials are governed largely by intermolecular (that is, van der Waals) forces.[18] Technology that merely involves scaling existing micromechanical processes to submicron scale is "nanoscale technology."

As indicated above, the first challenge with nanotechnology is the ability to precisely and deliberately create molecules of any design. As pharmaceutical companies are already demonstrating, once the genetic structure of a particular form of an illness is known, it is possible at the submolecular level to design medicines that can cure these diseases. As also mentioned above, once the human genome is successfully decoded and the Rosetta stone is built, well-trained microbiologists will have the capacity to engineer pathogens for which, even at the genetic level, the human system has no built-in immunity.[19]

The second area of concern for future attacks deals with the production of high-density materials using nanotechnology to precisely arrange molecular structures in a manner which optimizes explosive power. While modern explosives are several times more powerful than trinitrotoluene (TNT), future explosives may be much more powerful still.

One of the principal limitations of modern explosives is the availability of oxygen at the time and place of detonation. This causes the explosive to do two things. First, some explosive molecules may not ignite due to the oxygen-depleted environment and as such will reduce the total energy produced. Second, the explosive molecules that are not able to pair with the necessary oxygen immediately may still detonate but will do so after a short delay while they are waiting for additional oxygen molecules. This extends the duration of an explosion at the cost of reducing the initial blast effect. Using nanotechnology to pair oxygen atoms directly with the explosive atoms that require them would theoretically improve the efficiency of the explosive burn.[20] This same process could be used to enhance the thrust produced by rocket fuels, which are, in essence, controlled explosions themselves.[21]

While it is theoretically possible to achieve explosive yields of up to 1,000 times those of modern explosives, near-term advancements are likely to be much more modest.[22] Though nanotechnology is a rapidly advancing field, the ability to create the assemblers necessary to produce such explosives on a meaningful scale is currently limited, and in the next 10–20 years, most scientists in the field believe an advancement of 5- to 10-fold is likely. Nonetheless, a 10-fold advancement makes future explosives so powerful that the three-ounce bottle of liquid one is allowed to carry on board a civilian jetliner may have to be reduced to 0.3 ounces—only a few drops. Very small and easily concealed explosives could pose significant risks to lives and property, and this miniaturization may result in a more challenging threat in the years ahead.[23]

Militarily, there are two positive aspects to this technology. First, the meticulousness needed to create these explosives would produce a very precise and reliable yield, allowing for potentially greater accuracy and lower collateral damage from newer weapons designs. Second, the increased thrust potential emanating from these materials may significantly solve challenges associated with getting heavy objects into space.

Historically, roughly 90 percent of all rocket mass has been either fuel or the systems that contain the fuel. The amount of thrust that a unit of fuel can produce is called specific impulse (ISP). Increasing the energy content of the fuel 5- to 10-fold would increase the ISP proportionately and greatly reduce the amount of mass of a rocket that would need to be devoted to fuel and its associated system.[24] Though this dynamic has long been understood, the breakthroughs in nanotechnology may soon allow the dynamic to be exploited. While this may make it easier for man or robots to explore the stars or launch satellites, it would, of course, make it easier for other actors to launch objects at long distances, posing yet another potential threat.

The last area where nanotechnology poses a potential threat is in designing molecules or nanoparticles to interact with materiel to cause severe damage to infrastructure or materiel. "White nanoparticles" are designed to specifically interact with their environment and to "pick up" any foreign debris located on the surface to which they are applied. In short they are created as a very powerful agent designed to strip the surface of anything that should not be there. Similar agents could be designed to cause the degradation of materials and play havoc with critical components or infrastructure.[25]

Nuclear Weapons

The study participants do not see nuclear weapons disappearing from the world stage during the time frame being examined. Nuclear weapons will remain a threat. Today, the "nuclear club" is estimated to stand at nine, and for the record, the study participants do include Israel in this number.[26] Iran's nascent nuclear program has been well reported in the press, and North Korea has already successfully accomplished nuclear tests.

Counterproliferation as a mission set would appear to have failed. While the Stuxnet virus may set Iran's program back by a few years, it does not guarantee an end to the program. While the engineering to refine the materials is dangerous and difficult and the safety systems needed to protect workers are complex, the science behind these devices has been published in high school physics textbooks for the past 30 years.[27]

By the 2030s, it would seem likely that the gradual upward trend of states with nuclear weapons will continue. Already, Iran's potential quest for a nuclear weapon has triggered interest in the Persian Gulf region, and this dynamic may well spread elsewhere. As will be discussed further, it seems likely that nation-states can be deterred from using these weapons. However, the more widely proliferated they become, the more opportunities groups and individuals may have to appropriate one. For reasons that will be discussed more fully, this study team considers such a scenario the greater risk of proliferation.

Directed Energy

This study addresses two different forms of directed energy, both of which represent threats to military and civilian personnel. The first is the pulsed type, which includes such phenomena as pulsed high-powered microwaves, electromagnetic pulses, and a set of natural phenomena that mirror the effects of these two weapons types. The second type of directed energy threat is continuous wave in nature. The power output of these weapons, usually referred to as lasers, has reached tactically significant levels in the last few years, and further developments are likely in the near future.

The discovery of the potential anti-electronic utility of pulsed forms of energy came by accident. In 1962, shortly after the Soviet Union had breached a nuclear testing moratorium, the United States tested a 1.4-megaton nuclear device 400 kilometers above Johnston Atoll in an experiment called Starfish Prime.[28] Approximately 1,300 kilometers away, in the Hawaiian Islands, street lights burned out, radio stations were knocked off the air, cars stopped due to burned-out generators and alternators, and some telephone systems were knocked off-line. The relationship between these events was not initially obvious and took some time to verify.[29] It is important to note that not every street light was disabled, that many cars still ran, and that some telephones still worked. Nonetheless, many systems stopped working that night. Only later did the reasons become clear.

A few years later, in 1967, both the United States and the Soviet Union replicated these pulsed-energy effects. It was discovered that nuclear detonations above the ionosphere would charge this region of the upper atmosphere and generate intense electromagnetic fields across the earth's surface. These fields fluctuate quickly and induce electric currents in all metallic objects they encounter. If the electricity generated is above the designed load for the system, the system shorts out and subsequently fails.[30] Fearing the effects such weapons could create, the United States and USSR together drafted the "Outer Space Treaty" (more formally, *The Treaty on Principals Governing the Activities of States in Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*), which bans only weapons of mass destruction from space and does so because of the electromagnetic pulse (EMP) phenomenon.[31]

A very similar phenomenon can be reproduced using a nonnuclear pulsed power generator on the earth's surface. While physicists will be quick to point out that the precise shape of the pulsed waveform is different from that of a nuclear blast, its effects on electronics are nonetheless the same.[32] Inducing an electromagnetic field across wires, computer circuits, or any other conductive material produces electric current within the wires. Like EMP, this current can wreak havoc with computers, power distribution, and electronic control systems—the very systems involved in controlling our national critical infrastructure, financial and banking systems, and computers and communications systems used to command and control military forces worldwide.

The level of damage done to these systems is related to the field strength of the magnetic field induced by the pulsed microwave device and the sensitivity of the equipment.[33] It is important to realize that as computer chip spacing becomes more compact in our quest to produce ever more powerful and faster computers, the amount of energy needed to short out the computer circuits decreases with the square of the chip spacing. Stated more plainly, the ability to destroy or damage computer control systems is increasing exponentially as the computer chips become faster.[34] Just as important, our ability to store and generate pulsed power in the form of microwaves is also increasing exponentially with time. In 2003 it was possible to produce 20 gigawatts of pulsed power output in a 400-pound device. Today several efforts are in the works on terawatt-class devices, some of which are explosively powered, representing a near-100-fold improvement in roughly a decade.[35] In 2002 conventional pulsed microwave devices had relatively short ranges. Today small, portable, reusable weapons have ranges in the hundreds of meters. At the rate these technologies are changing, by the 2030s the ranges of these systems will be in miles or tens of miles, making them tactically and strategically significant.[36]

As the team was studying the troubling effects of pulsed power on computer and electrical systems, we stumbled upon a disturbing finding that changes the way the United States must look at deterrence specifically in this area. There is a natural phenomenon that creates these same electromagnetic fields, at very high levels, that can damage or destroy the nation's computer and electrical infrastructure. Unlike individuals, groups, or nation-states, this phenomenon is not deterrable. In short the day will come when the United States, and indeed the world, will have to deal with this problem on a massive scale, and the astronomical record suggests it happens on average once every 50 years or so.[37]

Solar coronal mass ejections—solar flares—send charged particles into the earth's ionosphere, which in turn can create strong magnetic fields on the earth. One such flare, much smaller than the once-every-50-year event referred to above, occurred on 13 March 1989. Perturbations in the earth's magnetic field caused by the charged solar particles induced electrical currents in power lines and all conductive metals. These currents flowed into generators and transformers at power plants across the globe, affecting some severely. The power failed across much of eastern Canada, and due to continued current fluctuations in the power lines, restoration could not begin for nine hours. The Toronto Stock Exchange had to close.[38] While most pieces of the power grid survived the flare, some did not.[39]

It is important that the flare of 13 March was just barely an X-class flare.[40] Much larger solar flares are in the astronomical record, but they predate the construction of the modern electrical grid. The result is that our electrical and computer systems have never faced an extremely large flare, and as a result, no one has personal experience with what such an event would be like. We do have computer models based on smaller flares that give us an indication of what could happen, and what they tell us is disturbing.

Figure 6 shows the impact of a once-every-50-year solar flare, notionally at a level of 4,800 nanoteslas per minute and centered at about the latitude of the US-Canadian border. This is a flare similar to the one that hit the earth in May 1921. The areas outlined in black would see blackouts with concomitant destruction of the electrical-producing infrastructure. The sizes of the circles (both red and green) indicate the level of current that would be induced along the power lines and other metallic objects. The color merely indicates whether the charge would be positive or negative, but it is important to note that both can cause catastrophic damage. The transformers that would be destroyed would take years to replace as these are custom-manufactured pieces of equipment. The economic impact would be well into the trillions of dollars and result in an economic downturn of depression magnitude.[41]

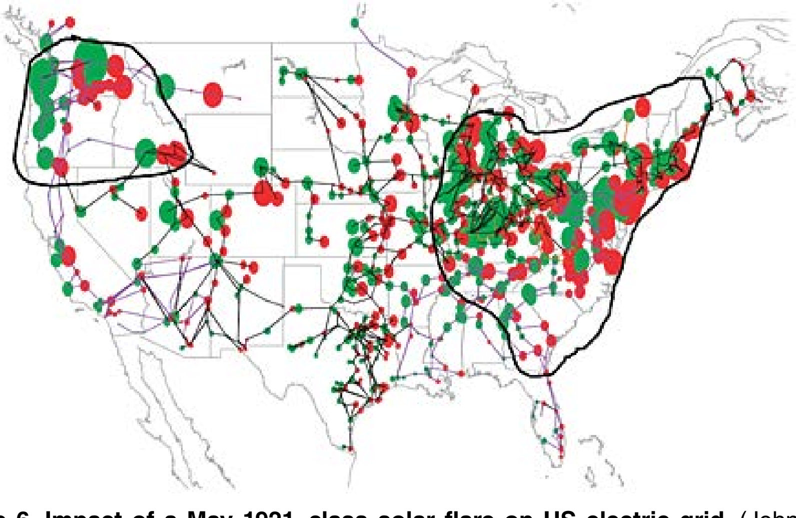


Figure 6. Impact of a May 1921–class solar flare on US electric grid. (John Kappenman, "The Future: Solutions or Vulnerabilities?" [presentation, Space Weather Workshop, National Oceanic and Atmospheric Administration, Boulder, CO, 28 April – 1 May 2008].)

The May 1921 solar flare is not, however, the worst-case scenario. On 1 September 1859, a British scientist had sketched a set of sunspots. As he was drawing them, a solar flare so large that it could be seen with the unaided eye blotted out the spots. Within a minute, the flare was over. The next morning, the aurora borealis and aurora australius were seen well into the tropics. The auroras were so bright that newspapers could be read outside at night as if it were daytime. Telegraph wires went haywire and operated even after the batteries had been disconnected. Electric arcing from these systems electrocuted operators and set telegraph papers on fire.[42] There were reports in the Great Plains of electrical arcing or lightning bolts dancing from cattle fences to the ground as the wires between posts were energized. The models that suggest nearly half the nation would lose electricity in a 1921-like event indicate that should another flare the size of the 1859 event occur, virtually the entire electrical grid would be catastrophically damaged with recovery time estimated at over 10 years.[43]

As we found with cybersecurity issues, very little is being done to address this problem. Protection of our computer and electrical infrastructure against pulsed wave forms, whether man-made or natural, is not occurring. In addition, policy guidance is also lacking. The result is that while the dangers of our current systems are known, the vulnerabilities remain.[44]

The other form of directed energy is continuous wave, the most common being lasers. While lasers have overpromised and underdelivered for decades, this is no longer true. In November 2010, CSAT placed an order for a small, handheld category IV weapons-grade laser for $299. To the researchers' surprise, the order processed on "Black Friday," the Friday after Thanksgiving, resulting in CSAT's receiving the "three-for-one" special deal. We paid less than $100 for each of the three lasers that arrived on our doorstep about six weeks later. Figure 7 depicts the blue variant of this laser, which measures approximately 20 centimeters long and approximately five centimeters in diameter, weighing about 250 grams. It is a potentially lethal device, but its greatest dangers come from its ability to permanently blind a person in less than 0.25 seconds at a range out to approximately 150 meters. It is capable of melting plastic and setting flammable materials ablaze (451° F or 233° c).[45] The laser runs off a single lithium-ion battery, roughly size AA, which enables the laser to operate continuously for 120 minutes on a single charge.

