

DEFENSE THREAT REDUCTION AGENCY Scientific & Technical Review Information

PA CONTROL NUMBER:

6 June PA 11-291

SUSPENSE: 23 June 2011

PM / PHONE / EMAIL:

Nicole Whealen 703.767.6354

DATE: 23 May 2011

BRANCH CHIEF / PHONE / EMAIL:

DIVISION CHIEF / PHONE:

DIRECTORATE / DIRECTOR / PHONE Bill Hostyn 703.767.4453

ENTERPRISE / OFFICE / PHONE:

PUBLIC AFFAIRS:

Richard M. Cole (Chief, PA) / J. Caines

DATE: 3 June 11
DATE: 6/13/11

1. TITLE: Revolutions in Science & Technology: Future Threats to US National

CONTRACT NUMBER

ORIGINATOR Boyd, Dallas; Algert, Dave

2. TYPE OF MATERIAL: ☒ PAPER ☐ PRESENTATION ☐ ABSTRACT ☐ OTHER

3. OVERALL CLASSIFICATION: ☒ CONTRACTOR UNCLASS ☒ PROJECT MANAGER UNCLASS

A. Review authority for unclassified material is the responsibility of the PM. Your signature indicates the material has undergone technical and security review.

B. Warning Notices/Caveats: ☐ RD ☐ FRD ☐ CNWDI ☐ NATO RELEASABLE
☐ SUBJECT TO EXPORT CONTROL LAWS

C. Distribution Statement:

☒ A. Approved for public release; distribution is unlimited (unclassified papers only).

☐ B. Distribution authorized to U.S. Government agencies only; (check the following):

☐ Contractor Performance Evaluation
☐ Foreign Government Information
☐ Administrative or Operational Use
☐ Specific Authority
☐ Premature Dissemination

☐ Proprietary Information
☐ Test and Evaluation
☐ Software Documentation
☐ Critical Technology

CLEARED
for public release

JUN 13 2011

PA Opns
Defense Threat Reduction Agency

☐ C. Distribution authorized to U.S. Government agencies and their contractors: (check the following):

☐ Critical Technology
☐ Specific Authority
☐ Administrative or Operational Use

☐ Software Documentation
☐ Foreign Government Information

☐ D. Distribution authorized to the Department of Defense and U.S. DoD Contractors only; (check the following):

☐ Foreign Government Information
☐ Critical Technology
☐ Administrative or Operational Use

☐ Software Documentation
☐ Foreign Government Information

☐ E. Distribution authorized to DoD Components only; (check the following):

☐ Administrative or Operational Use
☐ Premature Dissemination
☐ Critical Technology
☐ Foreign Government Information
☐ Direct Military Support

☐ Software Documentation
☐ Specific Authority
☐ Proprietary Information
☐ Test and Evaluation
☐ Contractor Performance Evaluation

☐ F. Further dissemination only as directed.

☐ X. Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25 (unclassified papers only).

4. MATERIAL TO BE: ☐ Presented ☐ Published Date Required:

Name of Conference or Journal:

Remarks: To be published on the ASCO website and distributed as needed.

DEFENSE THREAT REDUCTION AGENCY
Scientific & Technical Review Information

Remarks Cont:

Revolutions in Science and Technology: Future Threats to U.S. National Security

Project Manager:

Dallas Boyd
SAIC

April 2011

[This report is the product of a collaboration between the Defense Threat Reduction Agency's Advanced Systems and Concepts Office and Science Applications International Corporation, SAIC

The views expressed herein are those of the authors and do not necessarily reflect the official policy or position of the Defense Threat Reduction Agency, the Department of Defense, or the United States Government.

****[Pending Distro statement]**



**Defense Threat Reduction Agency
Advanced Systems and Concepts Office**

Report Number ASCO 2011 014

Contract/MIPR Number DTRA01-03-D-0017

Project Cost: \$180,000

The mission of the Defense Threat Reduction Agency (DTRA) is to safeguard America and its allies from weapons of mass destruction (chemical, biological, radiological, nuclear, and high explosives) by providing capabilities to reduce, eliminate, and counter the threat, and mitigate its effects.

The Advanced Systems and Concepts Office (ASCO) supports this mission by providing long-term rolling horizon perspectives to help DTRA leadership identify, plan, and persuasively communicate what is needed in the near term to achieve the longer-term goals inherent in the agency's mission.

ASCO also emphasizes the identification, integration, and further development of leading strategic thinking and analysis on the most intractable problems related to combating weapons of mass destruction.

For further information on this project, or on ASCO's broader research program, please contact:

Defense Threat Reduction Agency
Advanced Systems and Concepts Office
8725 John J. Kingman Road
Ft. Belvoir, VA 22060-6201

ASCOInfo@dtra.mil

2011 0121

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
The public reporting burden for this 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 the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 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 any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE		3. DATES COVERED (From - To)	
12-04-2011		Research		October 2010 - April 2011	
4. TITLE AND SUBTITLE Revolutions in Science and Technology: Future Threats to U.S. National Security			5a. CONTRACT NUMBER		
			DTRA01-03-D-0017		
			5b. GRANT NUMBER		
			N/A		
			5c. PROGRAM ELEMENT NUMBER		
			N/A		
6. AUTHOR(S) Dallas Boyd Lisa Andivahis Jeffrey R. Cooper Stephen J. Lukasik Victor Oancea George W. Ullrich			5d. PROJECT NUMBER		
			N/A		
			5e. TASK NUMBER		
			TI 53-10-02		
			5f. WORK UNIT NUMBER		
			N/A		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)				8. PERFORMING ORGANIZATION REPORT NUMBER	
Science Applications International Corporation 1710 SAIC Drive McLean, Virginia 22102				N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Threat Reduction Agency Advanced Systems and Concepts Office 8725 John J. Kingman Road Ft. Belvoir, Virginia 22060				10. SPONSOR/MONITOR'S ACRONYM(S)	
				DTRA/ASCO	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
				ASCO 2011-006	
12. DISTRIBUTION/AVAILABILITY STATEMENT					
Distribution A: Approved for public release; distribution is unlimited					
13. SUPPLEMENTARY NOTES					
None					
14. ABSTRACT					
The accompanying report provides a framework for evaluating S&T developments through the lens of their national security implications. This framework allows analysts to assess postulated technologies using a multi-tiered filtering process. The process consists first of a determination of whether the technology qualifies as a "weapon of mass effect," a term for which a new definition is provided. The next step assesses whether the technology possesses various qualities that would make it particularly consequential. These include: reduced barriers to acquisition; system integration; novel delivery means; self-propagation; novel radical empowerment; mitigation of effects; and diverse applicability. To illustrate the framework, the report examines eight technologies/capabilities that were identified as potential WME: ultrafast laser technology; genetically-engineered pathogens; advanced laser isotope separation; electromagnetic interference micro-jammers; botnet technology; circuit board hacking; quantum computing; and "E-bombs." The analysis of these technologies identifies the factors that may drive or inhibit their development, as well as the drivers/counter-drivers that influence their attractiveness from an adversary's perspective.					
15. SUBJECT TERMS					
S&T, R&D, technology, WME, WMD, terrorism, ultrafast lasers, bioweapons, electromagnetic pulse, laser isotope separation, EMI micro-jammers, botnets, circuit board hacking, quantum computing, E-bombs.					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			David Algert
UNCLASS	UNCLASS	UNCLASS	SAR	166	19b. TELEPHONE NUMBER (Include area code)
					(703) 767-5704

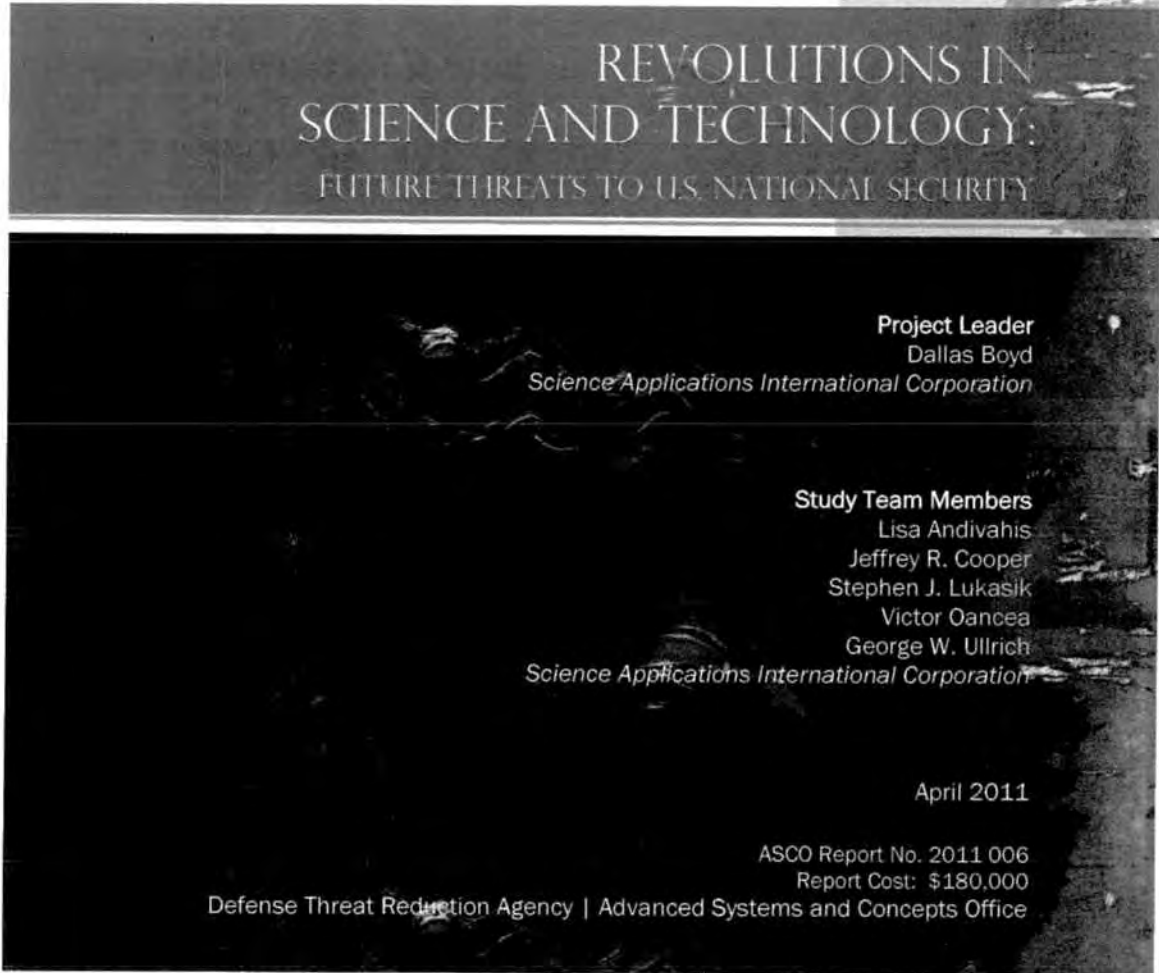


REVOLUTIONS IN SCIENCE AND TECHNOLOGY.

FUTURE THREATS TO U.S. NATIONAL SECURITY

APRIL 2011

DEFENSE THREAT REDUCTION AGENCY
ADVANCED SYSTEMS AND CONCEPTS OFFICE



REVOLUTIONS IN SCIENCE AND TECHNOLOGY: FUTURE THREATS TO U.S. NATIONAL SECURITY

Project Leader
Dallas Boyd
Science Applications International Corporation

Study Team Members
Lisa Andivahis
Jeffrey R. Cooper
Stephen J. Lukasik
Victor Oancea
George W. Ullrich
Science Applications International Corporation

April 2011

ASCO Report No. 2011 006
Report Cost: \$180,000
Defense Threat Reduction Agency | Advanced Systems and Concepts Office

The mission of the Defense Threat Reduction Agency (DTRA) is to safeguard America and its allies from weapons of mass destruction (chemical, biological, radiological, nuclear, and high explosives) by providing capabilities to reduce, eliminate, counter the threat, and mitigate its effects.

The Advanced Systems and Concepts Office (ASCO) supports DTRA's mission by providing long-term rolling horizon perspectives to help DTRA leadership identify, plan, and communicate what is needed in the near-term to achieve the long-term goals of the Agency's mission. ASCO also emphasizes the identification, integration, and further development of leading strategic thinking and analysis on the most intractable problems related to combating weapons of mass destruction.

For further information on this project, or on ASCO's broader research program, please contact:

Defense Threat Reduction Agency
Advanced Systems and Concepts Office
8725 John J. Kingman Road
Ft. Belvoir, VA 22060-6201

ASCOInfo@dtra.mil



"In the vast laboratories of the Ministry of Peace, and in the experimental stations hidden in the Brazilian forests, or in the Australian desert, or on lost islands of the Antarctic, the team of experts are indefatigably at work. Some are concerned simply with planning the logistics of future wars; others devise larger and larger rocket bombs, more and more powerful explosives, and more and more impenetrable armour-plating; others search for new and deadlier gases, or for soluble poisons capable of being produced in such quantities as to destroy the vegetation of whole continents, or for breeds of disease germs immunized against all possible antibodies; others strive to produce a vehicle that shall bore its way under the soil like a submarine under the water, or an aeroplane as independent of its base as a sailing ship; others explore even remoter possibilities such as focusing the sun's rays through lenses suspended thousands of kilometers away in space, or producing artificial earthquakes and tidal waves by tapping the heat at the earth's centre."

— George Orwell, 1984

ACKNOWLEDGEMENTS

The authors gratefully acknowledge Jennifer Borchard and Brenda McVeigh of Science Applications International Corporation for their many contributions to this report.



ACRONYMS

ABL	airborne laser
AFRL	Air Force Research Laboratory
ARPA	Advanced Research Projects Agency
ASAT	anti-satellite
ASCO	Advanced Systems and Concepts Office
BMA	British Medical Association
BTWC	Biological and Toxin Weapons Convention
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, or explosive
CBW	chemical and biological weapons
CIKR	critical infrastructure and key resources
CDMA	code division multiple access
CIA	Central Intelligence Agency
CPU	Central Processing Unit
CRS	Congressional Research Service
CTR	Computing-Tabulating-Recording Company
CW	continuous-wave
DARPA	Defense Advanced Research Projects Agency
DEW	directed-energy weapons
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DTIC	Defense Technical Information Center
DTRA	Defense Threat Reduction Agency
ECC	error-correcting code
EMI	electromagnetic interference
EMJ	EMI Micro-Jammer

EMP	electromagnetic pulse
EMS	electromagnetic spectrum
EO	electro-optical
ERDA	Energy Research & Development Administration
EW	electronic warfare
F CC	Federal Communications Commission
FCG	Flux Compression Generator
FFRDC	Federally Funded Research and Development Center
FOIA	Freedom of Information Act
fs	femtosecond
FSB	Federal Security Service (Russian Federation)
G AO	Government Accountability Office
GHz	GigaHertz
GPS	Global Positioning System
GW	GigaWatt
H PEM	High Power Electro-Magnetic
HPM	High-Power Microwave
I ED	improvised explosive device
ICRC	International Committee of the Red Cross
IND	improvised nuclear device
IR	infrared
ISP	internet service provider
K Hz	KiloHertz
L AN	local area network
LANL	Los Alamos National Laboratory
LLNL	Lawrence Livermore National Laboratory
M A	MegaAmpere
MAV	micro-unmanned aerial vehicle
MHz	MegaHertz
MILO	magnetically insulated line oscillators
MJ	MegaJoule
MW	MegaWatt
N IE	National Intelligence Estimate
NPS	Naval Postgraduate School
ns	nanosecond
P DA	personal digital assistant
ps	picoseconds
Q C	quantum computing
R &D	research and development
RF	radio-frequency

RFI	radio-frequency interference
RFQ	radio-frequency quadrupole
S&T	science and technology
SAIS	School of Advanced International Studies
SCADA	supervisory control and data acquisition
SDI	Strategic Defense Initiative
SIPRI	Stockholm International Peace Research Institute
SNM	special nuclear material
SNP	single nucleotide polymorphism
TDMA	time division multiple access
TIA	total information awareness
VoIP	Voice over Internet Protocol
WAN	wide area network
WMD	weapon of mass destruction
WME	weapon of mass effect

REVOLUTIONS IN S&T

TABLE OF CONTENTS

Acronyms	i
Introduction	1
Technology Threat Assessment Framework.....	2
Definition of a “Weapon of Mass Effect”	4
Definitions of “Game-Changing” Qualities	8
Report Roadmap.....	11
Narrative Template	14
Literature Search Methodology.....	15
Ultrafast Laser Technology: Future Applications for Directed-Energy Systems.....	17
Introduction	17
1. Technology Overview	18
2. Game-changing Qualities	24
3. Drivers/Counter-drivers of Technology Development	25
4. Drivers/Counter-drivers of Technology Attractiveness	26
5. Conclusion: Relevance to DTRA Mission	26
Advanced Biological Weapons: Genetically Engineered Pathogens.....	27
Introduction	27
1. Technology Overview	29
2. Game-changing Qualities	34
3. Drivers/Counter-drivers of Technology Development	35
4. Drivers/Counter-drivers of Technology Attractiveness	38
5. Conclusion: Relevance to DTRA Mission	44
Advanced Laser Isotope Separation and Enrichment.....	45
1. Technology Overview	45

2. Game-changing Qualities	49
3. Drivers/Counter-drivers of Technology Development.....	50
4. Drivers/Counter-drivers of Technology Attractiveness	50
5. Conclusion: Relevance to DTRA Mission	50

EMI Micro-jammers (EMJs): Exploiting ElectroMagnetic Interference For Disruption of Critical Networks and Infrastructure53

1. Technology Overview	53
2. Game-changing Qualities	58
3. Drivers/Counter-drivers of Technology Development.....	60
4. Conclusion: Relevance to DTRA Mission	61

Cyber Technology: Botnet Technology and Circuit Board Hacking.....63

1. Technology Overview	63
A1. Botnet Technology	70
A2. Game-changing Qualities	74
A3. Drivers/Counter-drivers of Technology Development.....	75
A4. Drivers/Counter-drivers of Technology Attractiveness	75
A5. Conclusion: Relevance to DTRA Mission	76
B1. Circuit Board Hacking.....	76
B.2 Game-changing Qualities	77
B.3 Drivers/counter-drivers of Technology Development.....	78
B.4 Drivers/counter-drivers of Technology Attractiveness	78
B.5 Conclusion: Relevance to DTRA mission.....	79

Quantum Computing Applications81

1. Technology Overview	81
2. Game-Changing Qualities	86
3. Drivers/Counter-Drivers of Technology Development	87
4. Drivers/Counter-drivers of Technology Attractiveness	88
5. Conclusion: Relevance to DTRA Mission	90

The E-Bomb: Urban Threat or Urban Legend?93

Introduction	93
1. Technology Overview	94
2. Game-Changing Qualities	98
3. Drivers and Counter-Drivers of Technology Development.....	100
4. Drivers and Counter-Drivers of Technology Attractiveness	100
5. Conclusion: Relevance to DTRA Mission	102

Concluding Observations on S&T Threat Analysis 103

1. The Awkward Matter of Time Frame	103
2. The Idiosyncratic Nature of Efforts of this Type	104
3. Where are the New "Impossibles"?	104
4. Red-Blue Perspectives in Assessing Technology	105
5. Roles, Missions, and the Problem of being Too Organized	105
6. Exploring a Sparse Multidimensional Space of Impossibles for Possibles	106
7. Technology does not Threaten People, People Threaten People.....	106

Appendix A: Team Member Biographies 107

Lisa Andivahis, Ph.D.....	107
Dallas Boyd.....	107

Jeffrey R. Cooper	108
Stephen J. Lukasik, Ph.D.	108
Victor Oancea, Ph.D.	108
George W. Ullrich, Ph.D.	109
Appendix B: Literature—General	111
Appendix C: Literature—Ultrafast Laser Technology.....	117
Appendix D: Literature—Advanced Biological Weapons	121
Appendix E: Literature—Advanced Laser Isotope Separation and Enrichment	129
Appendix F: Literature—EMI Micro-Jammers.....	133
Appendix G: Literature—Botnet Technology and Circuit Board Hacking.....	137
Appendix H: Literature—Advances in Quantum Computing.....	141
Appendix I: Literature—E-Bombs	149

REVOLUTIONS IN S&T



INTRODUCTION

"However far modern science and technics have fallen short of their inherent possibilities, they have taught mankind at least one lesson: Nothing is impossible."