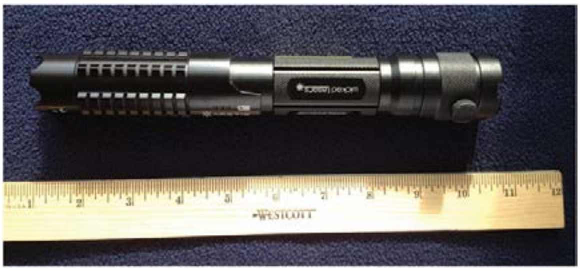


Figure 7. Spyder Arctic III Blue Laser

A company operating in Hong Kong began producing and marketing the laser in the fall of 2010. At the time of production, only the country of Malta had definitive restrictions on the sale or importation of this device.[46] In the United States, importation was legal. Though not directly attributable to this laser, in the first nine months of 2010, the United States had 299 lasing incidents against civilian aircraft. There were 2,700 more in the last three months of that year. Blinding incidents have also increased in other countries, including some attacks on motorists.[47]

Meanwhile, lasers for aircraft and weapons applications have reached tactically significant power levels. Chemical oxygen iodine lasers (COIL) have been designed for applications ranging from missile defense to ground attack. The airborne laser system, recently decommissioned by the US Department of Defense, was a megawatt-class system, roughly 1 million times more powerful than the handheld laser above. Air Force Special Operations Command placed a much smaller COIL device on board a C-130 aircraft and successfully disabled targets on a weapons range, including stopping a Ford F-150 truck.[48]

As with pulsed power devices, laser efficiency and effectiveness are continuing to improve. Small handheld devices powerful enough to blind or kill soon will be in the hands of those who may seek to create fear or terror. Larger lasers, with speed-of-light kill capability, will likewise be obtainable via arms markets well within the next 20–30 years.[49]

Space

The last of the six threat areas explored by the team involves threats to assets in space. Both China and the United States have demonstrated that satellites in low Earth orbit are vulnerable to direct-ascent attacks.[50] Directed energy research is continuing in several countries and will pose a risk to satellite operations in the very near future.[51] Lasers that can dazzle or destroy satellites, likely all the way to geostationary orbit, will probably be fielded by the 2030s. The result is that space assets, both military and civilian, are and will increasingly be vulnerable to attack, either from the ground or from space.

What many may not realize is the important roles that satellites play in the economy and in our everyday lives. Most people intuitively understand that the Global Positioning System (GPS) provides their location and, in combination with a receiver, can help them locate hospitals or gas stations. What is not widely understood is that GPS operates by triangulating one's position through the use of very precise timing of the receipt of signals from the satellite constellation. So precise is this timing that GPS time data, including stoplight timing, is now an integral part of traffic control systems. They are also crucial for the operation of automated teller machines that enable banking customers to obtain cash when they are not at a branch of their primary banking institution and are integrated into the machines that process credit and debit card purchases. GPS timing data control the sequencing of mobile phone calls through the cellular tower network in many countries. Airlines rely on them for direct-route navigation. They also control the switching of power networks and the transfer of electrical power between grids to avoid power surges on power lines as generators are brought online or taken offline as the power load increases and decreases.[52] The reliance on these signals is rapidly increasing.[53]

The loss of this satellite constellation alone would suddenly stop credit card transactions, produce gridlock in many of the world's cities as traffic lights ceased to operate, take the mobile phone network offline, and keep bank customers from being able to withdraw cash from their savings or checking accounts unless they dealt directly with a bank teller at their banking institution. The second- and third-order effects to people's lives and the nation's economy would be considerable.

Other satellites provide us with data essential for weather warnings, facilitate long-distance telecommunications, transmit television signals, and enable rapid transfers of data from distant locations. These systems are all potentially vulnerable as well.

From a military standpoint, military aviation and ground system locations are dependent, at least in part, on GPS positioning. Military operations are affected by the weather, and satellite pictures and the atmospheric data embedded therein are crucial to modern weather forecasting.[54]

The study team's research and interviews with a variety of space-reliant companies and government agencies revealed that, much like the national critical infrastructure on the ground, our space assets are poorly protected.[55] As with the ground-based systems, the cost of hardening or making these systems resilient to attack is greater than the cost of insuring them against loss, and as such, a positive financial market disincentive exists to address any current or projected space vulnerabilities.

Notes

1. Peter Schwartz, *The Art of the Long View* (New York: Doubleday, 1991), 17–169.

2. See the argument presented by Peter Schwartz, *Inevitable Surprises: Thinking Ahead in a Time of Turbulence* (New York: Gotham Books, 2003).

3. Idaho National Laboratory, US Department of Energy, "Protecting the National Infrastructure: Idaho's Test Range," fact sheet (Idaho Falls, ID: Idaho National Laboratory, n.d.), accessed 14 May 2012, http://www.inl.gov/nationalsecurity/factsheets/docs/critical_infrastructure_test_range.pdf.

4. The precise area of attack appears to remain classified, so the authors cannot say what system or set of systems was affected to result in the catastrophic failure of the generator. That the generator catastrophically failed is known and was aired on CNN News and is also available via other media, including YouTube. For the original article on the test, see Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," *CNN.com*, 26 September 2007, accessed 14 May 2012, http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US.

5. Jill Slay and Michael Miller, "Lessons Learned from the Maroochy Water Breach," *Critical Infrastructure Protection* 253 (November 2007): 73–82. For a broader discussion of these events, see also Rose Tsang, "Cyberthreats, Vulnerabilities and Attacks on SCADA Networks" (working paper, University of California–Berkeley, 2009), accessed 14 May 2012, http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf.

6. Pierre Thomas, "Teen Hacker Faces Federal Charges," *CNN Interactive*, 18 March 1988, http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html.

7. For more on this see David E. Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy* (New York: Anchor Books, 2010), 35.

8. Microsoft developed "Photosynth," a program to stitch pictures together smoothly and seamlessly. Available on the Internet for free, the program enables compilation of images across space and time to produce the ability to conduct three-dimensional walk-throughs of any facility ever photographed. For more see John P. Geis II, Ted Hailes, and Grant Hammond, "Technology and the Comprehensive Approach: Part Problem, Part Solution," in *Capability Development in Support of Comprehensive Approaches: Transforming International Civil-Military Relations*, ed. Derrick Neal and Linton Wells (Washington, DC: National Defense University Press, 2011), 69–86.

9. Ibid.

10. Human Genome Program, Office of Biological and Environmental Research, Department of Energy, "Human Genome Project Information," 31 July 2012, http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml.

11. Michael B. Miller, "How Tall of a Stack of Paper Would We Need to Print Out an Entire Human Genome?," working paper (Minneapolis: Division of Epidemiology and Community Health, University of Minnesota, 15 October 2005), http://bio4.us/biotrends/human_genome_height.html.

12. Human Proteome Organisation (HUPO), "Human Proteome Project (HPP)," HUPO, 21 March 2012, accessed 14 May 2012, http://www.hupo.org/research/hpp/.

13. More specifically, these medications are called tyrosine-kinase inhibitors, and they block reproduction by inhibiting the enzymes involved in signal transduction cascades by adding a phosphate group to the appropriate protein. For some of the latest in developments on the leukemia medications, see Nicholas J. DiBella, "First-line Treatment of Chronic Myeloid Leukemia: Imatinib versus Nilotinib and Dasatinib," *Community Oncology* 8, no. 2 (February 2011): 65–72.

14. "Mouse Pox or Bioweapon?," *BBC World Service*, 17 January 2001, accessed 15 May 2012, http://www.bbc.co.uk/worldservice/sci_tech/highlights/010117_mousepox.shtml.

15. William Bains, *Biotechnology from A to Z* (New York: Oxford University Press, 2004), 52.

16. The dictionaries issued to the authors by the federal government are among those that do not yet contain an entry for *nanotechnology*.

17. Stores J. Hall, *Nanofuture: What's Next for Nanotechnology* (Amherst, NY: Prometheus, 2005), 15–22.

18. Definition synthesized from ibid., 15–51.

19. Leading biological scientists, interviews.

20. Witold Gutkowski and Tomasz A. Kowalewski, *Mechanics of the 21st Century: Proceedings of the 21st International Congress of Theoretical and Applied Mechanics, Warsaw, Poland, 15–21 August 2004* (Dordrecht, Netherlands: Springer, 2005), 379; and Oleg Vasylkiv, Yoshio Sakka, and Valeriy V. Skorokhod, "Nano-Blast Synthesis of Nano-size CeO_2-Gd_2O_3 Powders," *Journal of American Ceramic Society* 89, no. 6 (June 2006): 1822–26.

21. John W. Cole, Isaac F. Silvera, and John P. Foote, "Conceptual Launch Vehicles Using Metallic Hydrogen Propellant," *American Institute of Physics Conference Proceedings* 969 (2008): 977–84.

22. It is interesting to note that a yield increase of 1,000-fold would create a set of conventional ordnance with yields in excess of the bombs dropped on Hiroshima and Nagasaki during World War II. This would necessitate revisiting the question of what constitutes a weapon of mass destruction.

23. Ancel Yarbrough, *The Impact of Nanotechnology Energetics on the Department of Defense by 2035* (Maxwell AFB, AL: Air War College, 2010), http://www.au.af.mil/au/awc/awcgate/cst/bh2010_yarbrough.pdf.

24. Henry D. Baird et al., "Spacelift 2025: The Supporting Pillar for Space Superiority," in *Air Force 2025*, vol. 2 (Maxwell AFB, AL: Air University Press, 1996), 117–50.

25. Of course nanotechnology, like biotechnology above, can cut both ways. The same basic science that can create nanocorrosives can also create nanocoatings that would make systems resist corrosion. There are over 30,000 scholarly articles on this subject. Among the more heavily cited are S. Radhakrishnan et al., "Conducting Polyaniline-nano-TiO_2 Composites for Smart Corrosion Resistant Coatings," *Electrochimica Acta* 54, no. 4 (30 January 2009): 1249–54; Lidia Benea et al., "Wear Corrosion Properties of Nano-Structured SiC-Nickel Composite Coatings Obtained by Electroplating," *Wear* 249, no. 10–11 (November 2001): 995–1003; and Martin Kendig, Melitta Hon, and Leslie Warren, " 'Smart' Corrosion Inhibiting Coating," *Progress in Organic Coatings* 47, no. 3 (September 2003): 183–89.

26. The study participants believe that the United States, Russia, China, the United Kingdom, France, India, Pakistan, Israel, and North Korea are nuclear states. Iran and Myanmar appear to be attempting to join the ranks though this is not knowable with certitude.

27. A discussion of the chain reaction necessary and the detonation of a nuclear weapon can be found in George Shortley and Dudley Williams, *Elements of Physics*, 5th ed. (Englewood Cliffs, NJ: Prentice Hall, 1971), 924–27. This book was used for high school physics at Brookfield East High School, in Brookfield, Wisconsin, in 1979. As this was the book's fifth printing, the authors make the assumption that it was likely being used in several other learning institutions at the same time.

28. House of Representatives, *Electromagnetic Pulse Threats to U.S. Military and Civilian Infrastructure: Hearing before the Military Research and Development Subcommittee of the Committee on Armed Services, 106th Cong., 1st sess., 7 October 1999* (prepared statement of Lowell Wood, member of director's technical staff, Lawrence Livermore National Laboratory), 30–36. See also John P. Geis II, *Directed Energy Weapons on the Battlefield: A New Vision for 2025* (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2003), 8–11.

29. *Electromagnetic Pulse Threats*; and Geis, *Directed Energy Weapons*.

30. A. B. Pittock et al., "Direct Effects of Nuclear Detonations," in *Environmental Consequences of Nuclear War*, vol. 1, ed. A. Barrie Pittock, Mark Harwell, and T. C. Hutchinson (New York: John Wiley and Sons, 1986), 1–23.

31. Geis, *Directed Energy Weapons*, 9.

32. Pittock et al., "Direct Effects of Nuclear Detonations," 17–20; and Geis, *Directed Energy Weapons*, 11–14.

33. For a complete discussion on the precise thresholds of field strength to cause certain levels of damage, see Geis, *Directed Energy Weapons*, 11–15.

34. There is a method to harden computer chips against this phenomenon, but such hardening is expensive, and very few foundries in the world produce these chips.

35. Carlo Kopp, "The Electronmagnetic Bomb—A Weapon of Electrical Mass Destruction," *Air and Space Power Journal: Chronicles Online Journal,* 1996, http://www.airpower.au.af.mil/airchronicles/cc/apjemp.html.

36. Geis, *Directed Energy Weapons*, 11–15.

37. Paul Kintner (professor of electrical and computer engineering, Cornell University), interview by the authors, 17 September 2009. Dr. Kintner served on the science board of the National Academies and was regarded as one of the nation's leading scientists on the impacts of space weather on both space and terrestrial systems. He was also the director of the Global Positioning Systems Laboratory at Cornell.

38. Leigh Dayton, "Solar Storms Halt Stock Market as Computers Crash," *New Scientist*, 9 September 1989, 35. Dayton also quotes Canadian scientists as attributing rashes of computer failures across the country—to include individuals". As such, it would typicall personal computers at home—to the solar flare activity of March 1989.

39. Tony Phillips, "Solar Shield—Protecting the North American Power Grid," *NASA Science News*, 26 October 2010, accessed 19 December 2012, http://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield/.

40. The biggest flares are known as "X-class flares," based on a classification system that divides solar flares according to their strength. The smallest ones are A-class (near background levels), followed by B, C, M, and X. Similar to the Richter scale for earthquakes, each letter represents a 10-fold increase in energy output. So an X is 10 times stronger than an M and 100 times stronger than a C. Within each letter class there is a finer scale from 1 to 9.

C-class and smaller flares are too weak to affect Earth noticeably. M-class flares can cause brief radio blackouts at the poles and minor radiation storms that might endanger astronauts.

Although X is the last letter used in the scale, there are flares more than 10 times the power of an X1; so X-class flares can go higher than 9. The most powerful flare measured with modern methods occurred in 2003, during the last solar maximum, and it was so powerful that it overloaded the sensors measuring it. The sensors cut out at X28. Mark Paquette, "What Exactly is an X Class Solar Flare?" *Astronomy Blog,* AccuWeather.com, 10 March 2011, accessed 5 March 2013, http://www.accuweather.com/en/weather-blogs/astronomy/what-exactly-is-a-xclass-solar-flare/53605.

41. Committee on the Societal and Economic Impacts of Severe Space Weather Events, Space Studies Board, National Research Council of the National Academies, Severe Space Weather Events—Understanding Societal and Economic Impacts (Washington, DC: National Academies Press, 2008), accessed 17 May 2012, http://www.nap.edu/catalog/12507.html; and Kintner, interview. The National Academies estimate the economic impact at over $1 trillion and perhaps as much as $2 trillion, or a loss of roughly 10 percent of gross deomestic product, which is the economic definition of a depression. Some of the over 130 million people who would lose electricity in such a scenario would have to wait the entire six years before the lights came back on though restoration to others via rolling blackouts could happen more quickly.

42. Trudy E. Bell and Tony Phillips, "A Super Solar Flare," *NASA Science News*, 6 May 2008, accessed 17 May 2012, http://science.nasa.gov/science-news/science-at-nasa/2008/06may_carringtonflare/.

43. Kintner, interview.

44. Michael Walters (Department of Homeland Security), e-mail and phone conversations with the authors. Kenneth Friedman (Department of Energy), e-mails and phone conversations with the authors. In e-mail and telephone conversations, both sources confirmed that there are no plans in place to address the challenges posed to the national critical infrastructure by solar flares or other like effects. E-mails and phone conversations occurred 9–13 May 2010.