— Lewis Mumford, *Technics and Civilization*, 1934

The objective of the following analysis is to advance a key mission of the Advanced Systems and Concepts Office (ASCO)—to identify and execute high-impact research concerning weapons of mass destruction (WMD) on behalf of the Defense Threat Reduction Agency (DTRA), the Department of Defense (DoD), and the whole of the U.S. government. This study supports ASCO's mission to encourage new thinking, address current technology gaps, identify developing threats, and improve the operational capabilities of federal agencies to respond to the threat from these weapons. The study's premises are that future science and technology (S&T) trends will inform adversaries' development of advanced weapons and understanding potential developments in S&T is crucial to U.S. planning. These weapons may include improvements to traditional WMD as well as new classes of weapons and capabilities referred to hereafter as "weapons of mass effects" (WME).

It is useful for policymakers to assess the technology areas that are most promising (from an adversary's perspective) in the development of new weapons. This is so for several reasons. Perhaps most importantly, this knowledge improves policymakers' situational awareness and helps fulfill a timeless national security imperative—the avoidance of technological surprise by one's enemies. An additional benefit is the potential identification of technologies that might negate or otherwise respond to evolutions in adversary capability. Finally, even if technological remediation is not possible, understanding novel adversary attack modes nonetheless informs U.S. planning and policymaking.

The approach adopted in this study represents a nexus between two broad categories of analysis, each with a substantial pedigree. The first of these concerns forecasts of technological developments. Such exercises date back decades and have attempted, with varying degrees of rigor, to predict what new marvels science will impart to humanity, how quickly, and with what implications.¹ While some of these forecasts relate specifically to security concerns (e.g., assessments of adversary nuclear programs), the vast majority concern broader S&T developments and are mostly produced and consumed by the private sector. The second category consists of conjecture on future adversary threat vectors, including malevolent applications of new technologies and potential policy responses to these developments. A vast literature exists comprising both categories of analysis. Since the terrorist attacks of September 11, 2001, the demand for syntheses of the two has also greatly increased. Consequently, there is no shortage of studies devoted to enumerating novel adversary threats enabled by high technology.² It is not the purpose of this analysis to lengthen this already substantial list.

TECHNOLOGY THREAT ASSESSMENT FRAMEWORK

Rather than providing another recitation of meta-level technology trends, the purpose of this study is to provide a *framework* for evaluating S&T developments through the lens of their national security implications. This framework allows analysts to extract a postulated technology or capability from available S&T forecasts and assess it using a multi-tiered filtering process. The process consists first of a determination of whether the technology qualifies as a potential WME; it is followed by an assessment of the qualities that would make the technology worrisome from a national security standpoint. A more detailed description of the framework elements follows.

Step One. The first step in the process is to identify a list of technologies of potential interest from the technology forecasting literature. A representative example of this literature is a National Intelligence Council analysis performed in 2008 as part of its *Global Trends 2025* project.³ This effort sought to identify “potentially disruptive” civil or dual-use technologies that might arise in the next 15 years. The study defined a disruptive technology as “a technology with the potential to cause a noticeable—even if temporary—degradation or enhancement in one of the elements of U.S. national power (geopolitical, military, economic, or social cohesion).” The following six technologies were ultimately identified from a list of 102 initial candidates: biogerontechnology, energy storage materials, biofuels and bio-based chemicals, clean coal technologies, service robotics, and the “Internet of Things.” Similar S&T forecasts abound, many of which are germane to the field of national security. These resources provide a substantial pool of future technologies that can be monitored on an ongoing basis.

¹ See, for example, *STAR 21—Strategic Technologies for the Army of the Twenty-First Century*, Board on Army Science and Technology, Commission on Engineering and Technical Systems, and National Research Council, Washington, D.C.: National Academy Press, 1992; “21st Century Strategic Technology Vectors—Volume I: Main Report,” Defense Science Board 2006 Summer Study, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., February 2007; William E. Halal, et al., “The GWU Forecast of Emerging Technologies: A Continuous Assessment of the Technology Revolution,” *Technological Forecasting and Social Change*, Vol. 59, September 1998; and “Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025,” National Intelligence Council, April 2008.

² See, for example, Gregory Giles, et al., “Thwarting an Evil Genius,” and Dallas Boyd, et al., “Thwarting an Evil Genius II,” Science Applications International Corporation, reports prepared for DTRA/ASCO, 2006 and 2009, respectively.

³ “Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025,” National Intelligence Council, April 2008.

Step Two. The second step involves assessing whether a technology has potential as a “weapon of mass effect,” a term for which no commonly accepted definition exists. For the purposes of this study, a technology or mode of attack is defined as a WME by virtue of its potential to produce one or more of the following effects:

- ▶ Substantial human casualties
- ▶ Destruction or disruption of societal critical systems
- ▶ Substantial alteration to our way of life
- ▶ Reaction that is greatly disproportionate to the provocation
- ▶ New or previously unrecognized weapon effects

These effects are described in greater detail below. Technologies or capabilities that do not qualify as WME can be set aside at this point in the filtering process.

All of the technologies examined in the sub-reports of this analysis were determined to qualify as WME. They were selected by the study team on the basis of their utility in illustrating the third step in the framework.

Step Three. The third step involves an assessment that mixes objective and subjective evaluations to determine if a technology merits particular scrutiny from the national security community, including investments in offsetting capabilities. Specifically, the step requires analysts to assess whether a technology might be considered “game changing” by virtue of its possessing some or all of the following qualities:

- ▶ Reduced barriers to entry
- ▶ System integration
- ▶ Novel delivery means
- ▶ Self-propagation
- ▶ Novel radical empowerment
- ▶ Mitigation of effects
- ▶ Diverse applicability

The assessment of these qualities is a relatively straightforward, objective exercise. It relies largely on the weight of expert opinion and is informed by multiple sources, ranging from the scholarly literature to intelligence assessments. The more subjective dimension involves a judgment about whether a technology crosses a certain “threshold of concern” as a result of these qualities. A technology may or may not be considered truly revolutionary if two or three of these criteria are met; however, it may satisfy only one and still be cause for alarm if that characteristic is sufficiently threatening. Technologies that are so identified are by definition those that should be the subject of closer study; in particular, for the technologies deemed to be on the verge of vastly greater availability, assessments should be made to confirm the timeline for this development and determine if countervailing efforts can be taken to influence this event. Yet for any advanced technology that threatens to degrade U.S. security, the defense establishment must be prepared to respond to the challenge. Additionally, it should be noted that while several of these categories concern qualities that would be particularly desirable to an *adversary*, the framework does not assume that S&T advances are useful only to malevolent actors. In several instances in the report, technologies are judged on the basis of their utility to the United States and its allies.

Adversaries

The focus of the study is on weapon-enabling technology rather than the specific actors who may make use of it. The analysis is therefore capabilities-based rather than adversary-based—the *ability* to harness a technology for destructive purposes is considered to be more consequential than the identity or motivation of the actor who utilizes it. The adversaries discussed in the study are therefore generally not specified. The term “Red” is frequently used as a proxy for U.S. adversaries writ large, including both state and non-state actors, as well as individuals in certain cases. Likewise, “Blue” is often used to connote the United States. The latter term may also apply to non-governmental entities such as private technology firms that develop capabilities for government use, as well as privately operated critical infrastructure that plays the role of “defender,” in game theory parlance, by virtue of its being targeted by “Red.”

Timeframe

The study considers a range of technologies, some of which will, in all likelihood, remain accessible to only the most sophisticated actors and others that will, over time, become commonly available. For the purposes of this report, the timeframe for the development of technologies is 6-20 years in the future.

DEFINITION OF A “WEAPON OF MASS EFFECT”

The technologies examined in this study have been included by virtue of their potential to be used as WME. This category is broader and somewhat more nebulous than the more familiar category of WMD. (WME shall be considered inclusive of traditional WMD, which are by definition agents of mass effect.)

The Homeland Security Advisory Council has defined WME as “weapons capable of inflicting grave destructive, psychological and/or economic damage,” including chemical, biological, radiological, nuclear, or explosive weapons.⁴ In short, WME is simply presented as a synonym for chemical, biological, radiological, nuclear, or explosive (CBRNE) weapons. However, this list is incomplete because it neglects, *inter alia*, malicious computer code, directed energy weapons, and a host of other capabilities that may produce significant disruption.⁵ A more appropriate definition

would characterize WME on the basis of their potential effects rather than the attributes of the weapons themselves. These effects include:

Substantial Human Casualties

The potential for mass casualties—whether deaths or non-fatal illnesses—is obviously among the U.S. government’s foremost concerns. However, defining “substantial” is a somewhat subjective exercise. Previous attempts to set thresholds that distinguish qualitative categories of attack have been dubious. At one point,



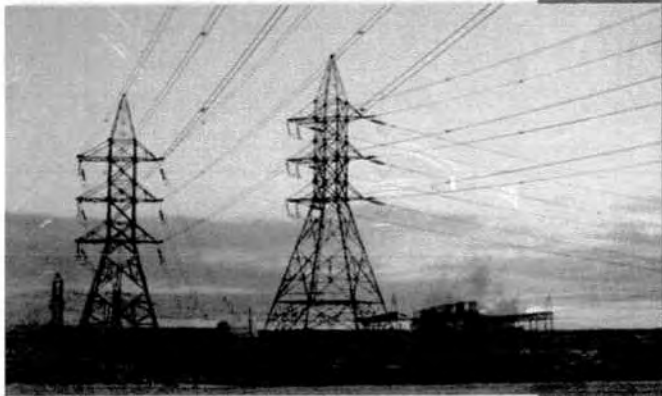
⁴ Report of the Homeland Security Advisory Council Weapons of Mass Effect Task Force on Preventing the Entry of Weapons of Mass Effect Into the United States, January 10, 2006.

⁵ See also Maria Rasmussen and Mohammed Hafez, “Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators,” Report for the Defense Threat Reduction Agency, Advanced Systems and Concepts Office, Report Number ASCO 2010-019, August 2010.

the Department of Homeland Security (DHS) experimented with the term “Incident of National Significance” to signify events of particular import, but this formulation was ultimately rejected.⁶ The term “catastrophic event” has also been used; it was defined as “any natural or manmade incident...that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions.”⁷ Former DHS official Maureen McCarthy supplied a more quantitatively precise definition of a “catastrophic” attack—one that produced 10,000 or more casualties (and greater than \$50 billion in economic damage), which would result in a “major global policy shift.”⁸ Yet the precision of these numbers is largely meaningless. It is difficult to imagine that an attack resulting in 10,000 victims would produce a substantively different response than one involving “only” 5,000 casualties (or 1,000 for that matter). Consequently, it is unnecessary to assign a specific number of casualties or level of economic damage that must be reached before an attack is classified as “substantial.” In all likelihood, the government will use the same criterion to define such an attack that Justice Potter Stewart used to identify lascivious material: “I know it when I see it.”⁹

Destruction or Disruption of Societal Critical Systems

This category recognizes that adversary attacks can be deeply significant despite their failure to produce human casualties. One variety of attacks fitting this definition involves the destruction or disruption of societal critical systems (e.g., transportation, communications, electricity, healthcare, food supply, etc.), which may produce significant economic damage, degradation of crucial government functions, as well as possibly loss of life. The DHS *National Infrastructure Protection Plan*, which concerned the protection of the nation’s “critical infrastructure and key resources (CIKR),” defined these as “systems and assets, whether physical or virtual, so vital to the United States that [their] incapacitation or destruction...would have a debilitating impact on national security, national economic security, public health or safety, or any combination of those matters.”¹⁰ While not all of the targets covered under the DHS definition can truly be described as “societal critical systems,” the plan nonetheless recognized that targeting physical or electronic systems can produce devastating effects on the United States.



Substantial Alteration to Our Way of Life

Defining a “way of life” presents an obvious challenge, as does establishing the threshold for an event that produces a “substantial” alteration to it. However, despite its subjectivity, this category captures a potential outcome that is distinct from casualties, physical destruction, and other direct effects of attacks. For example, after the 9/11 attacks, the overwhelming majority of Americans expe-

⁶ See *National Response Plan*, Department of Homeland Security, December 2004. p. 4.

⁷ *National Response Plan*, December 2004. p. 43.

⁸ Steve Coll, “The Unthinkable,” *New Yorker*, March 12, 2007.

⁹ Supreme Court Justice Potter Stewart, concurring opinion in *Jacobellis v. Ohio* 378 U.S. 184 (1964).

¹⁰ *National Infrastructure Protection Plan*, Department of Homeland Security, 2009.

experienced few visible impacts on their daily lives beyond the inconvenience of enhanced airport security. Nevertheless, by virtually any definition, 9/11 would be described as having altered the American way of life in a fundamental way. Not least, the attacks greatly diminished Americans' sense of their own security.



In the wake of future attacks, psychological effects that fall under this category may include: reluctance to engage in normal behavior (e.g., utilization of public transportation, gathering in public places); perception of a threat to personal safety sufficient to cause work/school absenteeism; perception of a national trauma that undermines confidence in the future of the country; willingness to evacuate one's home in response to a threat; avoidance or fear of foods or exposures to social environments; disregard of government mandates; breakdowns of the norms of civilized behavior; and so on. Non-psychological effects may include the scarcity of certain essential commodities (e.g., food, fuel, etc.), restrictions on travel (e.g., denial of contaminated areas), and curtailment of basic civil liberties (e.g., denial of due process, removing the warrant requirement for government surveillance, etc.).

Reaction that is Greatly Disproportionate to the Provocation

This category covers responses to an attack that have the effect of compounding the injury sustained or otherwise producing unnecessary

additional damage. These reactions may include individual responses to an event (e.g., panicked citizens evacuating from a city after a CBRN attack),¹¹ as well as formal policy responses (e.g., disproportionate military action).¹² One episode frequently cited as an example of policy overreaction is the U.S. government's response to the 2001 anthrax attacks. During this incident, five people were killed and another 17 sickened by anthrax-laced letters.¹³ As John Mueller notes, the cost associated with these attacks for the U.S. Post Office alone was upwards of \$5 billion, or "\$1 billion for every fatality inflicted by the terrorist."¹⁴ Other government

¹¹ Long before September 11, 2001, terrorism scholar Ehud Sprinzak observed that while much analysis centered on the threat of catastrophic attacks, in reality "[t]he true threat of superterrorism will not likely come in the form of a Hiroshima-like disaster." Rather, he argued, it would take the form of "widespread panic caused by a relatively small [chemical- or biological-weapons] incident involving a few dozen fatalities." See Ehud Sprinzak, "The Great Superterrorism Scare," *Foreign Policy*, Fall, 1998.

¹² For further discussion of the dangers of reacting disproportionately to terrorist attacks, see Dallas Boyd and James Scouras, "The Dark Matter of Terrorism," *Studies in Conflict & Terrorism*, Vol. 33, Issue 12, December 2010.

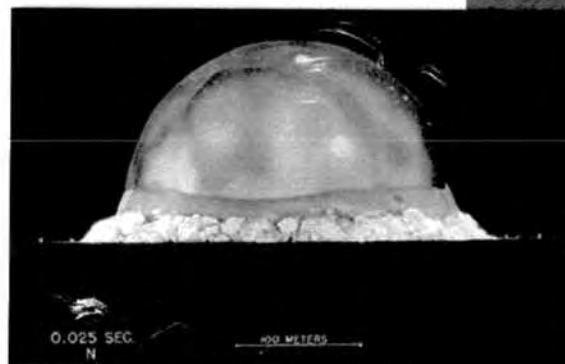
¹³ Scott Shane, "F.B.I., Laying Out Evidence, Closes Anthrax Case," *New York Times*, February 19, 2010.

¹⁴ John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*, New York: Free Press, 2006. p. 31. The total spent on the U.S. biodefense infrastructure since 2001 approaches \$50 billion, although this funding cannot be attributed wholly to the anthrax attacks. See Christian Enemark and Ian Ramshaw, "Gene Technology, Biological Weapons, and the Security of Science," *Security Studies*, Volume 18, Issue 3, July 2009. pp. 624-641. Additionally, Rutgers University Professor Leonard Cole calculated the economic impact of the anthrax attacks at over

policies since 9/11, including aviation security measures, the expanded use of warrantless wiretapping, the treatment of detainees, and, most controversially, the U.S. invasion of Iraq, are frequently assigned to this category as well. Yet whatever one's assessment of these individual policies, it has become increasingly clear to decision-makers and the public alike that, as Fareed Zakaria notes, "The purpose of terrorism is to provoke an overreaction."¹⁵ Terrorist capabilities that are particularly well suited to producing such overreaction should therefore be especially worrisome to U.S. policymakers. For example, given the dread of virulent disease and radioactive contamination, highly contagious pathogens and radiological weapons are ideal terror weapons.¹⁶

New or Previously Unrecognized Weapon Effects

Most analyses of future threats concern variations on familiar themes—more lethal biological agents, more effective delivery of explosives, and so on. However, the possibility of completely new weapon effects should not be ignored. As an example, consider the stunningly brief timeline of the development of the atomic bomb. Only 13 years separated the initial discovery of the neutron in 1932 and the battlefield use of nuclear weapons. In 1933, physicist Leó Szilárd first conceived the idea of a nuclear chain reaction.¹⁷ In 1939, Albert Einstein delivered his famous letter to President Roosevelt warning of "extremely powerful bombs of a new type" resulting from a chain reaction in a mass of uranium.¹⁸ Three years later, the world's first nuclear reactor went critical at the University of Chicago.¹⁹ Finally, in 1945 the Trinity test confirmed the design of the device that would be dropped on Nagasaki three weeks later.²⁰ In recent years, analysts have occasionally considered the achievement of similarly revolutionary effects. For example, in 1999, the Hart-Rudman Commission identified the possibility that "increasingly precise means of altering mental states" will be developed, including "new psycho-pharmacological methods of inducing happiness, self-esteem, and other emotions, entirely divorced from any behaviors in the world."²¹ The variety and impact of other technological leaps is limited only by the imagination. It suffices to note that the potential for new or previously unrecognized effects may be a key determinant of a technology's relevance in future threat assessments.



\$6 billion. See *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*, New York: Vintage Books, 2008, p. 8. For additional examples of counterterrorism policy overreactions, see John Mueller, "Six Rather Unusual Propositions About Terrorism," *Terrorism and Political Violence*, Vol. 17, Autumn 2005, pp. 487-505.

¹⁵ Fareed Zakaria, "Don't panic. Fear is al-Qaeda's real goal," *Washington Post*, January 11, 2010.

¹⁶ Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein, "Why Study Risk Perception?" *Risk Analysis*, Vol. 2, No. 2, 1982, pp. 83-93.

¹⁷ Richard Rhodes, *The Making of the Atomic Bomb*, New York: Simon & Schuster, 1986, pp. 27-28.

¹⁸ Caterina Dutto, "Einstein's Nuclear Warning," *Carnegie Endowment for International Peace*.

¹⁹ Rhodes, 1986, pp. 432-440.

²⁰ The "gun-type" uranium weapon dropped on Hiroshima was not tested in advance of the bombing; uranium was in such short supply, and the designers were so confident of the design, that a test was deemed unnecessary. The latter detail is noteworthy in the context of this analysis because the actual use of a weapon or capability might be the first manifestation.

²¹ *New World Coming: American Security in the 21st Century—Supporting Research and Analysis*, Phase I Report of The United States Commission on National Security/21st Century, September 15, 1999.

DEFINITIONS OF "GAME-CHANGING" QUALITIES

The technologies discussed in this report are analyzed through the lens of the "game-changing" qualities described below. While a number of these qualities involve subjective definitions (e.g., "novel" delivery means, "radical" conferment of power, etc.), they are intended to capture characteristics that make technologies especially consequential in the WME context. The categories below concern attributes such as the manner in which a technology is acquired, the means with which weapon effects are delivered, the broader impact that may result from their development, and so on.

Reduced Barriers to Entry

The first category concerns increases in the threat from an existing technology that results when its acquisition and/or use becomes substantially less difficult for malevolent actors. These developments may include greatly reduced cost, ease of production, ability to conceal the production signature, and so on. A hypothetical example might include new processes to enrich uranium for nuclear weapons that are considerably cheaper or easier to conceal than current methods. In this case, the weapon itself is hardly a novel technology, but the means of easily and discreetly developing it greatly increases the threat calculus. Another possible example is the increased availability of information on synthetic pathogens, which may lower the bar to creating advanced biological weapons.

System Integration

This category involves novel combinations of extant technology to produce new or particularly harmful effects. As an example of this quality, consider the malevolent use of social networking technology.²² During the height of the Iraq insurgency, militants frequently videotaped attacks on coalition military personnel. Insurgent-produced videos featured IED detonations, attempted shoot-downs of U.S. military helicopters, and other attacks that were then posted on jihadist web sites.²³ Other enemy uses of the Internet included disseminating videos of captured military personnel.²⁴ While neither these battlefield tactics nor the Internet were novel developments at the time of the conflict, their use in combination represented a significant enemy achievement. An attack in the United States using similar tactics would surely magnify its psychological effect. For example, terrorists might film the shoot-down of a domestic passenger aircraft and arrange its distribution to the U.S. media. While the mere knowledge of such an attack would be horrifying, graphic footage of the event would greatly intensify its impact.²⁵

²² A 2011 report by the Center for Strategic and International Studies described al-Qaeda's increasing use of Facebook and YouTube to communicate with affiliates and disseminate training and propaganda material. See Rick Nelson, et al., "A Threat Transformed: Al Qaeda Associated Movements in 2011," Center for Strategic and International Studies, February 2011.

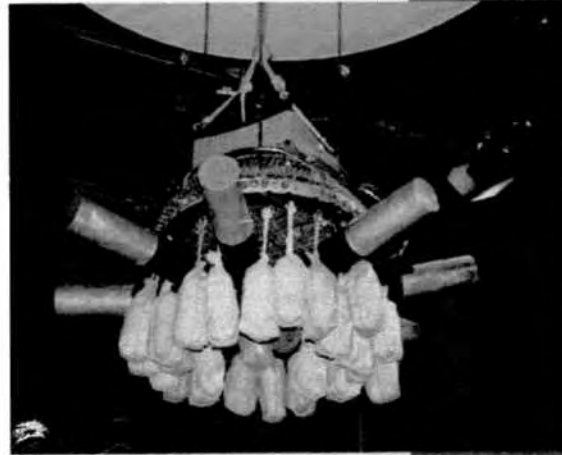
²³ A briefing prepared by the U.S. Army's Training and Doctrine Command notes that these videos are "complex and sophisticated, with detailed graphics, English subtitles, English narrators, Jihadist 'humor,' and insults directed at the coalition to weaken resolve and popular support." See John Diamond, "Insurgents give U.S. valuable training tool," USA Today, January 25, 2006. In 2005, one such video of a sniper attack on an U.S. Army medic became an Internet sensation, although its audience was not the intended one. The soldier's body armor deflected the round, and his panache under fire delighted American viewers. See Chris Foster, "256th BCT Soldier survives sniper attack," 256th Brigade Combat Team press release, July 5, 2005.

²⁴ Damien Cave, "Iraq Insurgent Group Claims It Killed Missing U.S. Soldiers," *New York Times*, June 5, 2007.

²⁵ There is a historical precedent for such an attack. In 1986, when Afghan *mujahideen* began firing U.S.-supplied Stinger missiles at Soviet helicopters, the attacks were filmed with cameras supplied by the CIA. Footage of the first successful attack, which claimed three Russian helicopters, was screened at the White House a short time later. See Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001*, New York: Penguin Books, 2004. pp. 149-150.

Novel Delivery Means

This quality concerns the dissemination of weapons or agents in an unconventional or previously unconsidered manner. One such example is Japan's use of balloon-borne bombs against the continental United States during World War II. Consisting of a 10-meter hydrogen-filled balloon and a small incendiary payload, these weapons were designed to cross the Pacific and ignite fires in American cities and forests. More than 9,000 were launched between 1944-1945, of which roughly 300 reached land.²⁶ While the balloons produced little damage, their potential to carry biological weapons concerned U.S. officials.²⁷ Twenty-first century incarnations of these devices are readily conceivable. For example, one 2005 analysis described a "future scenario involving swarms of micro UAVs (MAVs) carrying genetic weapons," an attack with the potential to produce "powerful and precise political, economical, and military effects from a tiny payload."²⁸ Other novel delivery means might involve the use of food or water supplies to spread toxins, aerosolized delivery of biological agents, and a host of other conveyances.



Self-propagation

This category describes weapons that, by virtue of their design or natural properties, can spread in their environment without the continued assistance of the perpetrator. The category obviously includes infectious diseases, as well as cyber "malware," which are aptly referred to as viruses. A less frequently considered form of self-propagation involves the spread of psychological trauma that may result from an attack. As a recent study of the National Academy of Sciences noted, "Little attention has been paid to secondary economic effects or to an attack's effects on personal and group behaviors—impacts that could be significant and may be the primary goals of terrorists."²⁹ An especially traumatizing attack might produce self-sustaining behavioral effects.³⁰ Additionally,

²⁶ See Robert C. Mikesh, *Japan's World War II Balloon Bomb Attacks on North America*, Smithsonian Institution Press, 1973. See also Bert Webber, *Retaliation: Japanese Attacks and Allied Countermeasures on the Pacific Coast in World War II*, Oregon State University Press, 1975.

²⁷ Nicholas D. Kristof, "Unmasking Horror—A Special Report: Japan Confronting Gruesome War Atrocity," *New York Times*, March 17, 1995.

²⁸ Daryl J. Hauck, "Pandora's Box Opened Wide: UAVs Carrying Genetic Weapons," Occasional Paper No. 47, Center for Strategy and Technology, Air War College, Air University, Maxwell AFB, Alabama, November 2005. See also James M. Abatti, "Small Power: The Role of Micro and Small UAVs in the Future," Occasional Paper No. 45, Center for Strategy and Technology, Air War College, Air University, Maxwell AFB, Alabama, November 2005; and International Symposium on Flying Insects and Robots, Monte Verità, Ascona, Switzerland, August 12-17, 2007.

²⁹ National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis*, Washington, D.C.: The National Academies Press, 2010. p. 5.

³⁰ However, it should not be assumed that the expected response to a terrorist attack, even a large-scale one, will be panic and disorder. Evidence such as the response to the July 2005 London Underground attacks indicates that publics often resume previous behaviors within a reasonably short time. See Thomas A. Glass and Monica Schoch-Spana, "Bioterrorism and the People: How to Vaccinate a City against Panic," *Clinical Infectious Diseases*, Vol. 34, January 15, 2002.

in the case of novel combinations of technology, the mere dissemination of information can constitute a form of self-propagation. Similarly, knowledge of the mechanics of an effective and easily replicable attack may prompt others to utilize it, producing a "viral" effect.

Novel Radical Empowerment

This quality concerns the empowerment of a group (or, theoretically, an individual) due to the attainment of an especially potent technology. "Radical" empowerment occurs when a group's stature rises to a level previously reserved to national governments.³¹ The prototypical example of this possibility is a terrorist organization's acquisition of a nuclear weapon. The use of such a device would entail destruction that only a small number of states are capable of producing. However, this status would extend far beyond the actual detonation of the weapon. A nuclear-armed terrorist group could use the capability as a bargaining instrument, which would profoundly complicate the U.S. policy of refusing to negotiate with terrorists. Lewis A. Dunn raises this possibility in an analysis challenging the assumption that al-Qaeda would use any nuclear weapon that it acquired.³² He suggests that Osama bin Laden would "think in terms of how best to leverage possession" to serve his long-term goals, including the establishment of a pan-Islamic Caliphate. Dunn argues that the "realization of this goal ultimately will require al-Qaeda to seize power in at least one Islamic state," and that "possession but nonemployment" could deter U.S. military action against the new country.³³ Other weapons that confer this power either exist but are unobtainable to terrorists or have yet to be developed. A biological weapon capable of producing deaths on the order of a nuclear attack would arguably qualify as the former; the ability to destroy or disable U.S. space assets might be an example of the latter.

Mitigation of Effects

This category applies to technologies that enable the mitigation of particular undesirable effects. For example, in the event of a terrorist nuclear attack, mass communication technologies may allow authorities to transmit crucial instructions to populations at risk of radioactive fallout. While this technology would not prevent deaths from prompt blast and radiation effects, tens of thousands of lives might be saved if an urban population can make an informed decision about whether to evacuate an area or shelter-in-place. Real-time plume modeling coupled with electromagnetic pulse (EMP)-resistant and saturation-proof communication technologies might provide this benefit. Indeed, a 2007 study called for the development of "an updated version of the Emergency Broadcast System" for just such an eventuality. This system would utilize modern media with "the capability to send text messages or emails to all citizens and/or responders who have wireless devices (cell phones, Blackberry and other PDA devices, etc.)."³⁴ Other examples might include

³¹ In the late 1990s, author Thomas Friedman warned of the rise of the "Super-Empowered Angry Man." Friedman's villain was a rage-filled individual who, because of technological advances and other aspects of globalization, was able to produce destruction on a previously inconceivable level. Hijacker Mohammed Atta is frequently held aloft as an exemplar of this phenomenon. See Thomas L. Friedman, *The Lexus and the Olive Tree*, New York: Farrar, Straus and Giroux, 1999, p. 381.

³² See, for example, the following statement by Rolf Mowatt-Larssen, former director of Intelligence and Counterintelligence at DOE: "Al-Qaeda's leaders yearn to acquire and use weapons of mass destruction against the United States; if they acquired a nuclear bomb, they would not hesitate to use it." See Rolf Mowatt-Larssen, "Al-Qaeda's Nuclear Ambitions," *Foreign Policy*, November 16, 2010.

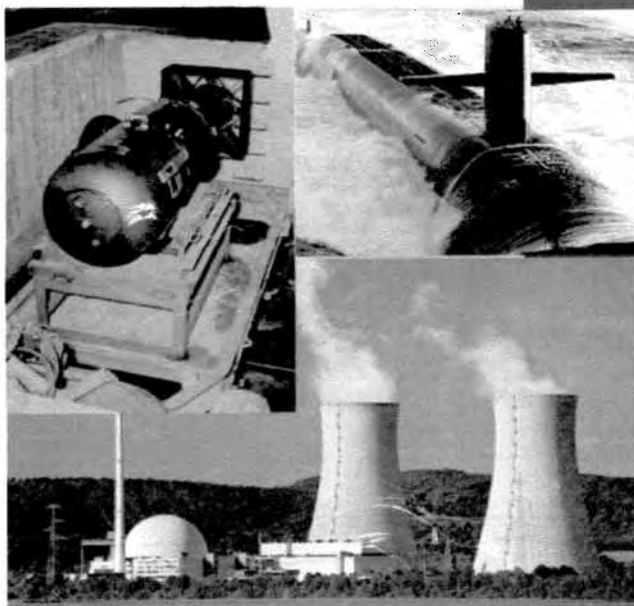
³³ Lewis A. Dunn, "Can al-Qaeda Be Deterred from Using Nuclear Weapons?" Center for the Study of Weapons of Mass Destruction Occasional Paper #3, Washington, D.C.: National Defense University, July 2005.

³⁴ See Ashton B. Carter, Michael M. May, and William J. Perry, *The Day After: Action in the 24 Hours Following a Nuclear Blast in an American City*. Cambridge, Mass.: Report for Preventive Defense Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2007.

improved vaccines against known pathogens and the ability to rapidly generate vaccines for synthetic (i.e., previously unstudied or vaccine-resistant) biological weapons.

Diverse Applicability

This category covers technological advances that have multiple applications. A technology is assumed to be more consequential if it has numerous potential applications rather than just a few. Diverse applicability can be defined in several ways, two of which are sufficient for this analysis. The first concerns the potential for multiple practical uses of a particular technology. Consider, for example, the array of applications of nuclear energy. Advances in our understanding of physics have led to the development of nuclear weapons, civilian electricity generation, propulsion for submarines and surface vessels, power for orbiting spacecraft, agricultural applications, medical therapies, and many other advances.³⁵ The second level of diverse applicability involves technologies that enable broad advancement across multiple scientific fields. The archetypal example of such a technology is the computer, which has become integral to virtually every facet of science and technology. In the not too distant future, nanotechnology and quantum computing may enable comparable breakthroughs across a range of scientific pursuits.



REPORT ROADMAP

The following section provides brief synopses of the sub-reports produced under this study. Each concerns a technology that was chosen based on its potentially revolutionary effect on adversary capabilities. However, the discussion of these technologies is principally intended to illustrate the analytical framework described above. The list is *not* meant to represent the study team's determination of the most worrisome over-the-horizon technologies. Indeed, in some cases, the reports conclude that the technology examined is less threatening than is widely believed. Nonetheless, in addition to demonstrating a useful methodology for evaluating novel technologies, each sub-report has value in raising DTRA's awareness of often obscure technological possibilities.

"Ultrafast Laser Technology: Future Applications for Directed-Energy Systems"

Lisa Andivahis, Ph.D.

This report considers ultrafast laser technology because of its potential to provide game-changing capabilities in applications such as the disruption of electro-optical (EO) and infrared (IR) sensors. The nature of the upward trend in the availability of ever more powerful lasers increases the potential for technological breakout in this domain. This evolution threatens to open up a broad range of threats as adversaries,

³⁵ A Cold War-era experiment, the Aircraft Nuclear Propulsion program, attempted to develop a nuclear propulsion system for bomber aircraft.

including individual actors, generate novel offensive applications for laser technology. However, it will also provide opportunities to improve U.S. defenses as the government capitalizes on creative applications of the technology. With the advent of nanotechnologies that facilitate relatively small, low-cost, high-power laser sources, coupled with their broad commercial availability, the potential emergence of directed-energy systems in adversaries' hands will be further increased.