45. No endorsement of the product being discussed is intended or implied. The products listed here are dangerous and require substantial training to handle safely. For academic purposes, additional data may be found at "Spyder Arctic," Wicked Lasers, accessed 15 January 2013, http://www.wickedlasers.com/lasers/Spyder_III_Pro_Arctic_Series-96-37.html. Following our initial research, a new company began marketing an

even smaller laser that is much more powerful than the Spyder. Its laser creates temperatures of up to 850 degrees at the point of lasing.

46. The authors searched for importation restrictions on lasers across the world. While it is possible some were missed, after an exhaustive search, only the country of Malta had laws we could locate that prevented the importation of a category IV device.

47. The authors presented early findings at the Aircraft Survivability Conference in Berlin, Germany, 13 October 2010. Discussions with members of the German parliament who were present revealed concern over recent lasing incidents on the autobahn. These government leaders were unaware of the newly marketed handheld device.

48. Matthew Potter, "Boeing Video of Advanced Tactical Laser (ATL) Aircraft," *Defense Procurement News*, 2 October 2009, accessed 25 May 2011, http://www.defenseprocurementnews.com/2009/10/02/boeing-video-of-advanced-tactical-laser-atl-aircraft/.

49. Geis, *Directed Energy Weapons*, 16.

50. Craig Covault, "Chinese Test Anti-Satellite Weapon," *Aviation Week and Space Technology*, 17 January 2007, accessed 19 December 2012, http://www.spaceref.com/news/viewnews.html?id=1188.

51. William Diehl, *Continued Optical Sensor Operations in a Laser Environment* (Maxwell AFB, AL: Air War College, 2011), http://dtlweb.au.af.mil///exlibris/dtl/d3_1/apache_media/L2V4bGlicmlzL2R0bC9kM18xL2FwYWNoZV9tZWRpYS81NjcwOA==.pdf.

52. National Coordination Office for Space-Based Positioning, Navigation, and Timing (NCO), "GPS Applications," 10 April 2012, http://www.gps.gov/applications/. As of 18 May 2012, GPS.gov is the official US governmental GPS website. The reader should note that the uses of GPS listed here are not exhaustive, and many others can be found on the site.

53. P. Daly, "Navstar GPS and GLONASS: Global Satellite Navigation Systems," *Electronics and Communication Engineering Journal* 5, no. 6 (December 1993): 349–57.

54. NCO, "GPS Applications"; and National Environmental Satellite, Data, and Information Service (NESDIS), "NOAA's Geostationary and Polar-Orbiting Weather Satellites," *NOAA Satellite Information System*, 6 December 2011, accessed 18 May 2012, http://noaasis.noaa.gov/NOAASIS/ml/genlsatl.html.

55. Hardening efforts remain stable but at low levels. In late 2010, Honeywell introduced a radiation-hard, 64-megabyte memory for satellites. This is the state of the art, which greatly lags chip sets and memory for terrestrial-based personal computers. For more information, see John McHale, "Radiation-Hardened Electronics Technology Remains Stable amid Steady Demand in the Space Market," *Military and Aerospace Magazine*, 21 May 2010, accessed 18 May 2012, http://www.militaryaerospace.com/articles/2010/05/radiation-hardened-electronics.html; and John Keller, "Megarad-Level Rad-Hard 64-Megabit Solid-State Memory Introduced by Honeywell for Military Satellites," *Military and Aerospace Magazine*, 10 December 2010, accessed 18 May 2012, http://www.militaryaerospace.com/articles/2010/12/megarad-level-rad-hard.html.

Chapter 3

A Structural Model of Deterrence

In order to evaluate the six technological threats previously discussed, the study team had to understand deterrence concepts and deterrence theory. The team undertook an intensive effort to review the literature on both conventional as well as nuclear deterrence theory and to determine what key elements transcended the writings of the various authors that helped the world develop an understanding of this dynamic.

Based on more than 20 works and deliberately selected to span Western and Eastern cultures, the model, depicted in figure 8, depicts already acknowledged aspects of deterrence theory and their relationships to each other.[1] As such, it became a framework for thinking and analysis. While the study team considered attempting to engage in Bayesian probability modeling as a study methodology, the necessary data was not readily available, and such an analysis could not be conducted within the study deadlines.[2] This model, however, could be used to undertake such efforts as part of a future research program.

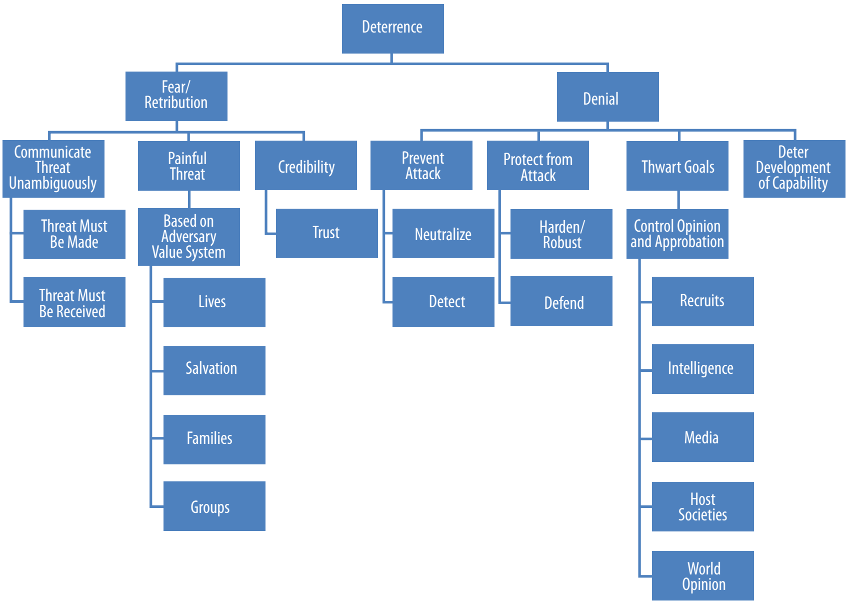


Figure 8. A structural model of deterrence theory

As the team examined the literature, it became clear that the focus during the Cold War was mainly on the left half of the model—the side labeled "Fear/Retribution." This thinking made sense because during this time frame, the treaties in effect limited each side (the United States and Soviet Union) to 100 ballistic missile interceptors.[3] Since each side in the Cold War had vastly more than 100 nuclear weapon systems, there was an implicit assumption that it would be impossible to deny the opposing side the ability to carry out a massive strike that would inflict severe damage on the opponent should it choose to do so. As a result, the "denial" side of the equation was limited in value only to that which was necessary to ensure that a retaliatory capability existed. There was no method by which one could deny the initial attack, and as such, much of the denial side of the model was ignored, leaving mutual destruction or unacceptable levels of damage (fear) as the linchpin upon which deterrence was based.

This study concludes that with regard to many of the future threats, the relative importance of the two sides of deterrence theory changes. It is important to recognize that the theory itself is structurally sound. The difference is that with regard to many of the threats we face in the future, there are opportunities to prevent or protect from attacks, to thwart the goals of prospective adversaries, and to deter or hinder the development of these capabilities in the first place. These key elements of the right-hand side of the model take on new levels of importance in the future and thus constitute a change in the way in which the Department of Defense and the Department of the Air Force need to operate in the future.

In operationalizing the model against the array of future threats, many of which are conventional, we turned to an equation verbally described in John J. Mearsheimer's book *Conventional Deterrence*. Mearsheimer argues that the failure of deterrence is specified as a calculus in the mind of the actor to be deterred, referring to this calculus as "the attacker's fear to the consequences of . . . action."[4] While Mearsheimer describes this calculus in great detail, this study turned it into a mathematical expression. An actor is deterred if the equation depicted in figure 9 holds.

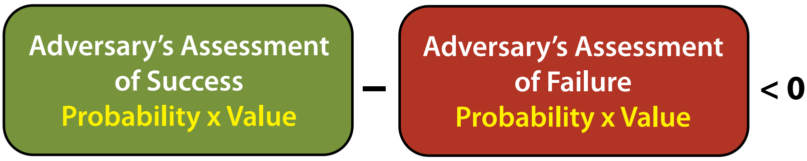


Figure 9. The deterrence equation

Mearsheimer argues that several factors play in this calculus of whether deterrence will succeed. The first is the adversary's perception of the value of success itself—the gain to be incurred by attacking. The second factor is the probability that the attack will succeed. The product of these two elements comprises the potential adversary's assessment of success (green box in fig. 9). Only if the assessment of failure is greater than that of success will a rational actor be deterred. This failure assessment is calculated in much the same manner—the cost of failing is multiplied by the probability of failure. If the failure assessment (red box) is the greater of the two terms, then the value of the equation is less than zero, and the actor is deterred.[5]

Some presuppositons embedded in this calculus are assumptions that must be highlighted in light of the new threats. First, it assumes the actor is rational. This does not mean that the actor's calculus is the same as one's own or that it matches one's values—only that it has a rational basis underpinning it. Second, it assumes that one can attribute the attack to the proper actor. While in the nuclear era this was relatively easy, as nation-states launching ballistic missiles in a global thermonuclear war do leave behind a "calling card" of sorts, this has recently proven much more difficult in newly created artificial domains such as cyberspace.

In fact it is important to explore what happens to the deterrence equation in the absence of attribution. Should attribution be problematic, it tilts both parts of the deterrence equation in favor of the potential aggressor. An inability to attribute an attack means that the probability of successfully carrying it out likely rises or at a minimum remains the same. The probability of incurring punishment clearly diminishes because without attribution it is impossible to know toward whom the punishment should be directed. As a result, in the absence of proper attribution, the deterrence equation tilts in favor of the potential adversary, making successful deterrence less likely.

Of equal concern is what happens when attribution is either assumed or figured incorrectly. A failure to properly attribute often leads to simple-minded decisions along the lines of what actors expect.[6] Further, in the absence of data or in the midst of uncertainty, decision makers tend to engage in more violent modes of coping with the ambiguity.[7] These dynamics were tested in exercises conducted by CSAT in conjunction with this research—exercises that placed participants in a war game in a position of relative uncertainty with regard to adverse conditions experienced by the United States and its allies. Even though sufficient data were available to the participants to uncover the actual actors, the dynamics predicted by attribution theory above were present. The vast majority of the participants attributed the hostile actions to the wrong actor.

In a real-world situation, such misattribution can have disastrous consequences. When Japan sequestered the Chinese fishing vessel for transgressing its territorial waters in the Senkaku Islands on 8 September 2010, imagine that a third-party state had launched a cyber attack against the United States via servers within mainland China. Had such an event occurred, and had the United States then misattributed the source of the attack to the Chinese government (an occurrence predicted by attribution theory), then the ensuing consequences would have been of a type that Japan, China, and the United States would not have wanted. Getting attribution correct is essential not only to realize deterrence but also to avoid unintended conflict.

Complicating the problem of attribution is the fact that the time to respond to attacks from several emerging threats is much less than the reaction time that was available in the nuclear deterrence era. As a result, the time necessary to observe events, orient to these events, decide on a course of action, and then act on that decision (a cyclical process designated by John Boyd as the observe-orient-decide-act [OODA] loop) is shrinking.[8] With several new technologies operating either at or near the speed of light, this decision loop is rapidly shrinking toward a point requiring much more rapid capabilities to observe and attribute incoming attacks.

We can see this dynamic at work in recent events. On 6 May 2010 at approximately 2:32 p.m. (EDT), a large mutual fund complex executed a single sell order for 75,000 E-Mini Standard & Poor's (S&P) 500 contracts, a trade valued at approximately $4.1 billion.[9] The sell order was programmed to execute sales at a level equal to 9 percent of the rate at which the securities had been sold up to that point in the day but without regard to price. In essence this was an order to sell these contracts at market price. While this was a large order, it was only the third-largest purchase for this security in the preceding 12 months. Nonetheless, after about nine minutes, the existing demand for these contracts had been exhausted, and the price was falling quickly, with the Dow Jones Industrial Average already down nearly 600 points. This caused short-term traders to sell shares in the equities markets to cover their losses on the S&P contracts. The result was a sudden fall in the market price of the S&P 500 and other equities within the markets. By 2:46 p.m., the Dow Jones average had fallen 1,000 points in 10 minutes. The investigation into the event showed that the original sell order triggered a trading "tipping point" that had been built into algorithms within the market's mechanisms. When all automatic trading mechanisms were halted just before 2:46 p.m., market prices began to recover.

The investigation as to how this event, called the "Flash Crash" or "Crash of 2:45 PM," occurred revealed that computer trading had moved so quickly that the machines were selling and buying shares of stocks and contracts faster than investors could keep up. This is a classic example of a complex dynamic system—sometimes called a chaotic system—in which tipping points that, if crossed, rapidly takes the system to a new state.[10]

The nation-states that comprise our global security system are similarly chaotic and capable of rapidly tipping from one state to the next. This is not merely a phenomenon of machines. For example, on 28 June 1914, the assassination of Archduke Franz Ferdinand of Austria triggered a conflict grossly out of proportion to the initial act. More than 9 million combatants would die in the conflict that ensued, which eventually involved large sections of the planet. In short, human society also can have tipping points where single acts or small sets of acts can cause reactions much larger than would normally be expected.

In the end, the human system in which we must deter is complex and chaotic. It has tipping points. Automation changes the speed with which these events can occur. In the "Crash of 2:45 PM," roughly 10 minutes elapsed between the time a decision to sell contracts was executed and the point at which the stock market had lost trillions of dollars in value. In the case of World War I, a full month elapsed between the assassination of Archduke Ferdinand and the Austro-Hungarian Empire's invasion of the Kingdom of Serbia. In the modern age, time is disappearing. The OODA loop decision cycle is shrinking and rapidly collapsing into an OODA point. As attacks and actions today can be initiated at the speed of light by ever-faster computers and weapon systems, the credibility of deterrence hinges on the capacity to accurately attribute such actions at ever-increasing speeds.