"Advanced Biological Weapons: Genetically-Engineered Pathogens"

Dallas Boyd

As part of the triad of "traditional" WMD, biological weapons have been a pressing security concern for generations. However, advances in the life sciences, and particularly leaps in our understanding of the human genome, raise the possibility that even more worrisome varieties of biological weapons will arise. Through genetic engineering, enhancements to existing pathogens are thought to be possible; these could increase the pathogens' infectiousness, lethality, resistance to treatment, and other characteristics. While research on genetically engineered bioweapons has occurred at the state level for several decades, this capability is not believed to have migrated beyond the most advanced (and clandestine) facilities. The proliferation of biotechnology research laboratories could lead to a considerable increase in the accessibility of this dangerous knowledge. An even greater concern than simply "boosting" known pathogens, however, is the possibility that biological agents may be developed that target specific populations while leaving others unaffected. As the knowledge of human genetics advances, it may be possible to identify unique genetic markers carried by members of a particular ethnic group. According to a small but growing number of scientists, this information could conceivably allow weapons to be developed that would target only carriers of these distinct markers.

"Advanced Laser Isotope Separation and Enrichment"

Jeffrey R. Cooper

Within the nuclear community, it is generally accepted that obtaining fissile material is the most difficult step in developing a nuclear explosive device. Historically, enrichment of uranium and reprocessing plutonium to weapons-grade quality has only been possible through the use of large, energy-intensive facilities whose operation creates recognizable signatures. These include nuclear reactors and gaseous diffusion and centrifuge facilities. Among the potential alternatives for isotope separation, there are techniques that pose a particular proliferation concern because of their reduced scale, cost, and efficiency. The use of lasers is one of these less conspicuous routes to isotope separation. The growing use of lasers for academic and industrial research, and their consequent availability in low cost, compact forms, increases the likelihood that researchers will discover additional approaches to exploiting laser chemistry. A truly compact, frequency-stable laser tunable to the frequencies of interest for isotope separation could allow many actors to exploit laser technologies for separation and enrichment. Coupled with innovative separation techniques based on differential responses (such as chemical bonding or spin) of the isotopes to the laser energy, these technologies could provide true breakthroughs with dramatic consequences for nuclear proliferation.

"EMI Micro-Jammers (EMJs): Exploiting Electromagnetic Interference for Disruption of Critical Networks and Infrastructure"

Jeffrey R. Cooper

Electromagnetic Interference Micro-Jammers (EMJs) exploit modern electronic, robotic, and nanotechnologies and could enable the widespread disruption of critical information networks and societal infrastructures at low cost to the attacker. EMJs could be distributed in a wide range of ways: by unsophisticated methods—such as

simply scattering by hand or blowing from moving vehicles—to more highly targeted emplacements by nano-bots or micro-flyers homing on specific radiated signals. This capability would create a new niche in the threat taxonomy that differs from existing concerns about corruption of information content or interruptions of communication flows by cyber attacks, disruption of specific waveforms and signals by traditional electronic warfare, as well as localized effects from high-power pulse devices such as EMP. This new threat is produced through the exploitation of increasing dependencies by modern societies on these networks and infrastructures for mission-critical services at very high reliability factors. In particular, EMJs could portend serious threats to distributed communications systems, including supervisory control and data acquisition (SCADA), and certain lesser recognized functions of the Global Positioning System (GPS) system, such as timing.

“Cyber Technology: Botnet Technology and Circuit Board Hacking”

Stephen J. Lukasik, Ph.D.

When compared to the much longer period of the development of computers and information technology, cyber conflict and cyber weapons have received public attention only relatively recently. Their origin dates to classified thinking in the early 1990s. Because of the nature of the technologies associated with these concepts, the evolution of cyber warfare and its effects on national security are difficult to predict. Two areas of concern are large-scale botnets and circuit board attacks. Botnets are the result of the easy scalability of systems of computers into larger systems of systems; they can be used for offensive or defensive purposes, providing easy methods to exploit weak Internet security. Circuit board attacks are enacted by the burn-out of a circuit element that requires replacement, usually of the entire board. Because the maintenance of an adequate level of spares would impose enormous economic burdens and replacement of large numbers of damaged devices takes time, if a circuit board attack is sufficiently widespread, the cumulative damage can overwhelm global supply chains.

“Quantum Computing Applications”

Victor Oancea, Ph.D.

Quantum computing has significant implications for the expansion of network-based applications requiring powerful processors, high-density storage, and high-speed switching. Currently, due to practical difficulties associated with their design and implementation, most quantum computers have been built in laboratory environments; until now, they have only been used to solve trivial problems. While quantum computing will not, in and of itself, pose a direct threat to the United States, the technology may enable a number of capabilities that impinge on national security. At the most basic level, the tremendous computing power that even a medium size quantum computer would provide could be used to integrate data and develop models of complex systems across multiple spatial and temporal scales. This would allow for modeling and simulation of complex natural or biological phenomena that would be difficult, if not impossible, to perform using existing computing capacities. It is possible that the knowledge and principles that arise from these discoveries could subsequently be applied for nefarious purposes. No matter how it is used, the era of quantum computing will be game-changing in a manner resembling the advances that have occurred in the current computing era.

“The E-Bomb: Urban Threat or Urban Legend?”

George W. Ullrich, Ph.D.

The continental-scale footprint of EMP effects from high-altitude nuclear detonations in terrestrial electrical systems were first observed in 1962. Research on conven-

tional pulse power has since shown that the high frequency component of nuclear EMP can be emulated with explosively-driven flux compression generators or electrically-driven high power microwave sources. Sensational media reports on these so-called "E-bombs" have suggested that entire cities can be darkened by the use of such devices. While U.S. civil and military infrastructures have increasingly been embedded with electronic components that are highly vulnerable to EMP, a realistic assessment of the technology suggests that the damaging effects of the most powerful non-nuclear EMP devices are limited to a range of a few hundred meters. Moreover, the level of technical knowledge required to fabricate such devices is likely beyond the reach of a Third World adversary or a non-state actor. The study concludes that non-nuclear EMP devices appear to have attributes that are highly desirable for Blue-on-Red engagements, including stealth, non-attribution, speed of light, tunable lethality, deep magazine, non-lethality to humans, and low collateral consequences. Such a capability complements the offensive capability of the U.S. military, providing more options to the commander in the field when lethal force may be inadvisable or unacceptable. The case for Red-on-Blue engagements is less compelling, especially for terrorist attacks in urban settings. Such adversaries do not share the U.S. obsession for minimal collateral effects. To the contrary, they would prefer to maximize collateral consequences of execution. This factor, coupled with the unpredictable nature of electronic attacks, makes it less likely that terrorists will pursue this technology.

Concluding Observations on S&T Threat Analysis

Stephen J. Lukasik, Ph.D.

The final section of the report provides a number of concluding observations relating to the analysis of future S&T developments.

Appendix A provides biographical sketches of the individual team members who contributed to the report.

Appendix B contains general literature related to S&T advances that may have WMD/WME implications.

Appendices C-I contain references that were consulted in the preparation of each sub-report. The references are arranged in descending chronological order for ease of location.

NARRATIVE TEMPLATE

The sections below generally conform to the following outline, with exceptions made as necessary given the particulars of the technology under review.

1) Technology Overview. This section introduces the reader to the technology under review; it provides historical background, evidence of the technology's harm potential, and other contextual information. The section also summarizes the present level of accessibility (i.e., whether the technology is accessible to states, sub-state groups, or individuals). Speculation is provided on the timeline for the technology's development (i.e., if the technology is undeveloped at present, the timeline of its initial development is estimated; if the technology is accessible only to advanced states, the timeline of its broader accessibility is considered).

2) Game-changing Qualities. This section identifies the applicability of the various "game-changing" qualities described above (e.g., reduced barriers to entry; novel delivery means; self-propagation; and so on) to the technology in question. The

authors supply descriptions of these qualities that are specific to the technology being considered.

3) **Drivers/Counter-drivers of Technology Development.** This section captures the factors that may drive or inhibit the development of the technology in the coming years. This category differs from the factors described below, which concern influences on technology *attractiveness*. Examples of development drivers/counter-drivers may include, but are not limited to, the following:

- ▶ **Driver:** The imperative to avoid drastic change to a way of life (e.g., research on geoengineering to cope with climate change).
- ▶ **Counter-driver:** Immaturity of information/expertise necessary to achieve technology; lack of resources; lack of societal investment (i.e., “buy in”).
- ▶ **Driver:** “Market” forces driven by the allure of potential benefits (e.g., stem-cell research to facilitate medical advances).
- ▶ **Counter-driver:** Regulation driven by threat concerns; normative/ethical considerations.

4) **Drivers/Counter-drivers of Technology Attractiveness.** This section captures the drivers/counter-drivers that influence the attractiveness of the technology from an adversary’s perspective. Consider, for example, the prospect of an adversary’s developing an Improvised Nuclear Device (IND). Among the factors that would influence this decision are: the cost and difficulty of acquiring fissile material, the possibility of being detected doing so, the difficulty of smuggling a weapon to the target, and the magnitude of its effects. Conversely, the factors that would influence Blue’s selection of IND countermeasures are: the cost of developing radiation portal monitors, the difficulty and expense of deploying scanners across multiple entry points, and the adversary’s ability to defeat or bypass them. The technologies are discussed through the prism of drivers/counter-drivers of attractiveness such as:

- ▶ Accessibility (e.g., cost, access to requisite materials);
- ▶ Signature (e.g., likelihood of detection);
- ▶ Ability to deploy (e.g., quality of delivery means); and
- ▶ Efficacy (e.g., effectiveness in producing the desired consequences).

5) **Conclusion.** The narrative concludes with observations on the relevance of the technology to DTRA’s mission to identify areas for S&T investment.

LITERATURE SEARCH METHODOLOGY

All of the material referenced in the literature review is unclassified. The authors conducted a thorough survey of the literature related to each technology examined in the study. In addition to supporting the report, this literature may serve as a useful starting point for further research on these subjects. References used in the individual sections are provided as appendices at the conclusion of the report. While this literature captures a substantial portion of the analysis devoted to the individual technologies, no such anthology can make any claim to comprehensiveness.

Among the sources of information searched were the following:

- ▶ **Scholarly / professional journal articles:** Scholarly articles related to S&T. This category also includes books, book chapters, and items from general-interest periodicals such as major newspapers, popular magazines, and Web publications.

- ▶ **Think tank / academic research institute analyses:** Analyses produced by non-profit think tanks and academic research institutes such as the MIT Strategic Studies Program, the Union of Concerned Scientists, the Carnegie Endowment for International Peace, Brookings Institution, Council on Foreign Relations, Nuclear Threat Initiative, and Federation of American Scientists.
- ▶ **S&T conference materials:** Research papers presented at, as well as the proceedings of, various technology-related conferences.
- ▶ **U.S. Government analyses:** Analyses produced by the individual U.S. military services, as well as Federally Funded Research and Development Centers (FFRDCs). These include The Johns Hopkins University Applied Physics Laboratory (APL), RAND's Project Air Force, the Government Accountability Office (GAO), the Congressional Research Service (CRS), and the Naval Postgraduate School (NPS). Declassified National Intelligence Estimates (NIEs) related to the S&T efforts of foreign nations, including the development of CBRNE weapons and other high-technology pursuits, were also consulted.
- ▶ **Government-sponsored scientific panel reports:** Reports and analyses resulting from panels assembled under the auspices of the National Academy of Sciences, JASON Defense Advisory Panels, the Defense Science Board, and other *ad hoc* bodies of distinguished scientists. This category also includes analyses produced by defunct U.S. government research institutes such as the Office of Technology Assessment.
- ▶ **National Laboratories and Technology Center analyses:** Analyses produced by the Department of Energy (DOE) national laboratories (e.g., Lawrence Livermore National Laboratory, Sandia National Laboratories, and Los Alamos National Laboratory).

The majority of the materials utilized in the study were obtained from public-use search engines and databases such as Google, Google Scholar, IngentaConnect, Academic Search Premiere, JSTOR, LexisNexis, and ProQuest. Documents originally produced by the U.S. Government were obtained from databases containing unclassified or declassified material, including the Defense Technical Information Center (DTIC), the CIA's Freedom of Information Act (FOIA) Electronic Reading Room, the National Security Archive at The George Washington University, and the Federation of American Scientists archives. As the initial literature review progressed, selected documents pointed the research team to additional material. To ensure that the search was comprehensive, the team reviewed the bibliographies of selected documents for relevant material. The team also obtained documents such as books and archived scholarly journals from public and university libraries.



ULTRAFAST LASER TECHNOLOGY: FUTURE APPLICATIONS FOR DIRECTED-ENERGY SYSTEMS

LISA ANDIVAHIS, PH.D.

"Nikola Tesla, father of modern methods of generation and distribution of electrical energy... announced a new invention, or inventions, which he said, he considered the most important of the 700 made by him so far. He has perfected a method and apparatus... which will send concentrated beams of particles through the free air, of such tremendous energy that they will bring down a fleet of 10,000 enemy airplanes at a distance of 250 miles from a defending nation's border and will cause armies of millions to drop dead in their tracks."

— New York Times, July 11, 1934

INTRODUCTION

The science and technology of directed-energy phenomenology has been evolving over the past five decades. The use of directed-energy technology such as laser beams, once confined to the realm of science fiction, gained ground in the scientific community in 1960 when Theodore Mainman demonstrated the first working ruby laser, soon to be followed in 1961 with Elias Snitzer's fiber laser.³⁶ As the early decades of laser technology advanced, serious interest in the potential of directed-energy phenomena for use in military applications took root in DoD offices such as the Defense Advanced Research Projects Agency (DARPA). This interest culminated in March 1983 when President Reagan thrust the specter of such weapons onto the

³⁶ Theodore H. Mainman, "Optical and microwave optical experiments in Ruby," *Physical Review Letters*, Vol. 4, No. 11, 1960. Elias Snitzer, "Proposed Fiber Cavities for Optical masers," *Journal of Applied Physics*, Vol. 32, No. 1, 36, 1961. A fiber laser uses optical fibers doped with rare earth ions as the lasing or gain medium.

public stage with his now famous speech introducing the Strategic Defense Initiative (SDI).³⁷

The SDI program was predicated on the use of directed-energy weapons (DEW) to defeat large numbers of Soviet ballistic missiles launched against the United States. High-energy laser technologies such as space-based chemical lasers and nuclear explosive-generated x-ray lasers, as well as ground-based free-electron lasers, were promoted with great zeal in expectation of their eventual attainment of required performance parameters and subsequent critical role in a fielded system. However, the technological development of, and enthusiasm for, laser-based DEW soon experienced scientific as well as political setbacks. These setbacks curbed appetite for and the capability to produce DEW. Beginning in the late 1980s, caustic public debate over both the cost and plausibility of using DEW to defeat incoming missiles, coupled with a pessimistic assessment of their scientific merits in a 1987 American Physical Society report, led to a period of reduced interest in DEW technology.³⁸ But by the mid 1990s, advances in laser technology helped broaden interest to include military applications in remote sensing and counter-sensing that depend on *high-powered* laser technology, as well as expand prospects for DEW applications that rely on *high-energy* laser technology.³⁹

I. TECHNOLOGY OVERVIEW

Both high-energy and high-power lasers work by propagating electromagnetic energy—in the form of a beam of photons—at the speed of light. However, high-

energy lasers, or those whose *average power* is in the hundreds of kilowatts, are required for DEW, which work by destroying their targets. The U.S. Air Force's airborne laser (ABL) is the prime example of a real-world military application of this technology.⁴⁰ The ABL consists of a high-energy chemical oxygen iodine laser designed to destroy ballistic missiles by burning through their skin. Burning through a target at a distance requires high energy (kilojoules per pulse), high beam quality (minimal divergence),

and stability in beam transport and pointing mechanisms (jitter). With current laser technology, only chemical lasers can achieve the high-energy requirement needed for ABL-like DEW. High-energy chemical lasers are relatively large (comparable in size to



³⁷ President Reagan proposed SDI, often referred to as "Star Wars," to combat the threat of Soviet ballistic missiles. See Ronald Reagan, "Address to the Nation on Defense and National Security," March 23, 1983.

³⁸ In 1987, the American Physical Society (APS) convened a Study Group to address the state of the art in DEW in response to President Reagan's 1983 Star Wars initiative. The DEW Study Group provided a rather pessimistic assessment. The Group focused on the use of DEW in ballistic missile defense applications. The APS assessment of then-current state-of-the-art technology was published in an unclassified report and stated that despite the fact that DEW technology had made substantial progress during the preceding two decades, significant gaps in scientific and engineering understanding persisted. The group went further stating that insufficient information was available to determine whether or not the estimated required system performance parameters (principally laser power and beam quality, which were several orders of magnitude shy of their required values) could be achieved, and if so when. For an in depth summary of the report, see "Report to the APS of the Study Group on Science and Technology of Directed Energy Weapons: Executive Summary and Major Conclusions," *Physics Today*, May 1987.

³⁹ The technique of chirped pulse amplification (CPA) originally developed for radars was first applied to lasers in the mid 1980s. CPA is a means of amplifying the power in a pulse without suffering from negative non-linear pulse-distortion effects. See for example D. Strickland and G. Mourou, "Compression of amplified chirped optical pulse," *Optics Communications*, Vol. 56, 1985; and S. Sauteret, et al., "Generation of 20-TW pulses of picosecond duration using chirped-pulse amplification in a Nd:glass power chain," *Optics Letters*, Vol. 16, No. 4, 1991.

⁴⁰ See "ABL YAL 1A Airborne Laser, USA," Available at: <http://www.airforce-technology.com/projects/abl/>

an 18-wheeler truck) and complex systems, requiring associated power sources and extensive cryogenic cooling components. As such, they are not conducive to small-scale portable systems. For these reasons, while ABL-like systems are certainly within the capacity of several adversarial states to design and build, they are not the focus of this analysis because they are not deemed to be paradigm game-changers even on the chance that they are developed.⁴¹

By contrast, the term high-power lasers as used here refers to pulsed lasers whose *peak power* is tremendously high, on the scale of terawatts, but comes at a cost to its *average power*, which is very low compared with high-energy lasers, typically ranging from milliwatts to tens of watts.⁴² While high-power, pulsed lasers are not associated with DEW because they are not capable of delivering the energy needed to destroy a target, these directed-energy systems (as opposed to weapons) do open up a new realm of military applications to include remote sensing and counter sensing. Advances in small, portable high-power lasers have led to technical gains, increasing the likelihood that these lasers may be co-opted as game-changing weapons given the right combination of motivation, application, and technological breakthrough. Unfortunately, this potential holds true not only for states but also for groups and individuals.

For these reasons, the focus here is on the prospect that high-power lasers could be exploited for new applications where the emphasis is on laser system designs that are portable and relatively cheap (associated operational requirements such as cooling and power sources are not so great as to restrict access to military and government laboratories alone) and application areas that differ from the traditional weapon-like usage. Specifically, a class of lasers termed "ultrafast" lasers will be considered in detail for their potential to provide game-changing capability in applications such as the disruption of electro-optical (EO) and infrared (IR) sensors. When powerful laser technology is readily commercially available to individuals worldwide, the likelihood that creative exploits in laser usage will yield novel applications increases—simply because there are more opportunities (i.e., more individuals in possession of high-powered lasers) for experimentation. This phenomenon opens up a broad range of potential threats when adversaries develop novel applications. With the advent of nanotechnologies that facilitate relatively small, low-cost, high-power laser sources, coupled with their broad commercial availability, the potential for directed-energy systems to emerge in adversaries' hands is mounting.⁴³ However, this evolution in technology also presents opportunities for the United States and its allies in the form of creative defensive applications.⁴⁴

⁴¹ For information on Chinese directed-energy weapons, see Bruce W. McDonald, "China, Space Weapons, and U.S. Security," Council of Foreign Relations Report, No. 38, September 2008; Vago Muradian, "China Attempted To Blind U.S. Satellites With Laser," *Defense News*, September 28, 2006; "US claims that China has used lasers to attack satellites," *Jane's Defense Weekly*, October 16, 2006; Andrea Shalal-Esa, "China jamming test sparks U.S. satellite concerns," *Reuters*, October 5, 2006; and Elaine M. Grossman, "Top Commander: Chinese Interference with U.S. Satellites Uncertain," *Inside the Pentagon*, Vol. 22 No. 41, October 12, 2006.

⁴² For continuous wave (CW) lasers, there is effectively no pulse train, and the average power of the beam defines the system. But for a pulsed beam, the average power is the product of the peak power times the pulse width times the pulse repetition (prf) rate. Thus for a high prf beam (say 10^{15} pulses per second), high peak powers equate to low average powers and this means low total energy on target.

⁴³ A 2007 Defense Science Board report states that "The development of laser and high power microwave technologies and systems available to potential adversaries poses a new set of challenges to U.S. military force capabilities which must be better understood and tracked." See "The Defense Science Board Task Force on Directed Energy Weapons," Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., December 2007.

⁴⁴ This paper emphasizes the threat to Blue stemming from a potential surprise technological breakthrough in ultrafast laser technology in the hands of Red. There are corresponding "counter-threat" benefits to Blue from future applications of ultrafast laser technology such as enhanced capability for remote sensing, stand-off detection, and counter-sensing.

1.1 Science and Technology Developments in Ultrafast Lasers

Lasers convert energy used to excite their lasing medium into a stream of light or microwave photons of a specific wavelength or color. The process of exciting the device is termed "pumping." The light is comprised of photons of energy defined by the difference in energy between the initial excited state and the final lower energy state. While the energy may be fixed for a given laser system, if the laser is a pulsed laser, then varying the pulse width allows for control over the *peak power*, defined as the power per pulse.⁴⁵ The width or duration of the pulse is inversely proportional to the peak power. Thus, for a given laser energy, the shorter the pulse duration, the larger the peak power it contains. Ultrafast lasers are by definition high-power, pulsed lasers with very short pulse durations, typically in the picosecond (10^{-12} s) range. The name "ultrafast" derives from the fact that the pulses last such a short time that they are delivered in fast bullet-like bursts, as opposed to a continuous beam. Ultrafast lasers are synonymous with ultra-short, high peak-power pulses.

Ultra-short pulses can be generated from solid-state lasers of either bulk or fiber designs.⁴⁶ Bulk lasers use crystals or glass as the lasing medium, whereas fiber lasers make use of flexible fibers, as illustrated in **Figure 1**. A fiber-based design makes an attractive candidate for ultrafast lasers because fiber lasers offer relatively high efficiency, require little to no cooling for heat dissipation, and are small in size compared with traditional lamp-pumped Nd-YAG lasers.⁴⁷

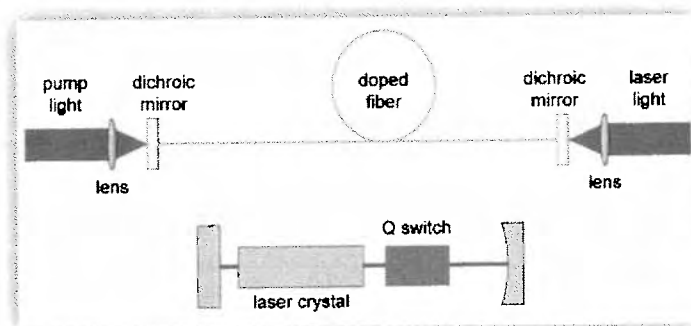


Figure 1: The upper diagram shows the schematic of a simple fiber laser. The Pump light is launched from the left-hand side through a dichroic mirror into the core of the doped fiber. The generated laser light is extracted on the right-hand side. The lower schematic shows the setup of a Q-switched bulk laser. The bulk components used are two mirrors, a laser crystal, and the Q switch. These diagrams are taken from the online Encyclopedia of Laser Physics and Technology. (Source: The online "Encyclopedia of Laser Physics and Technology" by Rudiger Pashotta.)

Recent advances in laser pulse compression techniques have led to fully functional ultrafast lasers with pulse durations down to the tens of femtoseconds (10^{-15} s). State-of-the-art technology is honing in on producing attosecond (10^{-18} s) pulse widths.⁴⁸ Reduction in pulse width (or equivalently, increases in peak power), coupled with breakthroughs in fiber laser technology over the last decade that have

⁴⁵ This is true for a Q-switched pulsed laser as opposed to cases where a continuous wave laser whose beam is converted to a pulsed beam external to the amplifying cavity.

⁴⁶ See, for example, Kyriakos Vlachos, et al., "Ultrafast Semiconductor-Based Fiber Laser Sources," *IEEE Journal of Selected Topics in Quantum Electronics*, Vol. 10, No. 1, pp. 147-154, Jan-Feb 2004; and C. Honninger, et al., "Ultrafast ytterbium-doped bulk lasers and laser amplifiers," *Applied Physics B*, Vol. 69, 1999, pp. 3-17.

⁴⁷ See Martin Richardson et al. page 15, wherein they state: "The footprint of a few kW fiber laser unit is ~6 sq ft versus 100 sq ft for a conventional lamp-pumped Nd:YAG laser."

⁴⁸ See for example: T. Eidam, et al., "57 W, 27 fs pulses from a fiber laser system using nonlinear pulse compression," *Applied Physics B-Lasers and Optics*, 2008; and Yi Wu, et al. "Isolated Attosecond Pulses Generated Directly from a Femtosecond Chirped Pulse Amplifier," *Optical Society of America*, 2009.

yielded an exponential increase in average power output for small portable lasers, are strong reasons to believe that ultrafast fiber laser technology has the potential to become game-changing in the relatively near future.⁴⁹

To be feasible for use as a directed energy system, a laser system must overcome technical issues as well as operational challenges. The two most pertinent technical issues concern beam output power and beam divergence. While laser light is collinear, all laser beams are subject to divergence due to the inherent wave-nature of light.⁵⁰ As the beam diverges over the range to the target, its intensity (power per surface area) decreases geometrically. Thus, even slightly divergent beams will suffer great reductions in power over large distances. Beam output power must be sufficient so as to render the desired target response, factoring in typical range to target, divergence issues, and atmospheric degradation. Once the technical challenges of generating the required beam characteristics are met, it must be operationally feasible to incorporate the laser in a larger system so as to carry out the intended mission. All laser systems confront operational barriers that constrain their use as directed-energy weapons or systems. In addition to potentially limiting properties of the laser system itself, such as its size, weight, cooling and power source requirements, one must also consider properties of the laser platform and operating environment. These include the ability to find, identify, and track the target (done by external means, but a more difficult problem for small scale mobile lasers operating in isolation), as well as the necessity of a highly precise and stable means of pointing and controlling the laser beam, which may be on a moving platform, such as the ABL, or a portable device requiring means of stabilization.

Not only have strides been made in the capability of ultrafast lasers, increasing both their average power and beam quality, but there have also been tremendous advances in understanding phenomena that result from material response to high-power, short-duration pulsed lasers. One such application concerns ultrafast laser-induced non-thermal changes in satellite sensors' optical characteristics, which could result in lasers being used to disrupt EO and/or IR satellite sensors. These changes could interfere with a satellite's ability to detect signals of interest from background noise. (This application would also require complementary and equally significant developments in laser platform, target tracking, and beam pointing techniques.) Should an adversary achieve a surprise technological breakthrough in this domain, it could be highly damaging to U.S. space assets.

1.2 Satellite Sensor Disruption

While ultrafast lasers do not have the energy to destroy a target by burning through its skin, they may prove useful at disabling certain vulnerable targets such as satellite sensors. This comes about due to non-thermal responses of semi-conductors exposed to the ultra-short pulses of moderately high power such as those generated from ultrafast lasers. **Figure 2** illustrates the time-scale for atomic

⁴⁹ Adrian Carter and Bryce Samson. "New Technology Advances Applications for High-power fiber lasers", Military and Aerospace Electronics; and Sze Y. Set et al. "Ultrafast Fiber Pulsed Lasers Incorporating Carbon Nanotubes," IEEE Journal of Selected Topics in Quantum Electronics, Vol. 10, No. 1 Jan-Feb, 2004.

⁵⁰ Actual laser beam divergence can be difficult to measure; however, a measure of the diameter of the beam footprint, d_p , at the target is related to the beam divergence, $\Delta\theta$, by: $d_p = 2r \tan(\Delta\theta/2)$, where r is the range to the target. For a range of 600 miles (the typical range to a LEO satellite), the footprint diameter is 55 feet for a 1mrad divergence at the laser. See, for example, Jie Shan and Charles K. Toth, eds., *Topographic Laser Ranging and Scanning: Principles and Processing*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2009, p. 244.

processes that occur when semi-conductor material undergoes excitation.⁵¹ The green bands correspond to different atomic processes where the onset of the process is indicated by the left-edge of the band, and the duration of the process is captured by the length of the band. As the time-scale decreases from microseconds (μ s), to nanoseconds (ns), to picoseconds (ps), to femtoseconds (fs), the dominating atomic processes experienced by an excited semiconductor go from thermal and structural effects such as heating and melting, which occur on the order of nanoseconds, to carrier removal, to thermalization, and lastly to carrier excitation.

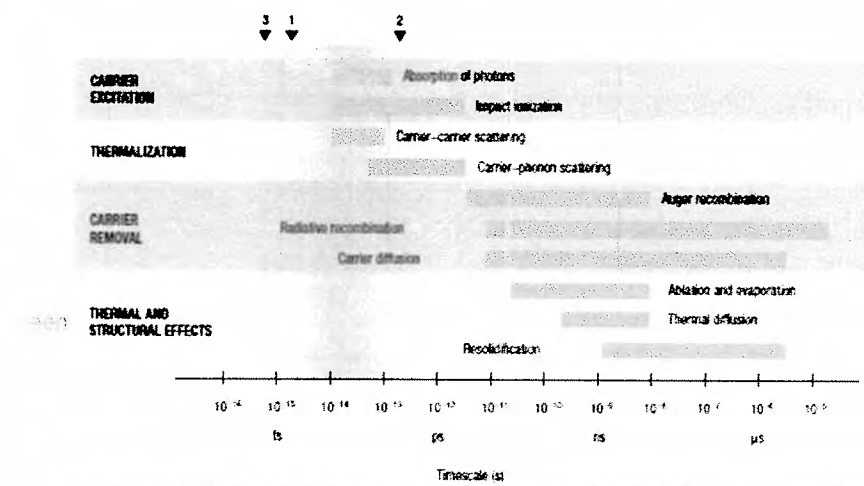


Figure 2. Timescales of various electron and lattice processes in laser-excited solids. The green bars represent an approximate range of characteristic times over a range of carrier densities from 10^{17} to 10^{22} cm^{-3} . The triangles at the top show state-of-the-art technology (circa 2008) in the generation of short pulses of electromagnetic radiation: 1 corresponds to 5 fs visible radiation; 2 corresponds to 120 fs x-ray radiation; and 3 corresponds to 0.5 fs far UV radiation. (Source: Figure from S.K. Sundaram and E. Mazur, "Inducing and probing non-thermal transitions in semiconductors using femtosecond laser pulses," *Nature Materials*, Vol. 1, December 2002.)

Of interest here are the non-thermal processes such as absorption of photons, scattering of photons, and impact ionization that take place in the sweet spot of fs to ps where ultrafast lasers operate. Such processes are initiated upon lattice excitation by ultra-short pulses and are of sufficiently short duration that the lattice relaxes before the onset of thermal and structural effects. These processes have the potential to alter temporarily the optical characteristics of semiconductors, namely the absorptivity, reflectivity, and transmittance, as well as affect the polarization characteristics. Thus, if they can be controlled and induced periodically, they pose an interesting means to disrupt or corrupt EO/IR sensor detection capability.⁵²

Future applications in which these fast, non-thermal responses are initiated in such a manner as to avoid the onset of thermal and structural changes could lead to temporal, fully reversible, disruption of semiconductor optical properties without necessarily destroying the sensor. With optical and IR sensors made from such

⁵¹ S.K. Sundaram and E. Mazur, "Inducing and probing non-thermal transitions in semiconductors using femtosecond laser pulses," *Nature Materials*, Vol. 1, December 2002.

⁵² Michael K. Rafailov, "Ultrafast Bandgap Photonics Semiconductor Phenomenology: Response to Ultra-short Pulse Laser," *International Society for Optics and Photonics, Proc. SPIE*, 7780, August 26, 2010.

semiconductor materials as HgCdTe, InSb, and InGaAs, application of IR sensor signal processing disruption via ultrafast laser technology could prove ideal because such interference could be done covertly and would be a means of selectively rendering space-based sensors inept without incurring space debris. Such future technology in adversaries' hands is cause for serious concern since the United States relies heavily on space-based satellites, many of which are highly vulnerable.

Technological advances in ultrafast laser technology

- ▶ Technological advances in fiber lasers have paved the way for higher and higher average power output, translating into even greater peak powers. Current continuous wave fiber lasers are capable of producing an average power on the order of one to ten kilowatts, while pulsed, ultrafast fiber lasers have average power from 10 to 100 watts.⁵³
- ▶ Advances in mode locking and pulse compression techniques to produce very short duration pulses, have pushed the envelope for pulse width down to the tens of femtoseconds.⁵⁴
- ▶ Small size, portability, reduced cost, and commercial availability are characteristics that would make ultrafast fiber lasers attractive for individual use.⁵⁵

Outstanding operational challenges

- ▶ Operational challenges confronting a fielded system capable of interfering with EO/IR sensors remain significant. Most notably, target identification and track for mobile, covert lasers operated by individuals without access to means to track satellites remains one of two major obstacles to targeting space-based assets. The second significant obstacle is beam divergence. Laser beam output power levels for ultrafast lasers are still too low to overcome atmospheric effects on beam divergence for long-distant targets.

1.3 Present-Day Accessibility

There are two parallel but competing processes taking place in the realm of high-powered laser technology that relate to their accessibility. On one hand, small portable lasers are becoming increasingly more powerful and their relatively low cost and commercial availability leads to reduced barriers to entry for the individual. These factors make it more likely that individuals seeking to acquire lasers for use either in criminal activity or terrorist plots will have greater power at their disposal and the potential to inflict greater harm. However, the ability to generate sophisticated effects with ultrafast lasers requires equally sophisticated laser subsystems. Therefore, the use of ultrafast laser technology to disrupt satellite sensors, even for future capabilities, is considered more likely to come from state-based threats rather than terrorist groups. While the barrier to obtaining an ultrafast laser may be significantly reduced for the individual, operating it to cause EO/IR sensor damage would be impossible without accompanying platforms. Yet, the nature of the upward trend in availability of ever more powerful lasers in the hands of individuals makes ripe the potential for both technological breakout and surprise

⁵³ Martin Richardson, Timothy McComb, and Vikas Sudesh, "High Power Fiber Lasers and Applications to Manufacturing," Conference Proceedings 1047, Laser and Plasma Applications in Materials Science, edited by E.H. Amara, S. Boudjemai, and D. Dournaz, American Institute of Physics, 2008.

⁵⁴ Ja-Hon Lin, et al. "Ultrashort Pulse Compression for Mode-Locked Ti:Sapphire Laser by Using a Tapered Fiber and Grating Pair," *Japanese Journal of Applied Physics*, Vol. 49, 2010.

⁵⁵ In 2008, Martin Richardson, et al. stated that the "high power fiber laser market, currently estimated to be ~\$200M, is predicted to grow at 25% for the next several years." They went further to cite B. C. Gahan, and B. Shiner, "New high-power fiber laser enables cutting-edge research," *GAS TIPS*, pp. 29-31, Winter, (2004), for their estimates circa 2004 "that during the typical lifetime of a source, the total cost of ownership of a fiber laser is about one-third that of a similar CO₂ or solid-state device."

stemming from novel usage. For example, today 1W lasers can be purchased commercially over the Internet for as little as a few hundred dollars.⁵⁶ While these are continuous-wave (CW) beams, their availability to the ordinary citizen increases the probability for novel use of these hand-held lasers.