Notes

[1] We derived the model primarily from the following scholars and works (the list is not exhaustive): Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966); Paul Huth and Bruce Russett, "What Makes Deterrence Work? Cases from 1900–1989," *World Politics* 36, no. 4 (July 1984): 496; Lawrence Freedman, *Deterrence* (Malden, MA: Polity Press, 2004); Christopher Layne, "From Preponderance to Offshore Balancing," in *The Use of Force: Military Power and International Politics*, 7th ed., ed. Robert J. Art and Kenneth N. Waltz (Lanham, MD: Rowman and Littlefield Publishers, 2009), 311–26; Andrew J. Goodpaster, C. Richard Nelson, and Seymour J. Deitchman, "Deterrence: An Overview," in *Post–Cold War Conflict Deterrence* (Washington, DC: National Academy Press, 1997), 10–38; Keith B. Payne, *The Fallacies of Cold War Deterrence* (Lexington: University Press of Kentucky, 2001); Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. (New York: Longman, 1999); John P. Geis II et al., Discord or "*Harmonious Society*"? China in 2030, Occasional Paper no. 65, Center for Strategy and Technology (Maxwell AFB, AL: Air University Press, 2011); Bruce Russett and Alan C. Stam, "Courting Disaster: An Expanded NATO vs Russia and China," *Political Science Quarterly* 113, no. 3 (Fall 1998): 361–82; Keith B. Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-First Century* (Fairfax, VA: National Institute Press, 2008); Union of Concerned Scientists, "Nuclear Weapons & Global Security: History of Russia's Anti-Ballistic Missile System," 2012, http://www.ucsusa.org/nuclear_weapons_and_global_security/missile_defense/policy_issues/history-of-russias.html; Yao Yunzhu, "Chinese Nuclear Policy and the Future of Minimum Deterrence," *Pacific Forum CSIS* 6, no. 2 (September 2005): 31–40, http://csis.org/files/media/csis/pubs/issuesinsights_v06n02.pdf; Kenneth N. Waltz, "Nuclear Myths and Nuclear Realities," in *The Use of Force: Military Power and International Politics*, 6th ed., ed. Robert J. Art and Kenneth N. Waltz (Malden, MA: Rowman and Littlefield, 2004), 102–18; Bob Gourley, "Towards a Cyber Deterrent," working paper (Vienna, VA: Cyber Conflict Studies Association, 29 May 2008), http://www.ctovision.com/cyber-deterrence-initiative.html; Thomas P. M. Barnett, "Deterrence in the 21st Century," in *Deterrence 2.0: Deterring Violent Non-State Actors in Cyberspace*, ed. Carl Hunt and Nancy Chesser (Washington, DC: US Strategic Command Global Innovation and Strategy Center, 10 January 2008), 25–31; Edward D. Mansfield, *Power Trade and War* (Princeton, NJ: Princeton University Press, 1994); John J. Mearsheimer, *Conventional Deterrence* (Ithaca, NY: Cornell University Press, 1985); Jack S. Levy, "The Causes of War: A Review of Theories," in *Behavior, Society and Nuclear War*, vol. 1, ed. Philip E. Tetlock et al. (New York: Oxford University Press, 1989), 209–333; A. F. K. Organski and Jacek Kugler, *The War Ledger* (Chicago: University of Chicago Press, 1980); Michael W. Doyle and Stephen Macedo, *Striking First: Preemption and Prevention in International Conflict* (Princeton, NJ: Princeton University Press, 2008); T. V. Paul, Patrick M. Morgan, and James J. Wirtz, eds., *Complex Deterrence* (Chicago: University of Chicago Press, 2009); and Anthony C. Cain, ed., *Deterrence in the Twenty-First Century: Proceedings* (Maxwell AFB, AL: Air University Press, 2010).

2. Bayesian probability theory provides a mathematical framework for performing inference using probability. It is used to judge the relative validity of hypotheses given sparse or uncertain data.

3. Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, US-USSR, 26 May 1972, accessed 18 May 2012, http://www.state.gov/t/isn/trty/16332.htm.

4. Mearsheimer, *Conventional Deterrence*, 23.

5. This calculus can be traced to Thucydides, who lamented in the fifth book of his *History of the Peloponnesian War* that in war "one side thinks that the profits to be won outweigh the risks to be incurred, and the other side is ready to face danger rather than accept an immediate loss." Cited in Athanassios G. Platias and Constantinos Koliopoulos, *Thucydides on Strategy: Grand Strategies in the Peloponnesian War and Their Relevance Today* (New York: Columbia University Press, 2010), 125.

6. Harold H. Kelly, "The Process of Causal Attribution," *American Psychology* 28, no. 2 (1973): 107–28; Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (27 September 1974): 1124–31; and Richard Nisbett and Lee Ross, *Human Interference: Strategies and Shortcomings of Social Judgment* (Englewood Cliffs, NJ: Prentice Hall, 1980).

7. Irving L. Janis and Leon Mann, *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment* (New York: Free Press, 1977); Daniel Heradstveit and G. Matthew Bonham, "Decision-Making in the Face of Uncertainty: Attributions of Norwegian and American Officials," *Journal of Peace Research* 23, no 4. (December 1986): 339–56.

8. John R. Boyd, briefing, subject: A Discourse on Winning and Losing, 1987, accessed 20 December 2012, http://dnipogo.org/john-r-boyd/.

9. US Commodity Futures Trading Commission, US Securities and Exchange Commission, *Findings Regarding the Market Events of May 6, 2010: Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues* (Washington, DC: Securities and Exchange Commission, 30 September 2010), 2, accessed 21 May 2012, http://www.sec.gov/news/studies/2010/marketevents-report.pdf. An E-Mini is an electronically traded futures contract on the Chicago Mercantile Exchange that represents a portion of the normal futures contracts. E-Mini contracts are available on a wide range of indexes such as the NASDAQ 100, S&P 500, S&P MidCap 400, and others. For example, the E-Mini S&P 500 futures contract is one-fifth the size of the standard S&P 500 futures contract. Advantages to trading E-Mini contracts include liquidity, greater affordability for individual investors, and around-the-clock trading.

10. James Gleick, Chaos: *Making of a New Science* (New York: Viking, 1987).

Chapter 4

The Delphi Study and Results

To better understand where the greatest challenges for deterrence lay, the study directors conducted a formal and informal Delphi study.[1] It drew upon participants (called "oracles" in the Delphi method) who had studied the six technologies under examination and had a working knowledge of deterrence theory and military strategy. These individuals were asked to respond in a manner that preserved their anonymity but made their comments, rationale, and ratings visible to all. After three rounds of the study, we had achieved consistency in the ratings for each of the three questions we sought to explore. Each question explored all of the six technologies and parsed the responses to separate dynamics that differed among nation-states, groups, and individuals.

The first question asked the respondents to use a Likert scale of one to five (very easy, easy, neutral, difficult, and very difficult) to rate the level of difficulty of deterring nation-states, groups, and individuals from launching an attack using each of the technologies shown in figure 10. The results show that it is more difficult to deter individuals, regardless of technology explored, than to deter nation-states. In addition we found that the team believed that bio-, nano-, and cyberspace technologies would likely be the most difficult to deter. Further, although the slope changed for each technology, the relationship across the three categories took on a mostly linear shape.

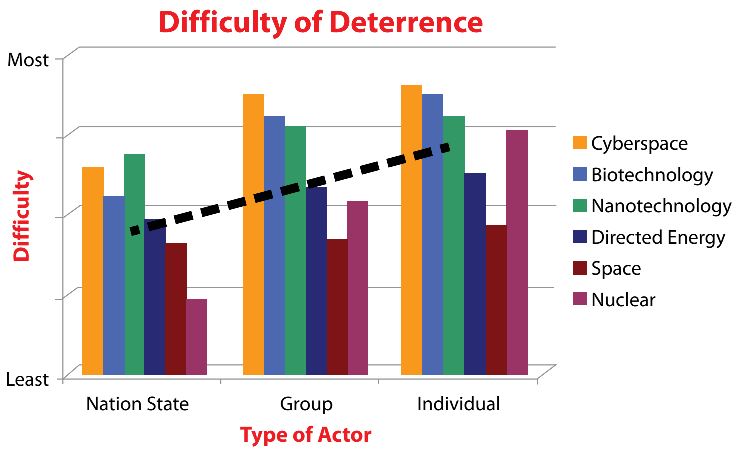


Figure 10. Difficulty of deterrence: Delphi results

In the anonymous discussions during the formal Delphi sessions and in the broader discussions that took place during the informal Delphi study, the respondents were asked why this relationship was perceived as it was. In general the study participants believed that nation-states and groups placed value in their respective reputations. Moral constraints to use force and the results of international approbation act most strongly on nation-states.[2] Yet the oracles believed that for groups, especially the larger ones, the reputational issues were strong enough to make them easier to deter than small groups and individuals. Individuals, they argued, would be least affected by international norms and thus the hardest to deter.

The second question focused on the difficulty of attribution. As with the previous question, this one was parsed by both type of actor and technologies involved.

The graph (fig. 11) takes on the same shape as the previous one but for different reasons. Here the individuals were considered the most difficult to attribute across all six technologies since they were the most likely to conduct an attack and successfully avoid leaving a distinguishing trail that would lead to properly attributing the source of the attack. Nation-states, on the other hand, because of their size and the bureaucracies that must approve these actions, often leave traceable indications of their responsibility for certain actions. Additionally, in some cases, the research efforts necessary to launch attack programs by nation-states in these areas would require funding of sufficient size to make it possible to trace the program.

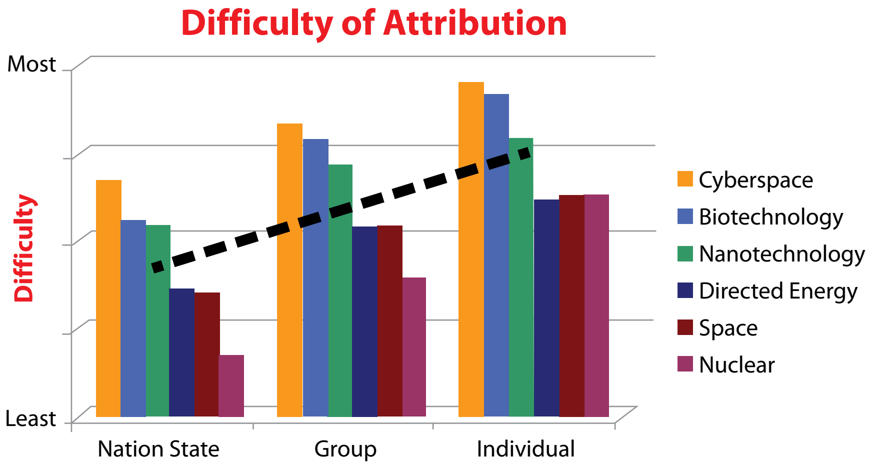


Figure 11. Difficulty of attribution: Delphi results

The respondents perceived three types of technologies to be much harder to attribute than the rest. Attacks in cyberspace were considered difficult to attribute because, with proper planning, the attacks could be made difficult to trace and routed through third-party servers. Biological attacks were considered problematic because tracing the source of a disease or pathogen may be difficult, especially if it has a considerable incubation period. Should such an agent be distributed at a major transit hub, such as a major international airport, viruses would be hard to trace to their origins since the passenger traffic would leave a very large number of potential paths to trace.[3] Nanotechnology threats were also considered difficult because they are small enough in size that they could remain dormant for extended periods, leaving great doubt as to when they were positioned.

The last area in which we collected data via the formal Delphi method regarded the likelihood of attack. Here, definitions proved important insofar as we were interested in the likelihood of only very large destructive or catastrophic events. For this segment of the study, a "catastrophic" attack was considered one that "threatens national survival or eliminates the US Air Force's ability to accomplish its mission." A "destructive" attack was one that "seriously impacts the US's ability to function or significantly degrades the US Air Force's ability to perform its mission." We asked the respondents to use a betting scheme that gave each of them $400 and even odds. We then instructed them to place bets on where the next destructive or catastrophic attack would occur, ignoring attacks below the destructive threshold for this exercise.

The results of this exercise are depicted in figure 12, which contains three patterns within the data that are worthy of explanation. First, the greatest perceived threats to the functioning of the United States or its Air Force were based on either biotechnology or cyberspace. The oracles believed that significant catastrophic risk to the nation and the Air Force resided in these two areas. The respondents believed this danger significant due to the relatively unprotected nature of the infrastructure against cyberspace attack and a very incomplete infrastructure to detect novel pathogens or viruses. Second, for three of the six technologies, the graph has a central "hump," showing a greater probability of catastrophic or destructive attacks coming from groups than from individuals or nation-states. In all three cases—cyberspace, biotechnology, and nuclear weapons—the oracles believed that the nation-states would be somewhat self-deterred due to the reputational issues previously mentioned. However, they also believed that very few individuals, if any, would be able to garner the resources single-handedly to create an attack of destructive or catastrophic scale. This created a curve for these three technologies that placed the maximum likelihood for attack at the group level. It should be noted that had we lowered the damage threshold of interest, it is likely that individuals would have scored much higher. Lastly, for the remaining three technologies (nanotechnology, directed energy, and space), nation-states were considered the most likely to attack catastrophically because we deemed it unlikely that even groups would have the resources to attack using these weapons on a massive scale.

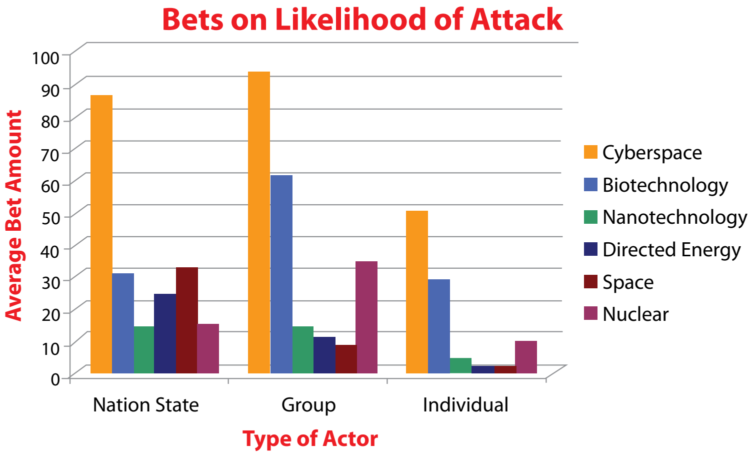


Figure 12. Likelihood of catastrophic attack: Delphi results

The study team then plotted all three of these Delphi results in three-dimensional space to get a better picture of the threat space. Depicted in figure 13, this plot shows that cyberspace and biological threats are the most critical, with some nuclear and space issues worthy of highlighting.