1.4 Timeline

- ▶ Handheld 1W CW lasers in hands of individuals are currently possible.
- ▶ A wide range of fiber lasers is available globally from IPG Photonics.⁵⁷

2. GAME-CHANGING QUALITIES

Based on its potential applications, ultrafast laser technology is assessed to have the following "game-changing" qualities:

- ▶ **Reduced Barriers to Entry:** The availability of small, portable, increasingly powerful lasers on the open market has coincided with an upswing in the use of such lasers to illuminate U.S. domestic aircraft in flight. Indeed, the Federal Aviation Association tracks and maintains a database of such events, which it reports to the FBI and local law enforcement agencies.⁵⁸ In one highly publicized case, a man in New Jersey was arrested and convicted for shining a handheld Class IIIa 5-milliwatt green laser into the cockpit of a chartered jet, temporarily blinding and distracting the pilots in their approach to Teterboro Airport. The laser was commercially available, and at least 100,000 were sold in the United States in 2004.⁵⁹ While these incidents have been criminal in nature, it is easy to visualize the potential for terrorist usage. Clearly the trend toward increased laser power packaged in smaller, portable devices leads to significant reduction in the barriers to entry, especially as these devices are readily commercially available and currently fairly weakly regulated.
- ▶ **System Integration:** See Novel Delivery Means below.
- ▶ **Novel Delivery Means:** States with advanced laser technology and the capability to place satellites in orbit (Russia, China, as well as a host of allies) might be motivated to place small lasers in space. Small, light, relatively low-powered ultrafast lasers embedded as components on satellite systems would represent a technological breakthrough needed to overcome beam divergence issues in disrupting satellite sensors.
- ▶ **Self-propagation:** N/A.⁶⁰
- ▶ **Novel Radical Empowerment:** High-power lasers in the hands of adversaries, coupled with future technological advances that mitigate current operational limitations, could provide them with radical empowerment much the way traditional fire-powered arms (e.g., rifles) empowered the individual.
- ▶ **Mitigation of Effects:** High-power ultrafast lasers can be used to negate effects for both Red and Blue opponents. For Red, lasers could be used in

⁵⁶ For example, Wicked Lasers produces the Spyder II Pro Arctic laser, a hand-held, 1W max power CW blue laser available online for about 300 dollars. This laser produces a blinding beam and is capable of burning flesh. It has a transmit path of over four miles. Wicked Lasers advertises shipment to any country in the world.

⁵⁷ See IPG Photonics 2009 Annual Report for a good overview of their fiber laser products and customer base.

⁵⁸ Madelyn I. Sawyer and John P. Sullivan, "Laser Weapons: An Emerging Threat," FBI Law Enforcement Bulletin, Quantico, VA, April 2008, pp. 18-21.

⁵⁹ John Keller, "Laser Pointer or Terrorist Threat," Editor's Notebook-Optoelectronics Watch, *Military and Aerospace Technology*, February 2005, p. 16.

⁶⁰ It is understood that the term "self-propagation" is considered in reference to lasers as an entity and not to the fact that laser beams propagate in air. Lasers as a class of weapon do not self-propagate.

the future to negate the capability of U.S. drones, aircraft, and satellite communications systems. While not addressed in this paper, ultrafast lasers in the nano and pico-second range, can be used to negate the effects of illicit transportation of chemical, biological and explosive materials into U.S. ports and at border cross points by remote sensing for the presence of such materials.⁶¹ Global society as a whole demonstrates fairly strong resistance to the weaponization of space, a domain viewed as part of the global commons, much like international waters. While this opposition to space-based weapons and war may be an inhibitor of DEW, it also can serve as a motivator for more covert means of populating space with directed energy systems for use in countering satellite communication systems.

- **Diverse Applicability:** Lasers in general are a diverse technology in that they have enabled advances in a wide range of scientific and industrial application areas from medicine, with the use of laser surgical procedures, to manufacturing and industrial applications such as cutting, welding and precision drilling, to practical everyday applications such as barcode readers found at grocery store checkout counters. Ultrafast laser technology, while quite specific, does lend itself to a range of applications related to sensing and counter-sensing.

3. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY DEVELOPMENT

Recent interest and funding for high-energy and high-powered laser technology has suffered from the above counter-driver—namely the lack of concerted focus on military applications in light of technological setbacks and failure to achieve “buy-in” that directed-energy laser weapon and defense capabilities offer unique niches. A recent Defense Science Board report on DEW concluded that “[t]he most fundamental issue affecting priority for developing and fielding laser and microwave/millimeter wave systems useful to combatant command missions is the need for cost-benefit analysis supporting priority choices.”⁶² The need is exacerbated by two underlying issues. Directed-energy weapons suffer from a history of overly optimistic expectations, which in some cases led to cancelling other competing programs that provided the needed capability via alternative methods. The second reason for the need for cost benefit analysis is that for many proposed laser applications, “there are competing and well understood conventional approaches to produce the desired effect.”⁶³ In light of the history of failed attempts at lasers, these conventional approaches are more credible to warfighters and force providers.

But this reason for the lull in U.S. directed-energy technological development will not necessarily be operative in other states. In fact, China would realize great gains from pursuing directed-energy programs because it does not possess comparable conventional means and, more importantly, there exists an asymmetry in vulnerability between China and its presumed strategic rival. The United States, with its huge dependence on space-based systems, is highly vulnerable; China, lacking comparable space assets, is not. At least until China achieves something approaching parity with the United States in space assets, this asymmetry will figure heavily in the former’s weapons programs.

⁶¹ Sara Wallin, et.al. “Laser-based Standoff Detection of Explosives: A Critical Review,” *Analytical and Bioanalytical Chemistry*, Vol. 395, 2009, pp. 259-274; and Jennifer L. Gottfried, et al. “Standoff Detection of Chemical and Biological Threats Using Laser-Induced Breakdown Spectroscopy,” *Applied Spectroscopy*, Vol. 62, No. 4, 2008.

⁶² “The Defense Science Board Task Force on Directed Energy Weapons,” Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, December 2007. p. xi.

⁶³ Ibid, p. x.

Lasers are already ubiquitous. There are many kinds of lasers used in a variety of applications, and they are widely available commercially. However, using lasers as space-based weapons, or simply to wage war in space, has many political dimensions. Strong international resistance exists to infringement of a nation's right to explore space. One need only recall the international condemnation that followed China's 2007 anti-satellite (ASAT) test and the United States' subsequent 2008 satellite shoot-down.⁶⁴ U.S. space policy is based on a set of principles, goals, and guidelines that it recommends other nations will adopt.⁶⁵ International space law is not fully formed. However, even if it were, formal policies would have no power to prevent non-state actors from perpetrating acts of "space piracy." Thus, while normative forces exist and seek to constrain state behavior *vis-à-vis* space weaponization policy, these forces would have little bearing on non-state actors.

4. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY ATTRACTIVENESS

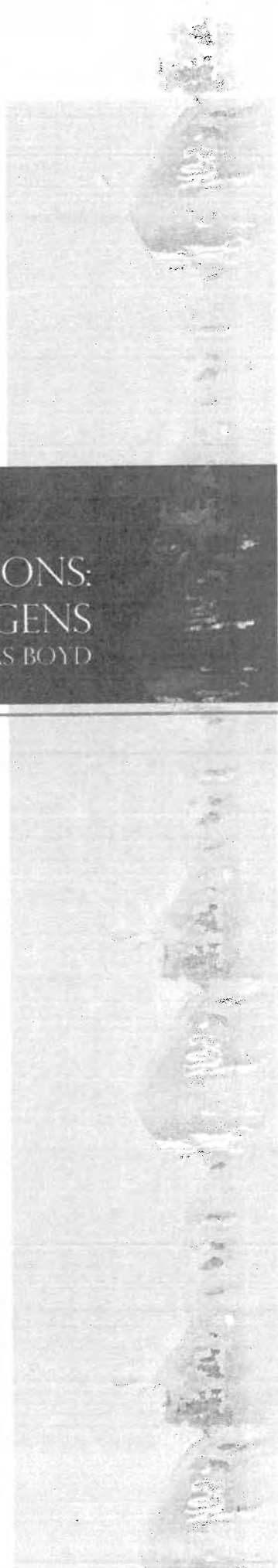
Relatively small, inexpensive and powerful ultrafast lasers would be attractive to adversarial states seeking to undermine U.S. space-based supremacy. Non-state actors such as terrorist groups might be enticed to pursue such systems for use in a tactical environment. In the timeframe under consideration in this report—6-20 years into the future—it is conceivable that such devices might be assembled from readily commercially available components. Novel uses for such lasers would almost certainly emerge. The uses suggested here, namely satellite sensor disruption, could be covertly undertaken, making directed-energy systems attractive to states that wish to appear as complying with international law. The efficacy of such weapons in the hands of adversaries, given the current U.S. asymmetry in space-based assets, would be high. From the U.S. vantage point, ultrafast laser technology for military applications may play a heightened role in defensive capabilities such as standoff detection and remote sensing. Technology to counter the effects from directed-energy technology would also be of considerable interest to the United States.

5. CONCLUSION: RELEVANCE TO DTRA MISSION

The history of laser development is one of stunningly rapid development. At their birth in 1960, lasers were identified as a tool in need of an application, whereas today lasers are nearly ubiquitous in applications ranging from grocery store scanners to medical instrumentation to metal-cutting and surveying devices. Given this history, there is sufficient momentum in the field of research and the density of science and technology suggests that it is ripe for future breakthrough developments. Both DHS and DTRA currently have research and development programs that address practical applications of these advances in ultrafast laser technology, and DTRA should continue to pursue these. Small, cheap, widely available lasers on the open market make it critical for DTRA to keep abreast of potential technological leaps, both in terms of new applications that DTRA may want to partake in, as well as potential game-changing threats from the nation's adversaries.

⁶⁴ See Gregory Kulacki and Jeffrey G. Lewis, "Understanding China's Antisatellite Test," *Nonproliferation Review*, Vol/15, Issue 2, July 2008. p. 335-347.

⁶⁵ National Space Policy of the United States of America, June 28, 2010.



ADVANCED BIOLOGICAL WEAPONS: GENETICALLY ENGINEERED PATHOGENS

DALLAS BOYD

*"Have you walked up and down upon the earth lately? I have;
and I have examined Man's wonderful inventions. And I tell you
that in the arts of life man invents nothing; but in the arts of death
he outdoes Nature herself, and produces by chemistry and
machinery all the slaughter of plague, pestilence, and famine."*

— George Bernard Shaw, "Man and Superman," 1903

INTRODUCTION

Of the multitude of terrorist threats facing the United States, two categories of weapons—biological agents and nuclear weapons—occupy a rarified class in their capacity to produce mass casualties. Save for the most imaginative, well-executed attacks on critical infrastructure, no other weapons have the potential to inflict comparable destruction.⁶⁶ Fortunately, acquiring or developing a nuclear weapon presents a formidable challenge to terrorists. Biological agents, by contrast, are understood to be far more accessible to malevolent actors. Relative to nuclear arms, only modest facilities are required to prepare them, and laboratories with dual-use functionality are proliferating across the globe. Lab technicians' educational backgrounds need not be terribly advanced to manipulate biological agents for nefarious purposes. Further, the fact that there are very few signatures associated with the production of these weapons complicates efforts to detect their development.

⁶⁶ The DHS *National Infrastructure Protection Plan* describes a category of attacks that do not involve WMD but employ the use of "components of the Nation's [critical infrastructure and key resources] as weapons of mass destruction," which could have "even more devastating physical, psychological, and economic consequences" than WMD themselves. This definition was presumably included to cover attacks such as the 9/11 hijackings. See *National Infrastructure Protection Plan*, Department of Homeland Security, 2009.

Finally, biological agents can be introduced to a target population using relatively simple means of delivery. For these reasons, bioweapons are arguably the more worrisome of the two threats.⁶⁷

The use of organic life as an instrument of warfare dates to antiquity.⁶⁸ Several accounts of the practice survive from ancient times—poisoning wells with toxic plants, driving plague-infected animals onto enemy lands, and hurling jars filled with snakes and scorpions at enemy soldiers.⁶⁹ In the Middle Ages, various attempts were made to infect enemy populations with disease. During the siege of Caffa in 1346, for example, plague-infested corpses were catapulted over the city walls, exposing inhabitants to the bacteria.⁷⁰ The use of biological agents in the modern era has

been similarly gruesome and has occurred on a vastly greater scale. During World War II, Japan's use of cholera, typhoid, anthrax, and plague is believed to have killed hundreds of thousands of Chinese.⁷¹

Though biological weapons remained in the arsenals of several nations for decades, revulsion at the prospect of their use ultimately led to the 1972 Biological and Toxin Weapons Convention (BWC).⁷² This accord sought to prohibit the development, manufacture, and stock-piling of biological agents for military use. However, the BWC lacked a verification regime to monitor compliance, and a number of states maintained clandestine weapons programs in contravention of the agree-

ment. Most notable among these was the Soviet Union, whose secret *Biopreparat* program produced massive quantities of pathogens for offensive use in the 1970s and 1980s, including anthrax, bubonic plague, Q fever, smallpox, tularemia, influenza, and the Marburg and Ebola viruses.⁷³ Another violator was apartheid-era South Africa, which initiated a secret program to develop offensive biological and chemical warfare capabilities.⁷⁴



⁶⁷ This assessment is consistent with DTRA literature concerning the agency's efforts on Chemical and Biological Defense: "Nuclear warheads are not the only weapons of mass destruction threatening the United States and our allies. Because nuclear weapons require sophisticated technologies and elements difficult to obtain, our nation's adversaries may find chemical and biological weapons more attractive."

⁶⁸ For numerous historical examples of biowarfare dating to ancient times, see National Research Council, *Biotechnology Research in an Age of Terrorism*, Washington, D.C.: The National Academies Press, 2004, pp. 19-21, 33-34.

⁶⁹ Adrienne Mayor, *Greek Fire, Poison Arrows & Scorpion Bombs: Biological and Chemical Warfare in the Ancient World*, New York: Overlook Duckworth, 2004.

⁷⁰ Mark Wheelis, "Biological Warfare at the 1346 Siege of Caffa," *Emerging Infectious Diseases*, Vol. 8, No. 9, September 2002.

⁷¹ See Sheldon H. Harris, *Factories of Death: Japanese Biological Warfare 1932-45 and the American Cover-Up*, Routledge, 1994. See also Wendy Barnaby, *The Plague Makers: The Secret World of Biological Warfare*, Frog Ltd, 1999; and Nicholas D. Kristof, "Unmasking Horror—A Special Report: Japan Confronting Gruesome War Atrocity," *New York Times*, March 17, 1995.

⁷² The formal name of the BWC is the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction.

⁷³ Ken Alibek and Stephen Handelman, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World—Told from Inside by the Man Who Ran it*, New York: Hutchinson, 1999.

⁷⁴ Chandré Gould and Peter Folb, "Project Coast: Apartheid's Chemical and Biological Warfare Programme," United Nations Institute for Disarmament Research, February 2003.

Terrorist attempts to develop biological agents have been considerably less advanced, attempted attacks using these weapons have been rare, and successful efforts rarer still. Of these, perhaps the most frequently cited is a 1984 event that is often described as the first bioterrorist attack in U.S. history.⁷⁵ In this incident, religious cultists deposited the bacterium *Salmonella typhimurium* in several restaurant salad bars in rural Oregon.⁷⁶ Though no fatalities resulted, 751 people reported illness resulting from the attack. However, the modest results of this and other attacks have not dampened the fears of many U.S. leaders and members of the general public, for whom the threat of biological weapons is an enduring concern. Yet, as alarming as biological weapons are in their "traditional" form, national security analysts have increasingly focused on the possibility that evolutionary leaps in biowarfare capability will occur. The focus of the following analysis is the potential for the development of highly advanced weapons whose effects depart substantially from the paradigmatic biological threat as it is presently understood.

I. TECHNOLOGY OVERVIEW

I.1 Genetically Engineered Biological Weapons

As virulent as many pathogens are in their natural state, advances in the life sciences hold the potential to make them still more harmful in the future. During the 1980s and 1990s, analysts began to grow concerned that vastly more potent bioweapons could be created through genetic engineering. In particular, enhancements were thought possible to increase their survivability, infectiousness, lethality, and/or resistance to treatment.⁷⁷ According to one analysis during this period, genetic engineering capabilities "raise the specter that known biological agents can be altered to create more invasive or faster-acting organisms, agents that thwart prophylactic medical defenses, or agents that are hardier and more robust when sprayed into the environment or loaded into munitions."⁷⁸ Other qualities might include greater difficulty of detection, improved safety of handling, and increased ease of dissemination.⁷⁹

In 1989, the defection of Soviet microbiologist Vladimir Pasechnik, who had served as the director of *Biopreparat's* Institute for Ultra Pure Biological Preparations, alerted U.S. authorities to the USSR's research on genetically engineered weapons.⁸⁰ After the Cold War ended, additional information came to light that revealed the horrifying scope of Soviet research. In one experiment, for example, a Soviet microbiologist combined the gene of the bacterium diphtheria with plague or tularemia

⁷⁵ W. Seth Carus, "Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900," Center for Counterproliferation Research, National Defense University, Washington, D.C. August 1998. See also W. Seth Carus, "The Rajneeshees," in Jonathan B. Tucker, ed., *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, Cambridge: The MIT Press, 2000.

⁷⁶ *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*, New York: Vintage Books, 2008. See also Judith Miller, William Broad, and Stephen Engelberg, *Germs: Biological Weapons and America's Secret War*, New York: Simon & Schuster, 2002. pp. 1-34.

⁷⁷ Michael J. Ainscough, "Next Generation Bioweapons: The Technology of Genetic Engineering Applied to Biowarfare and Bioterrorism," Counterproliferation Papers, Future Warfare Series No. 14, USAF Counterproliferation Center, Air University, Maxwell AFB, Alabama, April 2002.

⁷⁸ Seth Shulman, "Biohazard: How the Pentagon's Biological Warfare Research Program Defeats Its Own Goals," Center for Public Integrity, 1993.

⁷⁹ Stephen M. Block, "Living Nightmares: Biological Threats Enabled by Molecular Biology," in Sidney Drell, Abraham D. Sofaer, and George D. Wilson, eds., *The New Terror: Facing the Threat of Biological and Chemical Weapons*, Stanford, CA: Hoover Institution Press, 1999. p. 46-47.