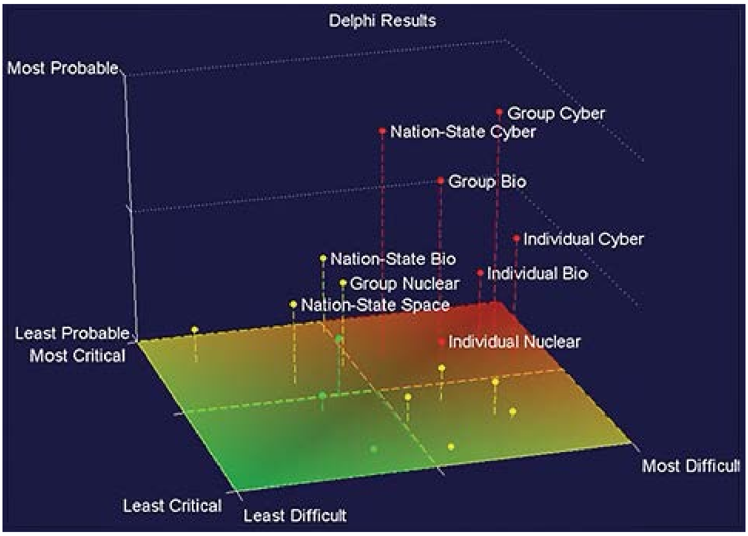


Figure 13. Delphi study threat data in 3-D

Notes

[1] Norman Dalkey and Olaf Helmer, *An Experimental Application of the Delphi Method to the Use of Experts* (Santa Monica, CA: RAND, July 1962); Harold A. Linstone and Murray Turoff, eds., *The Delphi Method: Techniques and Applications* (University Heights: New Jersey Institute of Technology, 2002).

[2] William D. Rogers, "The Principles of Force, the Force of Principles," in *Right v. Might: International Law and the Use of Force*, ed. Louis Henkin et al. (New York: Council on Foreign Relations, 1991), 95–108.

[3] This type of thinking can also be found in Ali Karami, "Pandemics and Its Consequences for the Future of Asia," in *Imagining Asia in 2030: Trends, Scenarios and Alternatives*, ed. Ajey Lele and Namrata Goswami (New Delhi, India: Academic Foundation Press, 2011), 153–65; and Angela Woodward, "Biological and Chemical Terrorism," in Lele and Goswami, *Imagining Asia* in 2030, 323–35.

Chapter 5

Findings and Implications for the US Air Force

The purpose of this study was to discern the role of the US Air Force in deterring future technologies. The report examines the issues that the study team uncovered which are directly relevant to the Air Force.

The study concluded that the answer to the fundamental thesis—how the Air Force should position itself to deter future threats—begins with its history. The Air Force and its forerunner, the Army Air Corps, pioneered flight. Initially, these flights were in lighter-than-air balloons and then in early aircraft. Airmen used these craft to see over the trenches in warfare, direct cannon, and gather the intelligence to allow for artillery attacks against the enemy.[1] In more recent years, the Air Force has led in the area of cyberspace. Since the service's inception, reconnaissance has always been part of its core mission set.[2] In fact, of the targeting chain frequently referred to as find, fix, track, target, engage, and assess (F2T2EA), surveillance and reconnaissance are an integral part of five of its six steps. In short, diminishing the "fog of war" was at the heart of both the Army Air Corps's creation and the Air Force's becoming a separate service. It remains a crucial role for the service today.[3]

Transparency

The first main finding of this study is that increased transparency is necessary to facilitate proper attribution and early warning of attack. Transparency has three elements. The first is technical developments that aid in tracking people and objects through space and time. The second is ongoing innovation in this area, and the last is the advent of new command and control concepts.

With the development of the Internet, most data—public and private—is archived for retrieval. Even when websites are updated or personal data removed, the old data is still available and can be retrieved.[4] The "Wayback Machine" enables a user to search through over 150 billion web pages archived from the early days of the Internet in 1996 until only a few months before the search is conducted. Should one wish to retrieve information from the past 90 days or so, Google's "cached" page function takes over.[5] The result is that anything which has been on the Internet can often still be found, enabling the searching for information not only across geographic space but also across time. These searches can synchronize raw data as well as pictorial information; they archive public (government) as well as private (personal) web postings. Data posted on YouTube, Facebook, MySpace, or other social media sites are readily searchable if such information is made public. As mentioned above, the pictorial data can be fused to create three-dimensional images that can be viewed across the fourth dimension: time.[6] With well over 100 billion pictures already on the Internet, more than 1 trillion video downloads on YouTube, and several billion more pictures and videos being posted each month, the Internet is morphing into a window to our world that allows us to see anywhere at almost any time.[7] In short the technological developments are moving us toward transparency.

As this enormous data set becomes available on the Internet, new innovations will be necessary to use it. As mentioned above, nascent versions of some of the necessary algorithms already exist. Photosynth, a readily available Microsoft program, can fuse pictorial data, as most cell phones now tag the photos with a geographical and chronological stamp. Other algorithms are able to examine patterns of human behavior and flag for analysis those activities that are not like the others. Such algorithms can be useful for enabling business to foresee the next major consumer product or for enhancing security. One such set of algorithms has been developed as part of the Risk Assessment and Horizons Scanning system in Singapore. That city-state has developed an analyst-intensive process that involves environmental scanning for data, provides indicators of possible activity, enables the conduct of sentiment analysis, and helps with data fusion and analysis that leads to scenario development and the development of strategies. This system, first put in place in 2004, has undergone several upgrades since its inception. While not fully automated, the system provides "insights to emerging risks and opportunities with national security implications."[8]

With a world of data available and the algorithms to flag events that may be indicators of risks, proper command and control can ensure that risks are properly assessed. Here the Air Force's global command and control capability becomes the last element of a new transparency system. As data suggest that a risk may be emerging in a part of the world, the command and information exchange systems—in conjunction with well-trained leadership—enable the analysis, further research, and assessment of the risks as they emerge.

The vision for how the transparency system would potentially operate is depicted in figure 14. The concept begins with the fusing of several streams of data. Intelligence data gathered through satellites, reconnaissance platforms, and other routine methods constitute the intelligence stream. The public data are published by news media, publishing houses, or governmental agencies that seek to make information available to the world. The "private" data may be a slight misnomer because this includes information on the Internet that is publically accessible, including public personal profiles that can be found in such places as Facebook or MySpace. Most users of these sites allow certain aspects of their profiles to be viewed by people not yet on their list of "friends."

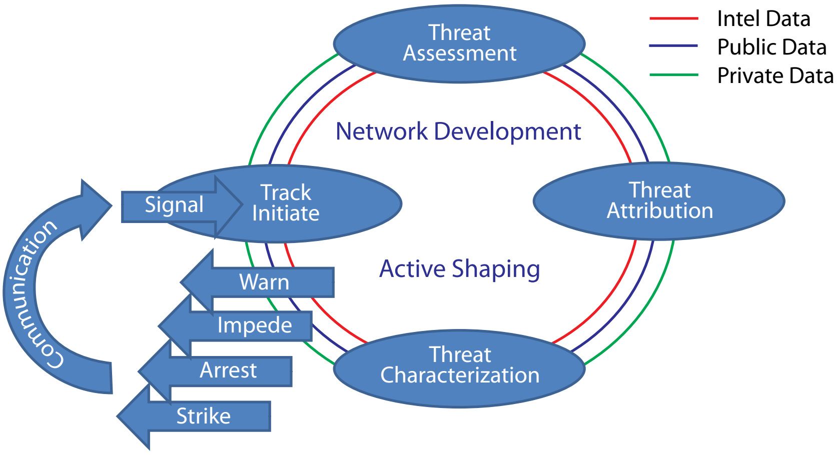


Figure 14. How transparency operates

These data are fused and processed using advanced algorithms that build on work already done. These algorithms will be designed to highlight or flag unusual patterns of behavior worthy of human analysis. Upon seeing such a signal, the analyst initiates tracking. The analyst drills into the data to determine if there is a concern that rises to the level of being a threat to US facilities or interests. If such a threat exists, then the analyst does additional analytical work with the data to attribute this threat to a specific actor or set of actors and then characterize that threat, including identifying its capabilities, operating procedures, and location. At that point, the government has many options available to deter a potential adversary. Depending on the nature of the threat and how early in the planning process an attack has been identified, the options may range from merely warning the individuals that they have already been discovered to potentially arresting or striking them if the threat they pose is more imminent. As these actions are taken, ripples or perturbations in the networks associated with these actors will likely appear within one or more of the streams of data. Additional fusing of data and repeating the above process will also flag other potentially dangerous actors associated with the initially discovered adversary for further analysis. Iterating this process will soon make obvious to actors who seek to hurt the United States that their likelihood of success has decreased, shifting the deterrence calculus in our favor.

It is important to realize that this process leverages things the Air Force has historically done well. It is a leader in technology and has an entire laboratory directorate devoted to the creation of new sensor technologies.[9] The Air Force was and remains the service responsible for reconnaissance and information gathering, and it has developed computerized operations centers where the fusion of these data can take place. In short the creation of transparency is an extension of extant Air Force missions, and the Air Force can and should lead in these areas.

From this proposed operational concept, this study concludes that transparency should be thought of as a second pillar of deterrence. From an Air Force standpoint, it has benefits very similar to those of air superiority in that it facilitates both attack and defense. More importantly to this analysis, transparency has a deterrent quality all its own. It is important to understand that transparency is about knowledge rather than control.

Along with the ability to strike globally, transparency has the potential to radically alter adversaries' deterrence calculus. If they believe that their actions will likely be discovered and attributed and that the punishment from the United States for an attempt to conduct catastrophic or destructive attacks on US interests will be severe, then the deterrence calculus shifts in favor of the attack being deterred. As a result of the development and proliferation of technologies that can create catastrophic effects over the next 10–20 years, this study concludes that by 2030, transparency and the associated concept of attribution will be essential. Moreover, as a requirement it will drive defense-procurement spending.

To fully realize the potential of how transparency can assist in deterring future adversaries, the Air Force must address a coherent vision, scientific research and development, further development of concepts of operations, and potential organizational changes. The study participants believe that as the service that established the terms of reference for the use of cyberspace, the Air Force is better prepared to lead these efforts than our sister services. Time is short, so it is important that we do so now.

Unfortunately, transparency is a two-way street, and by itself it does not fully address all the aspects of deterrence by denial. It is likely that adversaries will have some level of transparency versus the United States. The study team pulled the picture in figure 15 from the Internet while the aircraft depicted were still in these parking spaces at Al Udeid Air Base in Qatar. At one end of the ramp are fully loaded B-1 aircraft. Had these weapons been detonated by an attack on the base, the other aircraft on the flight line—which included roughly one-fourth of the Air Force's entire Airborne Warning and Control System and airborne command fleets—would have been destroyed. Notice that all the data needed to carry out an attack, including the target elevation and coordinates, were readily available.

As a result of this transparency, we need a set of means to deny potential adversaries a chance to succeed, even when our forces or infrastructure is in known locations. As Bob Pape argues, one must attack a potential adversary's strategy.[10] In short we need to deny success. To do this, the research team argues, we need a second concept called "immunization" as well.

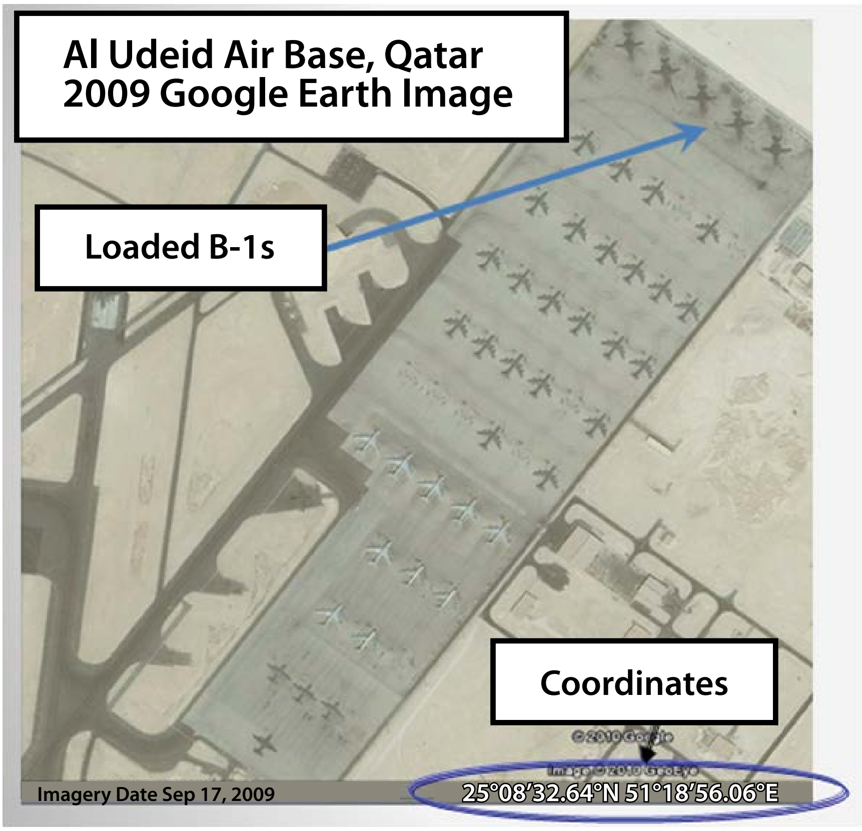


Figure 15. Al Udeid Air Base, Qatar, on 17 September 2009. (The authors discovered the picture on the Internet using Google's GeoEye in early 2010. The aircraft were still based at Al Udeid when the picture was found.)

Immunization

As it applies to the United States, immunization is analogous to an individual getting the annual influenza vaccine. It is a protective measure that reduces an attack's effectiveness. Properly immunized against the flu, one can be coughed upon all winter long and not feel any adverse effects. Similarly, a nation-state properly immunized against attack will not suffer significant damage, even if an attack is launched against it.

For nation-states like the United States, this immunization process involves implementing physical safeguards around pieces of critical infrastructure that would protect them in the event of an attack. This involves creating backup methods of operation and functional resilience that result in little or no denigration to operations should an attack happen, creating strategies that enable the flexible selection of options to mitigate the effects of an attack. It also results in the development of cognitive resilience within the populace and the military, creating a mind-set in which, even if an attack occurs, there is not a disproportionate psychological reaction to the strike.

As threats become more numerous and span increasingly large technological sets, immunization will require time, resources, and practice to attain. The methods of immunizing computer systems will be different than those of immunizing the populace against a biological pathogen. Nonetheless, the country must be prepared to do both as well as secure its interests from attacks of other types. If we can achieve a level of immunization that minimizes the gains realized by attacking the United States and its interests abroad, then the deterrence calculus shifts in favor of the defender, and the nation becomes more secure.

To insure that immunization actions are considered in that calculus, demonstrations of these capabilities will likely be required. It is important to note that deterrence by denial is not new. It has been a part of deterrence theory for over 50 years, but it is more important now than it has been in the past. In short, we are entering a world where the proliferation and cheapening of potentially harmful technologies will impose costs on those nation-states that value protecting their populace.

As such, there are several implications for the Air Force. For instance, immunization will require people and materiel. It is not free. The Air Force has experience with hardening facilities from attack by several of these weapon types, and in many cases the methods of hardening against traditional attacks will work for the new threats.

The panoply of new threats increases the requirements for the services to work together to create effective immunization and resilience. As we do this, we need to understand not only who is theoretically responsible for certain mission sets but also who is really going to accomplish them. For example, the US Army is required to defend US Air Force bases from guided rockets, artillery, mortars, and munitions. Yet, when the survey team conducted interviews with several senior US Army leaders and programmers regarding the steps the Army is taking to accomplish this task, they found little action being taken. For the Air Force, this means that making the assumption that the bases will be defended may carry with it serious risk.

These interdependences and risks, some of which have not been assessed, may force the reexamination of how the US Air Force presents forces. The current expeditionary method of operations using canvas as a protective material for personnel, command centers, computer systems, and operations centers is and will be ineffective. The range of threats emerging in the future is such that mere canvas as a protective layer will almost certainly be insufficient for the task. The Air Force will need to consider threats to its bases, logistics, and communications; moreover, it will need to examine new technologies and methods to shield aircraft, command centers, and personnel from attacks that may range from conventional guided munitions to electronic or pulsed electromagnetic attack. It will need to explore new and existing technologies to provide resiliency to aircraft, airfields, command and control facilities, and base infrastructure after attacks. Further, these same protection and resiliency considerations need to be extended to our assets in space.

As the team looked across the implications of these future threats, it was acutely aware that these considerations challenge the myopia that has been allowed to permeate the Department of Defense over the last decade. Today the United States remains focused on unconventional conflict as a result of having spent the last 20 years involved in wars in the Middle East. While Pres. Barack Obama has announced timelines for handing over the region to the indigenous governments, these timelines are ill defined and may stretch across a number of years.

While it is perfectly appropriate for war fighters to concentrate on the battle they are currently fighting, the consequence of this concentration is that America's military has been strictly focused on unconventional warfare in developing nations for a generation and will remain focused on this mission, at least in part, for several more years. While the threats in this study may come from terrorists, what is necessary to defeat this threat bears little resemblance to the types of combat in which we are now engaged—and we are not ready. Further, technology is changing at such a pace that those who fail to make a concerted effort to stay abreast of new developments find their thinking quickly rendered obsolete. The scope of the threats that we may face from the previously mentioned technologies is disturbing.

The good news is that some of the Air Force's greatest strengths have been a tradition of looking ahead, challenging current strategic assumptions, and embracing new technologies. This type of thinking is critical to the Air Force. Although the latter is not a named "core competency," the Air Force and its predecessor, the Army Air Corps, have foreseen where technology was leading and what the next new strategic leaps would be.

Recommendations

Based on the above research and findings, the study team has two sets of recommendations for the Air Force as it moves toward the 2030s. They deal with the development of a global vigilance strategy and the assessment and addressing of the Air Force's immunization needs. Properly addressing these two broad areas will make attacks easier to attribute, adversary opportunities easier to deny, and adversary success harder to achieve. Collectively these tilt the deterrence calculus in favor of the United States, making it much less likely that the adverse and severe consequences of the threats discussed above will ever have to be endured.

Notes

1. Franklin D. Margiotta, ed., “Artillery,” in *Brassey’s Encyclopedia of Land Forces and Warfare* (Washington, DC: Brassey’s, 1996), 99.

2. Today this is considered a subset of “information superiority” as one of the Air Force’s six distinctive capabilities. Department of the Air Force, “The Official Web Site of the U.S. Air Force,” 2012, accessed 22 May 2012, http://www.af.mil/main/welcome.asp.

3. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 117–21.

4. “Wayback Machine,” Internet Archive, n.d., accessed 24 April 2012, http://archive.org/web/web.php.

5. Nancy Blachman and Jerry Peek, “Cached Pages,” Google Guide, 28 December 2011, accessed 24 April 2012, http://www.googleguide.com/cached_pages.html.

6. Microsoft’s “Photosynth,” free of charge on the Internet, is one such program that enables this fusing. See Microsoft Corporation, “Photosynth,” n.d., accessed 22 May 2012, http://photosynth.net.

7. “Internet 2011 in Numbers,” *Pingdom* (blog), accessed 22 May 2012, http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/. In most cases, the numbers for 2011 were severalfold higher than the numbers for 2010.

8. Singapore is among the leaders in the development of this software. See Risk Assessment and Horizon Scanning (RAHS) Programme Office, Government of Singapore, “About Us: Vision, Mission & Values,” 13 January 2012, accessed 24 April 2012, http://app.rahs.gov.sg/public/www/content.aspx?sid=2951; and RAHS Programme Office, Government of Singapore, “Organisation Structure Website,” 30 March 2012, accessed 24 April 2012, http://app.rahs.gov.sg/public/www/home.aspx.

9. Air Force Research Laboratory, “Sensors Directorate,” n.d., accessed 22 May 2012, http://www.wpafb.af.mil/afrl/ry/.

10. Robert Anthony Pape, *Bombing to Win* (Ithaca, NY: Cornell University Press, 1996), 1–34.

Chapter 6

A Global Vigilance Strategy for 2035

To develop a global vigilance strategy for 2035, the Air Force must first reestablish itself as a leader in cyber warfare with increased research and development of equipment as well as increased training. This is essential to handling threats that emerge in cyberspace and echoes recommendations in the 2010 vector statement of Gen Norton Schwartz, former Air Force chief of staff.[1] The service, however, needs to broaden beyond mere electronic warfare and become a leader in the field of intelligence, surveillance, and reconnaissance. In these areas, the Air Force is the traditional lead service and should be again.

While the Air Force has made great strides in integrating remotely piloted aircraft (RPA) and space and cyberspace operations, this integration needs to move toward completion. Real-time sharing, fusing, and cross-cueing from information in each of these realms must be achieved.

As General Schwartz recommended in July 2010, the study also found and recommended that the Title 10 Futures Wargames should focus on vetting new technologies, innovative ideas, and future concepts of operations and finding novel ways to institutionally integrate RPAs, space, cyberspace, and real-time data fusion into new ways of conducting business. This creates a prerequisite that all Title 10 Futures Wargames be fully and completely staffed and run by visionary leaders who are knowledgeable about emerging technologies and their potential capabilities. This will involve much more careful selection of game players and senior mentors than has been the case in the past. Only by ensuring that those creating, playing, and running the games are conversant in these technologies and their potential can one create the new concepts of operations that will be needed to propel the Air Force into the future.

As the global vigilance strategy is developed and unfolds over time, the Air Force should constantly reexamine its organizational structures to determine if or when changes are needed to optimize the integration of global vigilance into all facets of its operations. While reluctant to posit precisely what these changes may be, the study team unanimously believed that existing organizational structures would be inadequate to handle transparency at the necessary levels in the 2030 time frame and that the Air Force leadership would need to examine organizational structures as the transparency strategy evolved over time.

Lastly, the study team, upon its outbrief, recommended that an informal interagency study group be formed to define the capabilities, capacities, organization, authorities, and systems needed to fully enable transparency. As this study's details became more widely known and coordinated, the National Security Staff became aware of and began to work on some of the issues embedded in this report. Presidential Policy Directive 8 (PPD-8) is an outgrowth of the National Security Staff's efforts in these matters. As a result of PPD-8, an interagency group has already been formed and was slated to present its conclusions to the president in 2012. This study believes that interagency cooperation and coordination will be necessary to optimally use precious taxpayer-provided resources to achieve a global vigilance strategy for 2035.

Immunization

As previously mentioned, because potential adversaries in the future will have access to many of the same transparency-creating technologies that we will have, implementing the concept called "immunization" is necessary. To do this, one must have a full assessment of immunization needs and understand where the service is already taking grave risks.

Unfortunately, a full assessment of all the risks the Air Force is taking with regard to its basing, current and future adversary threat laydowns, shortfalls in other services' efforts (such as the lack of any funding for defense against guided rockets, artillery, mortars, and munitions), and interagency issues (such as the lack of protection for the national critical infrastructure) has never been done. This leaves the Air Force in a position where the problem set itself remains inadequately defined. Our recommendations, therefore, take a problem-solution format.

The first—and immediate—step is to fully define this problem. Several Air Force missions in the future will be at risk due to the variety of threats that potential adversaries will field and due to our own as well as other agencies' and services' underfunding of needed capabilities. Increased transparency will mean that the locations of our forces will be known to our adversaries. The technologies previously discussed will also be in their hands. This combination places our combat capability at grave risk and will reduce our ability to achieve surprise. In an era of precisely targeted conventional missile attacks, directed energy weaponry, and cyber-domain warfare, our doctrine of operating from bare bases in an expeditionary manner may put us at unacceptable risk in some theaters. Add potential biological attack and attacks to our communication and space assets, and one begins to paint a multidimensional trade space that has never been fully mapped. The Air Force needs to create and understand this risk map to make mission risk visible, based on our own funding outlays and those of other services, agencies, or allies upon which we depend.

Only when this risk analysis is complete can we target research and development in the laboratory system to address the key vulnerabilities. Research and development to improve our ability to harden combat systems, personnel deployment locations, and support infrastructure will be needed to ensure that the Air Force is able to survive to operate in future combat environments. This research will likely need to target new material science and communications technologies to deny adversaries the ability to disable the Air Force.

Only by creating an Air Force that is capable of operating without significant degradation in the face of a potential adversary's attack can we deny him success. If we are able to achieve this level of immunization, then an adversary's gains to be won by attacking become so trivial that a rational actor will choose not to strike in the first place. This is part of how deterrence succeeds.

Issues for Other Departments

Because of the breadth of challenges that will confront the United States in the 2030s, this is much more than a Department of Defense problem. There are issues for the Departments of Homeland Security (DHS), Transportation, Health and Human Services, and Commerce, as a minimum. There are likely others this study has not stumbled upon as well.

The DHS is responsible for the defense of our national infrastructure and air transport system. Consequently it needs to understand the potential impact that directed energy will have on our electrical and banking systems.

Not to be forgotten is that while adversaries can be deterred, our sun cannot. The good news is that when the sun attacks (e.g., with solar flares), it gives warning, and the protection of the national infrastructure with warning is a rather trivial problem, assuming a plan is in place to do it.[2] Sadly, no such plan exists, and no agreed-upon threshold to take action in response to solar flares exists. While the Department of Commerce looks at weather effects and NASA looks at solar flares, there are no means by which their respective analyses are combined to make decisions on how to protect the utility systems upon which we all depend. Until there are, we will all remain at risk of a major flare destroying our electrical grid in a manner that could keep the lights out for years.

The DHS is also responsible for airline safety. Nanotechnological explosives will soon increase the potential for very small amounts of a substance to create very large explosions. While there is substantial public backlash against limitations such as the three-ounce-bottle limits on commercial aircraft, this problem is about to become 5- to 10-fold worse. The DHS will need to develop methods of detecting which compounds can explode and which cannot—and further, detect these when they may be chemically new materials or something just nanoengineered in an adversary's laboratory. The Department of Transportation has this same requirement but with respect to our major highways and bridges. The destruction of all bridges that cross the Missouri-Mississippi river system with nanoexplosives is something that must be guarded against as well.

The one potential extinction-level event discussed above is biological attack. The Blue Horizons III study recommended a major project to enable rapid detection and decoding of new genomic structures along with the ability to quickly prototype and produce vaccines. We stated then and reiterate now that a major project is needed on biogenetics to ready the nation and the world to rapidly respond to the outbreak of a novel virus, whether man-made or a natural mutation, within a matter of hours instead of the nearly one year it took to develop a vaccine for the H1N1 influenza in 2010. This study concludes that this recommendation remains valid and must be pursued. However, its implementation lies within the purview of the Centers for Disease Control and the National Institutes of Health.

In short the future technologies studied have the potential to threaten our lives, livelihoods, and infrastructure. Many aspects of protecting these do not lie in Title 10 and must be addressed by the responsible agencies. If they fail to do so, then our ability to deter an adversary by denial may exist within our Air Force but not within our nation as a whole. Deterrence is a team sport. It is one that all the federal agencies must play together.

Notes

[1] Norton A. Schwartz, "CSAF Vector 2010," 4 July 2010, accessed 24 May 2012, http://www.afa.org/grl/pdfs/CSAFVECTOR2010b.pdf.

[2] To protect transformers and generators from the electric currents generated inside power lines by a solar flare, one need only disconnect them from the grid—and need not do so elegantly. Power companies almost always have spare line; they almost never have spare transformers or generators. Thus, even quickly achieved and sloppy cuts to the lines can be repaired later.

Chapter 7

Summary

The Center for Strategy and Technology was asked to examine how the US Air Force could best deter attacks in space and cyberspace or attacks using biotechnology, nanotechnology, directed energy, and/or nuclear weapons. Looking toward the year 2035, CSAT discovered that these threats create a potentially dangerous future for the United States and many of our allies and partners around the world.

This study concludes that the threats in these six areas range from very dangerous to the potentially catastrophic, with the nexus between bio- and nanotechnologies holding the gravest risk of all. The study finds that little has been or is being done to protect American citizens or their infrastructure from these threats but also finds that technologies to mitigate these threats either already exist or can be developed with time.

It also finds that deterrence theory, as originally constructed, is still valid. The basic theory will hold in the future, but the way it must be applied will change. New technologies are susceptible to being deterred through denial not merely through retribution, as was the case with nuclear weapons during the cold war. As such, new strategies—specifically in the areas of transparency and immunization—are required.

In summary we have shown that deterrence is based on changing adversaries' assessments of whether the gains to be won from an attack outweigh the risks they incur. To do this, one can affect both sides of the deterrence equation by denying adversaries the opportunity and tools to initiate a successful attack, ensuring that the gains to be won are small, and punishing the attackers for the attack once it is launched. To achieve the capability to deter by denial and by punishment in the 2030s, the Air Force will need a new vision for global vigilance and a new strategy for immunization. To achieve the latter, we will need to map the risks that are inherent in our systems and doctrine and begin researching and developing work-arounds to mitigate these risks. If we do these things, then the adverse consequences and the likelihood of attack using modern conventional and nuclear systems in the 2030s can be significantly reduced, and the threats we fear most need never materialize.

Achieving this outcome requires cooperation across the whole of government. While the Air Force has an important role to play and will inevitably lead in some areas, it has neither the structure nor the mission to accomplish this task alone. Deterrence is a team sport, and every cabinet agency has a position to play on this team. Only when our nation acts in unity will it reach the common goal of deterring these new technologies.