⁸⁰ Tom Mangold and Jeff Goldberg, *Plague Wars*, New York: St. Martin's Press, 1999. As cited in Michael J. Ainscough, "Next Generation Bioweapons: Genetic Engineering and BW," in Jim A. Davis and Barry R. Schneider, eds., *The Gathering Biological Warfare Storm*, April 2002.



bacteria to create a hybrid biological agent, or “chimera.”⁸¹ Such information slowly began to shape U.S. scenario planning. By 1998, the media reported on a top-level exercise—code-named “Dark Winter”—designed to test the government’s response to a biological attack; the agent posited in the exercise was a genetically engineered hybrid of smallpox and Marburg virus.⁸² A year later, the Hart-Rudman Commission warned that developments in biotechnology could lead to the creation of genetically engineered pathogens that could “thwart most antibiotics and vaccines, and readily outcycle our detection, antidote development, and distribution timelines.”⁸³

After the 9/11 attacks, distress over biological weapons in general, and genetically engineered agents in particular, reached fever pitch.⁸⁴ Indeed, physicist Stephen Hawking suggested that scientific advances could lead not only to the deaths of large numbers of people but to the very extinction of the human species. “In the long term, I am more worried about biology,” he said. “Nuclear weapons need large facilities, but genetic engineering can be done in a small lab... The danger is that either by accident or design, we create a virus that destroys us.”⁸⁵ This risk was powerfully illustrated in the late 1990s by a group of Australian scientists conducting pest control research.⁸⁶ In a now infamous experiment, the scientists inserted the interleukin-4 gene into the mousepox virus with the aim of producing an “infectious contraceptive” for mice.⁸⁷ Rather than sterilizing the subjects, however, the modified mousepox killed them, including many mice that had been immunized against the unaltered form of the virus. The implications were ominous—a similar modification could potentially yield vaccine-resistant viruses that are lethal to humans, including smallpox.⁸⁸

In recent years, concern over advanced biological weapons has been fueled by what biologist Malcolm Dando has described as a “riotous development” of biotechnology.⁸⁹ As a measure of the government’s anxiety, the JASON Defense Advisory Panel has produced three classified reports on the subject in the last six years

⁸¹ David E. Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and its Dangerous Legacy*, New York: Random House, 2009, p. 296.

⁸² Judith Miller and William J. Broad, “Exercise Finds U.S. Unable to Handle Germ War Threat,” *New York Times*, April 25, 1998.

⁸³ *New World Coming: American Security in the 21st Century—Supporting Research and Analysis*, Phase I Report of The United States Commission on National Security/21st Century, September 15, 1999.

⁸⁴ Ironically, in a 1999 memo to an associate, unearthed after the U.S. invasion of Afghanistan, al-Qaeda second-in-command Ayman al-Zawahiri conceded that “[d]espite their extreme danger, we only became aware of [biological and chemical weapons] when the enemy drew our attention to them by repeatedly expressing concerns that they can be produced simply with easily available materials.” See Alan Cullison, “Inside Al-Qaeda’s Hard Drive,” *Atlantic Monthly*, September 2004. Zawahiri may have been referring to the media deluge that followed then-Secretary of Defense William Cohen’s 1997 appearance on the ABC’s “This Week,” in which he held aloft a five-pound bag of sugar and asserted that an equivalent quantity of anthrax could kill half the population of Washington, D.C. One account of Cohen’s performance described the press response thusly: “The media took off from there, with a frenzy of television and press stories about the horrors of possible anthrax, smallpox, or plague attacks.” See Jeanne Guillemin, *Anthrax: The Investigation of a Deadly Outbreak*, University of California Press: 2001, p. 248.

⁸⁵ Roger Highfield, “Colonies in Space May Be Only Hope, Says Hawking,” *Daily Telegraph*, October 16, 2001.

⁸⁶ Ronald J. Jackson, et al., “Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox,” *Journal of Virology*, Vol. 75, No. 3, 2001.

⁸⁷ Michael J. Selgelid and Lorna Weir, “The Mousepox Experience,” *EMBO reports* 11, December 11, 2009, pp. 18-24.

⁸⁸ Selgelid and Weir, op. cit.

⁸⁹ Jeremy Lovell, “Report Warns of Failure to Control Biological Weapons,” *Reuters*, October 26, 2004.

alone.⁹⁰ It has become commonplace to observe that absent the most robust safeguards, and perhaps in spite of them, scientific progress will confer upon U.S. adversaries the means to conduct biowarfare far in excess of currently understood capabilities. The following analysis examines a theoretical class of weapons on the far edges of science: genetically engineered weapons that target specific ethnic or national groups. Considerable disagreement exists among experts over the plausibility of such weapons. However, given the potentially radical impact of this capability, examining the security implications of its development is only prudent.

1.2 Ethnic-specific Genetic Weapons

Shortly after 9/11, former President George W. Bush enumerated the threats facing the United States in a dangerous new era, of which the specter of biological attack was among the most worrisome. In a comment that was then uncontroversial, he observed that infectious diseases “make no distinctions among people and recognize no borders.”⁹¹ However, it is theoretically possible that advances in the life sciences may one day render President Bush’s assertion false. That is, biological weapons may be developed that *do* make distinctions between people, afflicting certain groups on the basis of distinct genetic characteristics. The implications of this possibility are far-reaching. Little imagination is required to envision how these weapons might figure in ancient ethnic-based rivalries, as well as many other applications.

There is a rough historical precedent for using biological agents to target members of a specific ethnic group. During Pontiac’s Rebellion in 1763, British officers attempted to break the siege of Fort Pitt in Pennsylvania by providing smallpox-infected blankets to hostile Native Americans.⁹² The Indians’ lack of natural immunity to the virus made them particularly susceptible to infection. Repeating anything resembling this tactic in the modern era would be impossible without highly specialized research and development, and it is not clear that even significant scientific advances would enable the capability due to variations in genetic profiles. Nevertheless, a small but alarmed group of scientists has speculated that as understanding of human genetics advances, it may be possible to identify unique markers that are carried exclusively, or perhaps simply disproportionately, by members of particular ethnic groups. This information could conceivably allow weapons to be developed that would target only the carriers of distinct, ethnic-specific DNA markers such as single nucleotide polymorphisms (SNPs), gene deletions, or gene duplications.



Dr. Jacob M. Appel, the author of one of the more thorough analyses of ethnic-specific weapons, suggests that “the ways in which bioweapons may be targeted against specific ethnic, racial and cultural groups are as broad as humanity’s scien-

⁹⁰ The publicly available titles of these reports are: “Synthetic Viruses” (JSR-07-508, 2007), “Emerging Viruses” (JSR-05-502, 2005), and “BioEngineering” (JSR-05-130, 2005). For a comprehensive list of JASON study titles, see: <http://www.fas.org/irp/agency/dod/jason/>

⁹¹ Statement by George W. Bush, “Strengthening the International Regime against Biological Weapons,” The White House, Office of the Press Secretary, November 1, 2001.

⁹² Fred Anderson, *Crucible of War: The Seven Years’ War and the Fate of Empire in British North America, 1754-1766*, New York: Knopf, 2000. pp. 541-542.

tific imagination.”⁹³ One possibility he suggests is that a naturally occurring pathogen such as the Ebola virus might be engineered to attack only those with specific markers.⁹⁴ Another application involves exploiting the distinctive proteins of the immune system, which sometimes cluster in particular ethnic groups. According to Appel, an agent might be engineered to sabotage victims’ disease-suppressing capabilities by “knocking out cells containing particular molecular tags, much as HIV destroys helper T cells, thereby creating an entire population susceptible to opportunistic infections.”⁹⁵ Yet another approach concerns the creation of pathogens that compromise the effectiveness of particular medications in a target population.⁹⁶

The notion that pathogens might be manipulated to target specific ethnic groups was first broached in the 1960s. An early discussion of targeting populations based on shared genetic characteristics was presented in a 1970 article entitled, “Ethnic Weapons,” by Carl A. Larson, then head of the Department of Human Genetics at Sweden’s University of Lund.⁹⁷ While Larson’s piece focused on chemical rather than biological weapons, he observed that common, genetically-based reactions to drugs in certain populations could be exploited for offensive purposes. Mentions of ethnic-specific weapons, in both the national security and popular literature, occurred periodically over the next two decades. By the late 1980s, the public’s awareness of genetic science had risen, and stories highlighting the “dark side” of this research began to appear more frequently.

A 1988 piece in the *Los Angeles Times* referred to new “offensive visions” stimulated by biotechnology that included “organisms or toxins custom-made to ... prey upon an adversary’s ethnobiological characteristics.”⁹⁸ In a more scholarly treatment of the subject, in 1993 the Stockholm International Peace Research Institute’s (SIPRI) annual *Yearbook* examined the malign applications of genetic advances.⁹⁹ According to the study, “Theoretically, if...investigations provide sufficient data on ethnic genetic differences between population groups, it may be possible to use such data to target suitable micro-organisms to attack known receptor sites for which differences exist at cell membrane level or even to target DNA sequences inside cells by viral vectors...”¹⁰⁰

Former Secretary of Defense William Cohen was perhaps the first senior official to discuss the subject in public. In 1997, Cohen referred to speculation that malevolent scientists were “trying to devise certain types of pathogens that would be ethnic-specific so that they could just eliminate certain ethnic groups and races.”¹⁰¹ The

⁹³ Jacob M. Appel, “Is All Fair in Biological Warfare? The Controversy over Genetically Engineered Biological Weapons,” *Journal of Medical Ethics*, Vol. 35, 2009.

⁹⁴ Ibid.

⁹⁵ Ibid.

⁹⁶ Ibid.

⁹⁷ Carl A. Larson, “Ethnic Weapons,” *Military Review*, U.S. Army Command and General Staff College, Vol. L, No. 11, November 1970.

⁹⁸ Daniel Kevles, “The Rebirth of American Biological Warfare,” *Los Angeles Times*, May 8, 1988.

⁹⁹ See *SIPRI Yearbook 1993: World Armaments and Disarmament*, Stockholm International Peace Research Institute, 1993.

¹⁰⁰ See Tamas Bartfai, et al., Appendix 7A: “Benefits and Threats of Developments in Biotechnology and Genetic Engineering,” *SIPRI Yearbook 1993*. Additionally, a 1996 background paper for the Fourth Review Conference of the BWC noted that “It cannot be ruled out that information from [the sequencing of the human genome] could be considered for the design of weapons targeted against specific ethnic or racial groups.” However, the paper acknowledged that it is “far from clear that the development of such weapons could ever be anything more than a theoretical possibility.” See Background Paper on New Scientific and Technological Developments Relevant to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Geneva, Switzerland, October 30, 1996.

¹⁰¹ William S. Cohen, “Terrorism, Weapons of Mass Destruction, and U.S. Strategy,” Sam Nunn Policy Forum, University of Georgia, April 28, 1997.

following year, a highly controversial piece appeared in London's *Sunday Times* claiming that the State of Israel was developing a "genetically modified bacterium or virus" that would affect exposed Arabs but not Jews.¹⁰² A scathing editorial in the *New York Post* followed, which quoted an eminent genetic researcher's assessment of the notion as "totally fantastical."¹⁰³ However, other experts were less dismissive. University of Scranton scientist Dr. Victor Delvecchio claimed that the concept of an "ethno-bomb" was at least "theoretically possible."¹⁰⁴ Dr. Vivienne Nathanson, head of science and ethics at the British Medical Association (BMA), concurred, noting that "It will unfortunately be possible to design biological weapons of this type when more information on genome research is available."¹⁰⁵ In 1999, the BMA released a report, *Biotechnology, Weapons, and Humanity*, which asserted that "weapons could theoretically be developed which affect particular versions of genes clustered in specific ethnic or family groups."¹⁰⁶ The report provided the following elaboration:

Over the last few decades, rapid advances in molecular biology have allowed the heritable material (DNA) of different organisms to be interchanged. The Human Genome Project and the Human Genetic Diversity Projects are allowing the identification of human genetic coding and differences in normal genetic material between different ethnic groups.

During the review conferences on the [BWC], an increasing level of concern has been expressed by national governments over the potential use of genetic knowledge in the development of a new generation of biological and toxin weapons.

Legitimate research into microbiological agents, relating both to the development of agents for use in, for example agriculture, or to improve the medical response to disease causing agents, may be difficult to distinguish from research with the malign purpose of producing more effective weapons.¹⁰⁷

A second volume of the report released in 2004 renewed the concern, asserting that the ability to create genetic weapons is "now approaching reality."¹⁰⁸ Contrasting claims about the plausibility of ethnic-specific weapons are issued with some regularity. The more skeptical of these should caution against undue alarmism over the possibility that these weapons will be developed.

In 2004, Dr. David Goldstein, Director of Duke University's Center for Human Genome Variation, asserted that developing an effective weapon to distinguish between ethnic groups is "just not going to happen." Because ethnic groups are so similar, he asserts, high selectivity is simply out of the question. "The best you would probably do," Goldstein argued, "is something that kills 20% of one group and 28% of another."¹⁰⁹ A year later, however, Jacques Forster, vice-president of the International Committee of the Red Cross (ICRC), suggested that the "potential to target a

¹⁰² Uzi Mahnaimi and Marie Colvin, "Israel Planning 'Ethnic' Bomb as Saddam Caves In," *Sunday Times*, November 15, 1998.

¹⁰³ "Now Playing: A Blood Libel for the 21st Century," *New York Post*, November 22, 1998.

¹⁰⁴ Jeff Stein, "Debunking the Ethno-Bomb," *Salon*, December 2, 1998.

¹⁰⁵ Ethirajan Anbarasan, "Genetic Weapons: A 21st-Century Nightmare?" *UNESCO Courier*, March 1999.

¹⁰⁶ British Medical Association, *Biotechnology, Weapons, and Humanity*, Harwood Academic Publishers, 1999.

¹⁰⁷ Ibid.

¹⁰⁸ British Medical Association, *Biotechnology, Weapons, and Humanity II*, BMA Professional Division Publications, October 2004.

¹⁰⁹ David Adam, "Could You Make a Genetically Targeted Weapon?" *Guardian*, October 28, 2004.

particular ethnic group with a biological agent is probably not far off." This possibility was "not the product of the ICRC's imagination," he insisted, but rather had been confirmed by "countless independent and governmental experts."¹¹⁰

Ethnic-specific weapons would require considerable advances in mankind's basic understanding of the human genome, and in particular the systematic mapping of inter-ethnic genetic distinctions. It has been well established that certain genetic disorders appear more frequently in members of particular ethnic populations. For example, sickle cell anemia, an autosomal genetic blood disorder, is more prevalent in people of African and Mediterranean heritage. Cystic fibrosis occurs in roughly one in 2,500 Europeans but appears in only one in 90,000 Asians.¹¹¹ Tay-Sachs disease, a recessive autosomal genetic disorder, afflicts mainly Ashkenazi Jews.¹¹² Future advances in the understanding of the human genome will inevitably reveal additional ethnic-specific genetic information. Indeed, a 2010 study by the JASON Defense Advisory Panel reported that researchers will soon have "an enormous amount of data to use in the challenging effort to link genotypes with phenotypes of interest."¹¹³

Knowledge of genetics has advanced over the previous two decades under efforts such as the Human Genome Project. Begun in the 1990s, this project was launched to determine the sequence of the chemical base pairs that comprise DNA and identify the more than 20,000 genes of the human genome. In 2003, at the conclusion of the Human Genome Project's effort to map the complete genome, it was confirmed that the more than three billion chemical base pairs were 99.9 percent identical in every human being.¹¹⁴ The study of the remaining 0.1 percent was the purpose of the more controversial Human Genome Diversity Project, launched by Stanford University's Morrison Institute, which has been the key scientific vehicle for this undertaking.¹¹⁵ Similar research efforts include the International HapMap Project and the 1,000 Genomes Project.¹¹⁶

2. GAME-CHANGING QUALITIES

Based on their potential applications (which are discussed more extensively in Section 3 below), ethnic-specific biological weapons are assessed to have the following "game-changing" qualities:

- ▶ **Reduced Barriers to Entry:** The extent to which barriers to genetically engineered bioweapons are lowered will depend on the diffusion of genetic research around the world. For the most part, research in this field is restricted to a small number of well-funded and responsible research institutes. As this research becomes more widespread, and as the relevant knowledge expands to a greater number of facilities and individuals, opportunities to harness scientific advances for malevolent purposes will increase. With regard to ethnic-specific bioweapons, advances in the knowledge of the human genome—particularly those related to shared genetic

¹¹⁰ Jacques Forster, "Preventing the Use of Biological and Chemical Weapons: 80 Years On," International Committee of the Red Cross, delivered at the International Seminar on the Biological and Chemical Weapons Threat, October 6, 2005.

¹¹¹ Race & Genetics FAQ, National Coalition for Health Professional Education in Genetics, (undated).

¹¹² Dina Shiloh, "The DNA Dilemma," *Jerusalem Post*, August 8, 1997.

¹¹³ "The \$100 Genome: Implications for the DoD," JASON Report No. JSR-10-100, December 2010.

¹¹⁴ "Whole Genome Association Studies," National Genome Research Institute, National Institutes of Health. Last Reviewed: February 8, 2010.

¹¹⁵ L. Luca Cavalli-Sforza, "The Human Genome Diversity Project: Past, Present and Future," *Nature Reviews*, Vol. 6, April 2005.

¹¹⁶ The International HapMap Consortium, "The International HapMap Project," *Nature*, Vol. 426, December 18, 2003.

3.2 Counter-Drivers

The following discussion concerns factors that might militate against the development and/or use of genetically engineered biological weapons by state and sub-state actors. These factors include both capabilities-based constraints such as access to technology, as well as normative considerations.

3.2.1 Terrorist Capabilities

Salafist-jihadists' ambitions to develop biological weapons are well documented.¹¹⁹ In 2005, for example, an al-Qaeda web site featured a document entitled "Biological Weapons," which discussed the use of pneumonic plague as a terror weapon and examined methods of delivering biological agents using an aerosol system.¹²⁰ Fortunately, al-Qaeda's ability to produce even rudimentary biological weapons has not matched its ambitious rhetoric. In 2006, Charles E. Allen, then Chief Intelligence Officer of DHS, described terrorist capabilities in this domain as "crude and relatively unsophisticated," with no indications to suggest an imminent increase in their capabilities.¹²¹ This conclusion appears to track with assessments of al-Qaeda's earlier attempts to produce biological agents. Following the fall of the Taliban in 2001, U.S. forces discovered that al-Qaeda had established rudimentary chemical and biological programs in Afghanistan.¹²² Though foreboding as a reflection of their intent, these programs were generally assessed to have been amateurish.