Abbreviations

AU	Air University
COIL	chemical oxygen iodine laser
CSAF	Air Force chief of staff
CSAT	Center for Strategy and Technology
DHS	Department of Homeland Security
EMP	electromagnetic pulse phenomenon
F2T2EA	find, fix, track, target, engage, and assess
GPS	Global Positioning System
ISP	specific impulse
ISR	intelligence, surveillance, and reconnaissance
OODA	observe, orient, decide, and act
PPD	presidential policy directive
RPA	remotely piloted aircraft
S&P	Standard & Poor’s stock market index
SCADA	supervisory control and data acquisition
UN	United Nations

Bibliography

Articles

Bell, Trudy E., and Tony Phillips. "A Super Solar Flare." *NASA Science News*, 6 May 2008. http://science.nasa.gov/science-news/science-at-nasa/2008/06may_carringtonflare/.

Benea, Lidia, Pier Luigi Bonora, Alberto Borello, and Stefano Martelli. "Wear Corrosion Properties of Nano-Structured SiC-Nickel Composite Coatings Obtained by Electroplating." *Wear* 249, no. 10–11 (November 2001): 995–1003.

Bonham, G. Matthew, and Daniel Heradstveit. "Decision-Making in the Face of Uncertainty: Attributions of Norwegian and American Officials." *Journal of Peace Research* 23, no 4 (December 1986): 339–56.

Cole, John W., Isaac F. Silvera, and John P. Foote. "Conceptual Launch Vehicles Using Metallic Hydrogen Propellant." *American Institute of Physics Conference Proceedings* 969 (2008): 977–84.

Covault, Craig. "Chinese Test Anti-Satellite Weapon." *Aviation Week and Space Technology*, 17 January 2007. http://www.spaceref.com/news/viewnews.html?id=1188.

Dalkey, Norman, and Olaf Helmer. "An Experimental Application of the Delphi Method to the Use of Experts." *Management Science* 9, no. 3 (April 1963): 458–67.

Daly, P. "Navstar GPS and GLONASS: Global Satellite Navigation Systems." *Electronics and Communication Engineering Journal* 5, no. 6 (December 1993): 349–57.

Dayton, Leigh. "Solar Storms Halt Stock Market as Computers Crash." *New Scientist*, 9 September 1989, 35.

DiBella, Nicholas J. "First-Line Treatment of Chronic Myeloid Leukemia: Imatinib versus Nilotinib and Dasatinib." *Community Oncology* 8, no. 2 (February 2011): 65–72.

Grueber, Martin, and Tim Studt. "2012 Global R&D Funding Forecast." *R&D Magazine*, 16 December 2011. http://www.rdmag.com/articles/2011/12/2012-global-r-d-funding-forecast.

Huth, Paul, and Bruce Russett. "What Makes Deterrence Work? Cases from 1900–1989." *World Politics* 36, no. 4 (July 1984): 496–526.

Keller, John. "Megarad-Level Rad-Hard 64-Megabit Solid-State Memory Introduced by Honeywell for Military Satellites." *Military and Aerospace Magazine*, 10 December 2010. http://www.militaryaerospace.com/articles/2010/12/megarad-level-rad-hard.html.

Kelly, Harold H. "The Process of Causal Attribution." *American Psychology* 28, no. 2 (1973): 107–28.

Kendig, Martin, Melitta Hon, and Leslie Warren. " 'Smart' Corrosion Inhibiting Coating." *Progress in Organic Coatings* 47, no. 3 (September 2003): 183–89.

McHale, John. "Radiation-Hardened Electronics Technology Remains Stable amid Steady Demand in the Space Market." *Military and Aerospace Magazine*, 21 May 2010. http://www.militaryaerospace.com/articles/2010/05/radiation-hardened-electronics.html.

Meserve, Jeanne. "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid." *CNN.com*, 26 September 2007. http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US.

"Mouse Pox or Bioweapon?" *BBC World Service*, 17 January 2001. http://www.bbc.co.uk/worldservice/sci_tech/highlights/010117_mousepox.shtml.

Phillips, Tony. "Solar Shield—Protecting the North American Power Grid." *NASA Science News*, 26 October 2010. http://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield/.

Potter, Matthew. "Boeing Video of Advanced Tactical Laser (ATL) Aircraft." *Defense Procurement News*, 2 October 2009. http://www.defenseprocurementnews.com/2009/10/02/boeing-video-of-advanced-tactical-laser-atl-aircraft/.

Radhakrishnan, S., Giridhar Madras, Debajyoti Mahanta, Satish Patil, C. R. Siju. "Conducting Polyaniline-nano-TiO_2 Composites for Smart Corrosion Resistant Coatings." *Electrochimica Acta* 54, no. 4 (30 January 2009): 1249–54.

Ridley, Matt. "Humans: Why They Triumphed." *Wall Street Journal*, 22 May 2010. http://online.wsj.com/article/SB10001424052748703691804575254533386933138.html.

Russett, Bruce, and Allan C. Stam. "Courting Disaster: An Expanded NATO vs. Russia and China." *Political Science Quarterly* 113, no. 3 (Fall 1998): 361–82.

Slay, Jill, and Michael Miller. "Lessons Learned from the Maroochy Water Breach." *Critical Infrastructure Protection* 253 (November 2007): 73–82.

Thomas, Pierre. "Teen Hacker Faces Federal Charges." *CNN Interactive*, 18 March 1988. http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html.

Tversky, Amos, and Daniel Kahneman. "Judgment under Uncertainty: Heuristics and Biases." *Science* 185, no. 4157 (27 September 1974): 1124–31.

Vasylkiv, Oleg, Yoshio Sakka, and Valeriy V. Skorokhod. "Nano-Blast Synthesis of Nano-Size CeO_2-Gd_2O_3 Powders." *Journal of American Ceramic Society* 89, no. 6 (June 2006): 1822–26.

Yunzhu, Yao. "Chinese Nuclear Policy and the Future of Minimum Deterrence." *Pacific Forum CSIS* 6, no. 2 (September 2005): 31–40. http://csis.org/files/media/csis/pubs/issuesinsights_v06n02.pdf.

Books

Allison, Graham, and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. New York: Longman, 1999.

Anheier, Helmut, Marlies Glasius, and Mary Kaldor. "Introducing Global Civil Society." In *Global Civil Society 2001*, edited by Helmut Anheier, Marlies Glasius, and Mary Kaldor, 3–22. Oxford, UK: Oxford University Press, 2001.

Bains, William. *Biotechnology from A to Z*. New York: Oxford University Press, 2004.

Committee on the Societal and Economic Impacts of Severe Space Weather Events, Space Studies Board, National Research Council of the National Academies. *Severe Space Weather Events—Understanding Societal and Economic Impacts*. Washington, DC: National Academies Press, 2008.

Doyle, Michael W., and Stephen Macedo. *Striking First: Preemption and Prevention in International Conflict*. Princeton, NJ: Princeton University Press, 2008.

Eversole, Finley, ed. *Infinite Energy Technologies*. Rochester, VT: Inner Traditions, 2012.

Freedman, Lawrence. *Deterrence*. Malden, MA: Polity Press, 2004.

Friedman, Thomas L. *The World Is Flat: A Brief History of the Twenty-First Century*. New York: Farrar, Straus, and Giroux, 2007.

Gleick, James. *Chaos: Making of a New Science*. New York: Viking, 1987.

Goodpaster, Andrew J., C. Richard Nelson, and Seymour J. Deitchman. "Deterrence: An Overview." In *Post–Cold War Conflict Deterrence*, 10–38. Washington, DC: National Academies Press, 1997.

Gutkowski, Witold, and Tomasz A. Kowalewski. *Mechanics of the 21st Century: Proceedings of the 21st International Congress of Theoretical and Applied Mechanics, Warsaw, Poland, 15–21 August 2004*. Dordrecht, Netherlands: Springer, 2005.

Hall, Stores J. *Nanofuture: What's Next for Nanotechnology*. Amherst, NY: Prometheus, 2005.

Hallam, A., and P. B. Wignall. *Mass Extinctions and Their Aftermath*. Oxford, UK: Oxford University Press, 2002.

Janis, Irving L., and Leon Mann. *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment*. New York: Free Press, 1977.

Karami, Ali. "Pandemics and Its Consequences for the Future of Asia." In *Imagining Asia in 2030: Trends, Scenarios and Alternatives*, edited by Ajey Lele and Namrata Goswami, 153–65. New Delhi, India: Academic Foundation Press, 2011.

Kurzweil, Ray. *The Singularity Is Near*. New York: Penguin Books, 2005.

Layne, Christopher. "From Preponderance to Offshore Balancing." In *The Use of Force: Military Power and International Politics*, 7th ed, edited by Robert J. Art and Kenneth N. Waltz, 311–26. Lanham, MD: Rowman and Littlefield Publishers, 2009.

Levy, Jack S. "The Causes of War: A Review of Theories." In *Behavior, Society and Nuclear War*, edited by Philip E. Tetlock, Jo L. Husbands, Robert Jervis, Paul C. Stern, and Charles Tilly, 209–333. Vol. 1. New York: Oxford University Press, 1989.

Linstone, Harold A., and Murray Turoff. *The Delphi Method: Techniques and Applications*. University Heights: New Jersey Institute of Technology, 2002.

Mansfield, Edward D. *Power Trade and War*. Princeton, NJ: Princeton University Press, 1994.

Mearsheimer, John J. *Conventional Deterrence*. Ithaca, NY: Cornell University Press, 1985.

Nisbett, Richard, and Lee Ross. *Human Interference: Strategies and Shortcomings of Social Judgment*. Englewood Cliffs, NJ: Prentice Hall, 1980.

Organski, A. F. K., and Jacek Kugler. *The War Ledger*. Chicago, IL: University of Chicago Press, 1980.

Pape, Robert Anthony. *Bombing to Win*. Ithaca, NY: Cornell University Press, 1996.

Paul, T. V., Patrick M. Morgan, and James J. Wirtz, eds. *Complex Deterrence*. Chicago: University of Chicago Press, 2009.

Payne, Keith B. *The Fallacies of Cold War Deterrence*. Lexington: University Press of Kentucky, 2001.

———. *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-First Century*. Fairfax, VA: National Institute Press, 2008.

Pittock, A. B., T. P. Ackerman, P. J. Crutzen, M. C. MacCracken, C. S. Shapiro, and R. P. Turco. "Direct Effects of Nuclear Detonations." In *Environmental Consequences of Nuclear War*. Vol. 1, *Physical and Atmospheric Effects*, edited by A. Barrie Pittock, Mark Harwell, and T. C. Hutchinson, 1–23. New York: John Wiley and Sons, 1986.

Ridley, Matt. *The Rational Optimist: How Prosperity Evolves*. New York: HarperCollins, 2010.

Rogers, William D. "The Principles of Force, the Force of Principles." In *Right v. Might: International Law and the Use of Force*, edited by Louis Henkin, Stanley Hoffmann, Jeane J. Kirkpatrick, Allan Gerson, William D. Rogers, and David J. Scheffer, 95–108. New York: Council on Foreign Relations, 1991.

Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 1966.

Schwartz, Peter. *The Art of the Long View*. New York: Doubleday, 1991.

———. *Inevitable Surprises: Thinking Ahead in a Time of Turbulence*. New York: Gotham Books, 2003.

Shortley, George, and Dudley Williams. *Elements of Physics*. 5th ed. Englewood Cliffs, NJ: Prentice Hall, 1971.

Turing, Alan M. “Computing Machinery and Intelligence.” In *Parsing the Turing Test: Philosophical and Methodological Issues in the Quest for the Thinking Computer*, edited by Robert Epstein, Gary Roberts, and Grace Beber, 23–66. Dordrecht, Netherlands: Springer, 2008.

von Clausewitz, Carl. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1989.

Waltz, Kenneth N. “Nuclear Myths and Nuclear Realities.” In *The Use of Force: Military Power and International Politics*, edited by Robert J. Art and Kenneth N. Waltz, 102–18. 6th ed. Malden, MA: Rowman and Littlefield, 2004.

Woodward, Angela. “Biological and Chemical Terrorism.” In *Imagining Asia in 2030: Trends, Scenarios and Alternatives*, edited by Ajey Lele and Namrata Goswami, 323–35. New Delhi, India: Academic Foundation Press, 2011.

Hearings and Treaties

US Department of State. *Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, US-USSR*, 26 May 1972. http://www.state.gov/t/isn/trty/16332.htm.

US House of Representatives. *Electromagnetic Pulse Threats to U.S. Military and Civilian Infrastructure: Hearing before the Military Research and Development Subcommittee of the Committee on Armed Services*. 106th Cong., 1st sess., 7 October 1999. Prepared statement of Lowell Wood, member of director’s technical staff, Lawrence Livermore National Laboratory, 30–36.

Papers

Baird, Henry D., Steven D. Acenbrak, William J. Harding, Mark J. Hellstern, and Bruce M. Juselis. “Spacelift 2025: The Supporting Pillar for Space Superiority.” In *Air Force 2025*, 117–50. Vol 2. Maxwell AFB, AL: Air University Press, 1996.

Barnett, Thomas P. M. “Deterrence in the 21st Century.” In *Deterrence 2.0: Deterring Violent Non-State Actors in Cyberspace*, edited by Carl Hunt and Nancy Chesser, 25–31. US Strategic Command Global Innovation and Strategy Center, Washington, DC, 10 January 2008.

Briefing. John R. Boyd. Subject: A Discourse on Winning and Losing, 1987. http://dnipogo.org/john-r-boyd/.

Cain, Anthony C., ed. *Deterrence in the Twenty-First Century: Proceedings*. Maxwell AFB, AL: Air University Press, 2010.

Coates, Christopher. *The Air Force in SILICO: Computational Biology in 2025*. Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2007.

Courville, Shane. *Air Force and the Cyberpsace Mission: Defending the Air Force's Computer Network in the Future*. Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2007.

Danigole, Mark S. *Biofuels: An Alternative to U.S. Petroleum Dependency*. Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2007.

Diehl, William. *Continued Optical Sensor Operations in a Laser Environment*. Maxwell AFB, AL: Air War College, 2011.

Geis, John P., II. *Directed Energy Weapons on the Battlefield: A New Vision for 2025*. Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2003.

Geis, John P., II, Christopher J. Kinnan, Ted Hailes, Harry A. Foster, and David Blanks. *Blue Horizons II: Future Capabilities and Technologies for the Air Force in 2030*. Maxwell AFB, AL: Air University Press, 2009.

Geis, John P., II, Scott E. Caine, Edwin F. Donaldson, Blaine D. Holt, and Ralph A. Sandfry. *Discord or "Harmonious Society"? China in 2030*. Maxwell AFB, AL: Air University Press, 2011.

Geis, John P., II, Ted Hailes, and Grant Hammond. "Technology and the Comprehensive Approach: Part Problem, Part Solution." In *Capability Development in Support of Comprehensive Approaches: Transforming International Civil-Military Relations*, edited by Derrick Neal and Linton Wells, 69–86. Washington, DC: National Defense University Press, 2011.

Gourley, Bob. "Towards a Cyber Deterrent." Working paper. Cyber Conflict Studies Association. Vienna, VA, 29 May 2008. http://www.ctovision.com/cyber-deterrence-initiative.html.

Jovene, Vincent T. *Next Generation Nanotechnology Assembly Fabrication Methods: A Technology Forecast*. Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2008.

Kopp, Carlo. "The Electronmagnetic Bomb—A Weapon of Electrical Mass Destruction." *Air and Space Power Journal: Chronicles Online Journal,* 1996. http://www.airpower.au.af.mil/airchronicles/cc/apjemp.html.

Miller, Michael B. "How Tall of a Stack of Paper Would We Need to Print Out an Entire Human Genome?" Working paper. Division of Epidemiology and Community Health, University of Minnesota, 15 October 2005. http://bio4.us/biotrends/human_genome_height.html.

Moseley, T. Michael, *Blue Horizons 2007: Horizons 21 Study Report*. Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2007.

Tsang, Rose. "Cyberthreats, Vulnerabilities and Attacks on SCADA Networks." Working paper. University of California–Berkeley, 2009. http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf.

US Commodity Futures Trading Commission, US Securities and Exchange Commission. *Findings Regarding the Market Events of May 6, 2010: Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues*. Washington, DC: Securities and Exchange Commission, 30 September 2010. http://www.sec.gov/news/studies/2010/marketevents-report.pdf.

Yarbrough, Ancel. *The Impact of Nanotechnology Energetics on the Department of Defense by 2035*. Maxwell AFB, AL: Air War College, 2010.

Miscellaneous

Schwartz, Norton A. "CSAF Vector 2010," 4 July 2010. http://www.afa.org/grl/pdfs/CSAFVECTOR2010b.pdf.

Websites

Air Force Research Laboratory. "Sensors Directorate," n.d. http://www.wpafb.af.mil/afrl/ry/.

Human Genome Program, Office of Biological and Environmental Research, Department of Energy. "Human Genome Project Information," 31 July 2012. http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml.

Human Proteome Organisation (HUPO). "Human Proteome Project (HPP)." HUPO, 21 March 2012. http://www.hupo.org/research/hpp/.

Idaho National Laboratory, US Department of Energy. "Protecting the National Infrastructure: Idaho's Test Range." Fact sheet. Idaho Falls, ID: Idaho National Laboratory, n.d. http://www.inl.gov/nationalsecurity/factsheets/docs/critical_infrastructure_test_range.pdf.

Information Technology Associates. "Educational Score Performance—Country Rankings." *World Fact Book*, n.d. http://www.geographic.org/country_ranks/educational_score_performance_country_ranks_2009_oecd.html.

Intel Corporation. "The Evolution of a Revolution." *Intel Developer Forum*, n.d. http://download.intel.com/pressroom/kits/IntelProcessorHistory.pdf.

"Internet 2011 in Numbers." *Pingdom* (blog), n.d. http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/.

Internet Systems Consortium. "Internet Host Count History," n.d. http://www.isc.org/solutions/survey/history.

Kurzweil, Ray. "The Significance of Watson." *Kurzweil Accelerating Intelligence* (blog), 13 February 2011. http://www.kurzweilai.net/the-significance-of-watson.

National Coordination Office for Space-Based Positioning, Navigation, and Timing (NCO). "GPS Applications," 10 April 10 2012. http://www.gps.gov/applications/.

National Environmental Satellite, Data, and Information Service (NESDIS). “NOAA’s Geostationary and Polar-Orbiting Weather Satellites.” *NOAA Satellite Information System*, 6 December 2011. http://noaasis.noaa.gov/NOAASIS/ml/genlsatl.html.

Petersen, John L. “Punctuations.” *FUTUREdition* (blog), 15, no. 8 (30 April 2012). http://www.futuredition.org/?m=201105.

Risk Assessment and Horizon Scanning (RAHS) Programme Office, Government of Singapore. “Organisation Structure Website,” 30 March 2012. http://app.rahs.gov.sg/public/www/home.aspx.

———. “Our Processes,” 13 January 2012. http://app.rahs.gov.sg/public/www/content.aspx?sid=2954.

Union of Concerned Scientists. “Nuclear Weapons & Global Security: History of Russia’s Anti-Ballistic Missile System,” 2012. http://www.ucsusa.org/nuclear_weapons_and_global_security/missile_defense/policy_issues history-of-russias.html.

Center for Strategy and Technology

The Center for Strategy and Technology (CSAT) was established at the Air War College in 1996. Its purpose is to engage in long-term strategic thinking about technology and its implications for US national security.

CSAT focuses on education, research, and publications that support the integration of technology into national strategy and policy. Its charter is to support faculty and student research; publish research through books, articles, and occasional papers; fund a regular program of guest speakers; and engage with collaborative research with US and international academic institutions. As an outside funded activity, CSAT enjoys the support of institutions in the strategic, scientific, and technological communities.

Essential to this program is establishing relationships with organizations in the Air Force and other Department of Defense agencies and identifying potential topics for research projects. Research conducted under the auspices of CSAT is published as Occasional Papers and disseminated to senior military and political officials, think tanks, educational institutions, and other interested parties. Through these publications, CSAT hopes to promote the integration of technology and strategy in support of US national security objectives.

For further information on the Center for Strategy and Technology, please contact

Col Thomas D. "T-Mac" McCarthy, Director
Harry A. Foster, Deputy Director
Theodore C. Hailes, Chair for Force Transformation, Air University
Grant T. Hammond, Deputy Director, Global Strike
George J. Stein, Deputy Director, Cyberspace & Information Operations
Lt Col Christopher A. Bohn, Chief Scientist

Air War College
325 Chennault Circle
Maxwell Air Force Base, Alabama 36112
(334) 953-6996/6460/2985

Titles in the Occasional Paper Series

1
Reachback Operations for Air Campaign Planning and Execution
Scott M. Britten, September 1997

2
Lasers in Space: Technological Options for Enhancing US Military Capabilities
Mark E. Rogers, November 1997

3
Non-Lethal Technologies: Implications for Military Strategy
Joseph Siniscalchi, March 1998

4
Perils of Reasoning by Historical Analogy: Munich, Vietnam and the American Use of Force since 1945
Jeffrey Record, March 1998

5
Lasers and Missile Defense: New Concepts for Space-Based and Ground Based Laser Weapons
William H. Possel, July 1998

6
Weaponization of Space: Understanding Strategic and Technological Inevitabilities
Thomas D. Bell, January 1999

7
Legal Constraints on Information Warfare
Mark Russell Shulman, March 1999

8
Serbia and Vietnam: A Preliminary Comparison of U.S. Decisions to Use Force
Jeffrey Record, May 1999

9
Airborne and Space-Based Lasers: An Analysis of Technological and Operational Compatibility
Kenneth W. Barker, June 1999

10
Directed Energy and Fleet Defense: Implications for Naval Warfare
William J. McCarthy, May 2000

11
High Power Microwaves: Strategic and Operational Implications for Warfare
Eileen M. Walling, May 2000

12
Reusable Launch Vehicles and Space Operations
John E. Ward Jr., May 2000

13
Cruise Missiles and Modern War: Strategic and Technological Implications
David J. Nicholls, May 2000

14
Deeply Buried Facilities: Implications for Military Operations
Eric M. Sepp, May 2000

15
Technology and Command: Implications for Military Operations in the Twenty-First Century
William B. McClure, July 2000

16
Unmanned Aerial Vehicles: Implications for Military Operations
David Glade, July 2000

17
Computer Networks and Information Warfare: Implications for Military Operations
David J. Gruber, July 2000

18
Failed States and Casualty Phobia: Implications for Force Structure and Technology Choices
Jeffrey Record, October 2000

19
War as We Knew It: The Real Revolution in Military Affairs/Understanding Paralysis in Military Operations
Jan S. Breemer, December 2000

20
Using Lasers in Space: Laser Orbital Debris Removed and Asteroid Deflection
Johanthon W. Dampbell, December 2000

21
Weapons for Strategic Effect: How Important Is Technology?
Collin S. Gray, January 2001

22
U.S. Army Apache Helicopters and U.S. Air Force Expeditionary Forces: Implications for Halting Military Operations
Brad Mason, June 2001

23
The End of Secrecy? Military Competitiveness in the Age of Transparency
Beth M. Kasper, August 2001

24
Space-Based Global Strike: Understanding Strategic and Military Implications
Larry G. Sills, August 2001

25
Precision Engagement at the Strategic Level of War: Guiding Promise or Wishful Thinking
Timothy J. Sakulich, December 2001

26
Infrared Systems for Tactical Aviation: An Evolution in Military Affairs?
George B. Hept, January 2002

27
Unmanned Undersea Vehicles and Guided Missile Submarines: Technological and Operational Synergies
Edward A. Johnson Jr., February 2002

28
Attack Operations for Missile Defense
Merrick E. Krause, May 2002

29
Death by a Thousand Cuts: Micro-Air Vehicles in the Service of Air Force Missions
Arthur F. Huber II, July 2002

30
Sustained Space Superiority: A National Strategy for the United States
Larry J. Schaefer, August 2002

31
Hyperspectral Imagery: Warfighting through a Different Set of Eyes
Paul J. Pabich, October 2002

32
Directed Energy Weapons on the Battlefield: A New Vision for 2025
John P. Geis II, April 2003

33
Homeland Security and the Coast Guard: Postured for Technology Improvements
Arthur C. Walsh, June 2003

34
Non-Lethal Weapons: Setting our Phasers on Stun? Potential Strategic Blessings and Curses of Non-Lethal Weapons on the Battlefield
Erik L. Nutley, August 2003

35
Aircrew Performance Cutting-Edge Tech
Kris M. Belland, September 2003

36
Centralized Control with Decentralized Execution: Never Divide the Fleet?
Daniel F. Baltrusaitis, June 2004

37
The Decision Maker's Guide to Robust, Reliable and Inexpensive Access to Space
Gary N. Henry, July 2004

38
Global Mobility: Anywhere, Anytime, Any Threat? Countering the MANPADS Challenge
Jacqueline D. van Ovost, December 2005

39
Strategies for Defeating Commercial Imagery Systems
Stephen Latchford, December 2005

40–51
Netted Bugs and Bombs: Implications for 2010
Edited by Marsha J. Kwolek. December 2005

Part I: Network Centric Operations: Promises and Pitfalls

Network Warfare Operations: Unleashing the Potential
Richard A. Lipsey

Network-Centric Operations: Challenges and Pitfalls
Eric E. Silbaugh

Network-Enable Precision Guided Munitions
Benjamin F. Koudelka Jr.

Lowering the High Ground: Using Near-Space Vehicles for Persistent C3ISR
Andrew J. Knoedler

Part II: UAVs in 2010: Lean and Lethal

Unmanned Combat Aerial Vehicles: SEAD and EW for the Future
James C. Horton

Small Power: The Role of Micro and Small UAVs in the Future
James M. Abatti

Pesky Critters
Kirk M. Kloepple

Pandora's Box Opened Wide: UAVs Carrying Genetic Weapons
Daryl J. Hauck

Part III: Silver Bullets in Search of a Six Shooter

Perfecting War: Searching for the Silver Bullet
Eric J. Schnitzer

Who Pushes the Pickle Button?
John E. Marselus

Leveraging Simulation against the F-16 Flying Training Gap
Shaun R. McGrath

Electronic Pulse Threats in 2010
Colin R. Miller

52
Ground Truth: The Implications of Joint Interdependence for Air and Ground Operations
L. Ross Roberts, March 2006

53
"Heads, Not Tails": How To Best Engage Theater Ballistic Missiles?
Ronald C. Wiegand, February 2006

54
Transcendental Terrorism and Dirty Bombs: Radiological Weapons Threat Revisited
Chad Brown, February 2006

55
International Armament Cooperative Programs: Benefits, Liabilities, and Self-inflicted Wounds—the JSF as a Case Study
Stephen G. DiDomenico, February 2006

56
War without Oil: A Catalyst for True Transformation
Michael J. Hornitschek, May 2006

57–59
Streamlining DOD Acquisition: Balancing Schedule with Complexity
Edited by James Rothenflue and Marsha J. Kwolek, September 2006

A System as the Enemy: A Doctrinal Approach to Defense Force Modernization
Benjamin A. Drew

Impact of Weapons Systems Complexity on Systems Acquisition
Robert A. Dietrick

Faster Is Better . . . Can the USAF Acquisition Process be SAIV'D?
James L. Chittenden

60
The Seductive Effects of an Expeditionary Mindset
Michael Arnold, February 2007

61
The Air Force in SILICO—Computational Biology in 2025
Christopher Coates, November 2007

62
Biofuels: An Alternative to U.S. Air Force Petroleum Dependency
Mark S. Danigole, December 2007

63
Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future
Shane P. Courville, December 2007

64
Next Generation Nanotechnology Assembly Fabrication Methods: A Trend Forecast
Vincent T. Jovene Jr., January 2008

65
Blue Horizons II: Future Capabilities and Technologies for the Air Force in 2030
John P. Geis II, Christopher J. Kinnan, Ted Hailes, Harry A. Foster, and David Blanks, July 2009

66
Resurgent Russia in 2030: Challenge for the USAF
Theodore C. Hailes, Ronald Buckley, David Blanks, Mark Butler, Phillip Preen, and Michael Tarlton, September 2009

67
Failed State 2030: Nigeria—A Case Study
Christopher J. Kinnan, Daniel B. Gordon, Mark D. DeLong, Douglas W. Jaquish, and Robert S. McAllum, February 2011

68
Discord or "Harmonious Society"? China in 2030
John P. Geis II, Scott E. Caine, Edwin F. Donaldson, Blaine D. Holt, and Ralph A. Sandfry, February 2011

69
Finding the Shape of Space
Christopher C. Shannon, Scott J. Scheppers, Dustin P. Ziegler, Brian C. McDonald, David Suh Hoon Menke, John P. Geis II, Amanda S. Birch, and Tosha N. Meridith, July 2011

AIR UNIVERSITY
THE INTELLECTUAL AND LEADERSHIP CENTER OF THE AIR FORCE

The Occasional Papers
series was established by the
Center for Strategy and Technology
as a forum for research
on topics that reflect
long-term strategic thinking
about technology and its
implications for
US national security.

Center for Strategy and Technology
Air War College
Maxwell Air Force Base
Montgomery, AL 36112

AFRI AU PRESS
AIR FORCE RESEARCH INSTITUTE

http://aupress.au.af.mil

ISBN 978-1-58566-231-9