Arguably more worrisome than the danger posed by terrorist networks is the threat from a skilled "insider"—an individual who, for reasons of religious fervor, ideological motivation, or mental illness, uses legitimate biotechnology facilities for malefic purposes. This description probably fits Dr. Bruce Ivins, the deceased U.S. Army microbiologist who is suspected of committing the 2001 anthrax attacks.¹²³ Another avenue to obtaining biological expertise is to recruit scientific personnel from states that maintain or previously operated biological warfare programs. Scientists from the former Soviet Union are a perennial source of concern given the declining need for their expertise and their sporadic pay. According to Michael J. Ainscough, "Unless [terrorists] are able to buy knowledge or microbe cultures from large programs such as the former Soviet BW program, it is unlikely...that [they] would have access to or produce genetically engineered biologicals."¹²⁴ Even more advanced weapons, including theoretical ethnic-specific weapons, will almost certainly be inaccessible to all but the most sophisticated state-run weapons programs. As Jacob M. Appel notes, the development of such weapons "will not be the product of 'backyard

¹¹⁹ Salafism refers to the radical Sunni movement, of which al-Qaeda is but one part, that advocates returning to the form of Islam practiced by the Prophet Muhammad's companions and the two generations of believers that followed them.

¹²⁰ Steve Coll and Susan B. Glasser, "Terrorists Turn to the Web as Base of Operations," *Washington Post*, August 7, 2005.

¹²¹ Charles E. Allen, testimony before the House Homeland Security Subcommittee on Prevention of Nuclear and Biological Attack hearing "Bioscience and the Intelligence Community: Closing the Gap, Part II," May 4, 2006.

¹²² Alan Cullison, "Inside Al-Qaeda's Hard Drive," *Atlantic Monthly*, September 2004. Several makeshift "laboratories" to develop these agents were identified in Afghanistan. Additionally, U.S. personnel detected traces of anthrax bacteria in several buildings in that country, including Ayman al-Zawahiri's home in Kabul. See Sammy Salama and Lydia Hansell, "Does Intent Equal Capability? Al-Qaeda and Weapons of Mass Destruction," *Nonproliferation Review*, November, 2005; and "Al-Qaeda: Anthrax Found in al-Qaeda Home," *Global Security Newswire*, December 10, 2001.

¹²³ See Carrie Johnson, Carol D. Leonnig, and Del Quentin Wilber, "Scientist Set to Discuss Plea Bargain in Deadly Attacks Commits Suicide," *Washington Post*, August 2, 2008; and Carrie Johnson, Del Quentin Wilber, and Dan Eggen, "Evidence Against Scientist Detailed," *Washington Post*, August 7, 2008.

¹²⁴ Michael J. Ainscough, "Next Generation Bioweapons: The Technology of Genetic Engineering Applied to Biowarfare and Bioterrorism," Counterproliferation Papers, Future Warfare Series No. 14, USAF Counterproliferation Center, Air University, Maxwell AFB, Alabama, April 2002.

differences between population groups—will make the development of such weapons less formidable to groups below the state level.

- ▶ **System Integration:** N/A.
- ▶ **Novel Delivery Means:** Several of the theoretical applications of genetic weapons (e.g., targeting a particular individual using a genetically tailored weapon, activating a latent illness with an external cue, etc.) represent novel delivery means. While the symptoms they produce may be familiar, the method of discriminating between targeted populations or triggering an illness after a period of dormancy would signify a genuinely innovative means of attack.
- ▶ **Self-propagation:** Communicable viruses are by definition self-propagating. While some pathogens, such as the bacterium *Bacillus anthracis* (anthrax), are not transmissible from individual to individual, an adversary seeking to achieve the effects described in this section (e.g., infecting a particular ethnic group) would in all likelihood rely on a communicable agent.
- ▶ **Novel Radical Empowerment:** Achieving the capability to carry out, or simply threaten to carry out, a biological attack using a genetically engineered biological agent would confer considerable status to the perpetrator. Depending on the virulence of the agent and the breadth of its spread, the consequences of such an attack could be of unprecedented magnitude.
- ▶ **Mitigation of Effects:** One of the more troubling *theoretical* characteristics of genetically engineered biological agents is the potential ability to overcome vaccines and thus afflict even the most well prepared population.
- ▶ **Diverse Applicability:** N/A.

3. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY DEVELOPMENT

3.1 Drivers

A 2006 joint committee of the National Research Council and the Institute of Medicine, known as the Lemon-Relman Committee, sought to identify, *inter alia*, the “current scientific trends and the likely trajectory of future research activities in public health, life sciences, and biomedical and materials science” that are relevant to the development of “next generation” biological agents in the next five to ten years.¹¹⁷ As part of this effort, the committee enumerated a number of interacting forces, or “drivers,” that will influence “innovation in life sciences-related technologies and the rapid global dispersion of these technologies.” These drivers include the following:

- ▶ Economic forces such as the cost of labor, state-level R&D investment, and “shifting geographic trends in consumerism and purchasing power”;
- ▶ Social forces such as activities in the First World to capitalize on health and agricultural biotechnology and nanotechnology to increase quality of life; and
- ▶ Political forces such as the efforts by various countries (e.g., Mexico and Singapore) to establish biotechnology as an economic pillar of their economies.¹¹⁸

¹¹⁷ Stanley M. Lemon and David A. Relman, Co-Chairs, *Globalization, Biosecurity, and the Future of the Life Sciences*, Committee on Advances in Technology and the Prevention of their Application to Next Generation Biowarfare Threats, Institute of Medicine and National Research Council, Washington, D.C.: National Academies Press, 2006.

¹¹⁸ *Globalization, Biosecurity, and the Future of the Life Sciences*, 2006. pp. 79-80.

invention' but will require the investment of considerable intellectual capital from the best scientific minds in the world."¹²⁵

3.2.2 Regulation

Given the BWC's lack of a verification regime, little can be done to prevent clandestine state-level development of genetically engineered biological weapons. (One notable exception involves an often-overlooked potential source for such weapons: U.S. government laboratories. Christian Enemark and Ian Ramshaw argue that government-sponsored research into countermeasures against advanced biological weapons—research that “necessarily involves the production of genetically modified microorganisms”—may have catastrophic unintended consequences. In addition to producing stores of dangerous pathogens, which might be inadvertently or deliberately released, this research endows a greater number of individuals with the specialized knowledge to produce advanced weapons. This population may include one or more malicious insiders who could use the knowledge for destructive purposes.¹²⁶) Notwithstanding this exception, security policies would probably have the greatest relative effect in the private domain, where establishing a culture of security-consciousness is an ongoing challenge.

In 2006, the National Science Advisory Board for Biosecurity, which was established to provide security guidance related to life science research, recommended that a formal regulatory structure be established for the synthetic biology industry.¹²⁷ This has not yet occurred. However, in response to concerns over genetically engineered weapons, various voluntary approaches have been pursued to scrutinize commercial orders for certain DNA sequences. Several private DNA synthesis firms have used software to compare these orders against the DNA sequences of particularly dangerous pathogens, subjecting orders that match to secondary inspection.¹²⁸ Also in 2006, several American companies attempted to coordinate these practices under the International Consortium for Polynucleotide Synthesis, which was developed to “promote the development and adoption of corporate best practice with regard to safety and security in synthetic biology.”¹²⁹ In 2007, several German firms attempted to do the same. These efforts were followed by a joint U.S.-European initiative in 2009 to establish a “Code of Conduct for Best Practices in Gene Synthesis”¹³⁰; however, this attempt stalled over the question of using a human arbiter in the secondary phase of inspection, which adds additional expense to the process.¹³¹

With respect to the development of ethnic-specific biological weapons, the most obvious policy countermeasure would be to restrict the dissemination of ethnic-specific genomic information. However, attempts to do so would likely run afoul of the scientific community, whose members often bristle at the suggestion that scientific openness should be constrained by security concerns. For example, one of the researchers involved in the Australian mousepox experiment defended their

¹²⁵ Jacob M. Appel, “Is All Fair in Biological Warfare? The Controversy over Genetically Engineered Biological Weapons,” *Journal of Medical Ethics*, Vol. 35, 2009.

¹²⁶ Enemark and Ramshaw, op. cit. See also Jonathan B. Tucker, “Biological Threat Assessment: is the Cure Worse than the Disease?” *Arms Control Today*, Vol. 34, No. 8, 2004.

¹²⁷ Malcolm Dando, “Synthetic Biology: Harbinger of an Uncertain Future?” *Bulletin of the Atomic Scientists*, August 16, 2010.

¹²⁸ Dando, op. cit.

¹²⁹ Hans Bügl, et al., “A Practical Perspective on DNA Synthesis and Biological Security,” International Consortium for Polynucleotide Synthesis, December 4, 2006.

¹³⁰ Dando, op. cit.

¹³¹ Dando, op. cit.

publication on the grounds that "Anything scientifically interesting should be published."¹³²

Another possibility is the development of a voluntary self-regulatory culture among scientists that emphasizes "normative awareness." As Enemark and Ramshaw note, "With so many technological and professional factors driving open and free exchanges of knowledge, it would be too difficult for governments to impose a top-down scheme of legal regulation." A more effective approach, they argue, would entail a "bottom-up fostering of awareness of the need to balance science and security."¹³³

4. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY ATTRACTIVENESS

4.1 Drivers

4.1.1 The Psychological Effect of Biological Weapons

A characteristic that makes biological weapons attractive to certain terrorists is the potentially long duration of their effects. Biosecurity expert Michael Osterholm describes the use of biological agents as having a potential "echo impact" in the form of illnesses that persist for weeks after an attack. For contagious agents, in which transmission occurs in multiple generations, these weapons represent a "bomb that continues to go off."¹³⁴ Unlike the effects of an attack with explosives, which are finite and therefore psychologically manageable for survivors, in the case of a biological release, members of the targeted population would lack confidence that they had escaped the initial attack. Confronting the uncertain spread of disease would produce anxiety and possibly panic.



The most obvious application of ethnic-specific biological agents would be their use as terror weapons, in which one group seeks to kill or terrorize members of another group for whom it has antipathy.

4.1.2 Utility as Offensive Weapons

Apartheid-era South Africa initiated the country's notorious chemical and biological weapons (CBW) program—code-named Project Coast—sometime around May 1981.¹³⁵ During the "truth and reconciliation" period that followed the collapse of apartheid, the government officials who had launched the program pointed to the Soviet and Cuban threat as its initial catalyst.¹³⁶ However, as Project Coast expanded, more

¹³² Michael J. Selgelid and Lorna Weir, "The Mousepox Experience," *EMBO reports* 11, December 11, 2009. See also the following defense of scientific openness by the former president of the National Academy of Sciences: Bruce Alberts, "Modeling attacks on the food supply," *Proceedings of the National Academy of Sciences*, Vol. 102, No. 28, July 12, 2005.

¹³³ Enemark and Ramshaw, *op. cit.* See also the "Hourglass Initiative," whose mission, *inter alia*, is to "Promote codes of ethical conduct, education, and outreach efforts among scientists, engineers, and technologists to limit the spread of [WMD]." Available at: <http://www.hourglassinitiative.com/>.

¹³⁴ "Interview with Dr. Michael Osterholm," PBS Frontline, October 1998.

¹³⁵ Stephen F. Burgess and Helen E. Purkitt, "The Rollback of South Africa's Chemical and Biological Warfare Program," USAF Counterproliferation Center, Air War College, April 2001. p. 3.

¹³⁶ At the time, South African forces were heavily engaged in the Angolan civil war. Concern was widespread that chemical weapons might be deployed against South African personnel and that effective

nefarious capabilities were pursued. According to historians Stephen F. Burgess and Helen E. Purkitt, these included the use of chemical and biological agents as internal counter-insurgency weapons, tools for political assassination, and ultimately as a means of controlling the population of black South Africans.¹³⁷ This undertaking involved genetic engineering research whose purpose, Burgess and Purkitt recount, was to “produce a ‘black bomb,’ bacteria or other biological agents that would kill or weaken blacks and not whites. The black bomb could be used to wipe out or incapacitate an entire area where an insurrection was taking place.”¹³⁸ However, there is no evidence to suggest that this research produced anything approaching a workable weapon.

4.1.3 Utility as Delayed-onset Weapons

Another potential application of genetically engineered agents is the use of delayed-onset weapons. Several experts have suggested that populations could be exposed to biological agents that would not produce physiological effects until activated by some other stimulus. Dr. Christopher Davis, a former member of Britain’s Defense Intelligence, describes theoretical weapons that “affect the genes of a person by exposing them to a material which may work, over a very long period of time, on its own by attaching itself to the DNA in the cell or it may simply sit there until you expose them to another material at a time that you choose, which locks together with the first material and affects the genome...”¹³⁹ In this application, a genetically engineered virus might mimic the characteristics of several naturally occurring viruses (e.g., herpes simplex virus) whose effects remain latent until triggered. An individual infected with herpes might show no symptoms until certain stimuli such as sunlight or stress triggers an outbreak.¹⁴⁰

The strategic implications of this capability would be considerable. Assuming the author of a delayed-onset attack is an entity with political objectives, the threat of activating such a virus would serve as a potent tool for blackmail.¹⁴¹ The leaders of an infected population could be compelled to undertake, or refrain from undertaking, certain actions lest the symptoms be triggered. This capability would be especially useful as an instrument of deterrence, where freedom of military action is constrained by the threat to activate a weapon. Jacob M. Appel offers another chilling delayed-onset effect: “Advances in genetics make it theoretically possible to create weapons that might act in the manner of gene therapy, only in reverse, making the offspring of those affected susceptible to various forms of cancer or even precocious senility.”¹⁴² Given the extremely long delay in the manifestation of these effects, to say nothing of the extraordinary cruelty of targeting victims not yet born, one cannot imagine any use for this capability except its use as a terror weapon.

4.1.4 Utility as Assassination Weapons

Genetic weapons also offer the theoretical possibility to target a specific individual for illness or death with a weapon specifically tailored to his or her unique genetic fingerprint. This application might be thought of as the reverse of “personalized medicine,” the postulated medical trend in which therapies are custom-designed for

defenses against these agents must be developed. See Chandré Gould, *South Africa’s Chemical and Biological Warfare Programme 1981-1995*, Doctoral dissertation, Rhodes University, August 2005.

¹³⁷ Burgess and Purkitt, op. cit. p. 17.

¹³⁸ Ibid. p. 21.

¹³⁹ “Interview with Dr. Christopher Davis,” PBS Frontline, October 1998.

¹⁴⁰ Jon Cohen, “Designer Bugs,” *Atlantic Monthly*, July/August 2002.

¹⁴¹ Michael J. Ainscough, “Next Generation Bioweapons: Genetic Engineering and BW,” in Jim A. Davis and Barry R. Schneider, eds., *The Gathering Biological Warfare Storm*, April 2002.

¹⁴² Appel, op. cit.

individuals based on their distinct genetic makeup.¹⁴³ The following scenario describes the method:

Assassins seek to take down a world leader, but they won't need to risk using bullets or bombs. Instead, they stand on a receiving line and shake the leader's hand, coming away with a genetic sample—a fleck of skin, a stray hair—that reveals his secret vulnerabilities. Then they engineer a pathogen that will attack only the dignitary. The next time he addresses a crowd, one terrorist simply coughs, releasing the pathogen-loaded virus into the air. It circulates silently, a contagion harmless to all but its target. Within hours, the leader is dead.¹⁴⁴

Of the weapon applications discussed in this analysis, it is probably reasonable to conclude that this possibility is among the least technologically feasible. However, the attractiveness of this capability—to malevolent actors as well as respectable governments—may be a significant driver of its development. Terrorists and fanatics have long favored the assassination of political leaders. Many governments, scrupulous and unsavory, have also relied on the method for reasons spanning the spectrum of legitimacy. Despite the general disreputability of assassination, a moral case can arguably be made that the selective targeting of terrorist leaders or drug kingpins is more humane than conventional military operations to kill or capture them, which often produce collateral civilian deaths.¹⁴⁵ Consider the cases of Panamanian dictator Manuel Noriega, Somali warlord Mohamed Farrah Aidid, and Iraqi dictator Saddam Hussein; the removal of each resulted in substantial unintended loss of civilian life.

4.1.5 Utility as Defensive Weapons

While most postulated applications of ethnic-specific weapons are sinister, legitimate uses of these weapons are at least conceivable. For example, Jacob M. Appel suggests that such weapons “may have particular value in defensive warfare, as they offer the prospect of defeating an invading army of a different ethnic background without risking significant damage to one's own citizenry.”¹⁴⁶ Of course, this possibility would only exist in conflicts between states of dissimilar ethnic composition, such as a Russian defense against a Chinese invasion. Appel also raises the possibility that genetic weapons might have intriguing geopolitical effects by conferring a particular advantage to ethnically heterogeneous states (e.g., the United States) over largely homogeneous ones (e.g., China), thereby altering the global balance of power.¹⁴⁷

¹⁴³ See, for example, H.W. Willard and G.S. Ginsburg, *Genomic and Personalized Medicine*, Academic Press, 2009; and Lisa A. Haile, “Making Personalized Medicine a Reality,” *Genetic Engineering & Biotechnology News*, Vol. 28, No. 1, 2008.

¹⁴⁴ Erik Baard, “The DNA Bomb: Modified Crops Are In The Crosshairs Now. You May Be Next,” *Village Voice*, May 15, 2001.

¹⁴⁵ In 1976, President Gerald Ford signed E.O. 11905: United States Foreign Intelligence Activities, which stipulated that “No employee of the United States Government shall engage in, or conspire to engage in, political assassination.” The order came in response to public disclosures of previous CIA assassination plots against Cuban dictator Fidel Castro, Congolese Prime Minister Patrice Lumumba, and other figures. Two subsequent Executive Orders (E.O. 12036: United States Foreign Intelligence Activities, signed by President Jimmy Carter in 1978, and E.O. 12333: United States Intelligence Activities, signed by President Ronald Reagan in 1981) reiterated that “No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination.” In 2008, President George W. Bush signed E.O. 13470: Further Amendments to Executive Order 12333, United States Intelligence Activities, amending E.O. 12333 to strengthen the role of the Director of National Intelligence. The existing ban on assassinations was preserved in the amendment.

¹⁴⁶ Appel, *op. cit.*

¹⁴⁷ Appel, *op. cit.*

In May 2007, Russia's Federal Customs Service announced a ban on the export of blood and human tissue samples from Russia.¹⁴⁸ A variety of theories were presented to explain the curious ban; one suggested that the order was prompted by fears that Western nations could produce genetic weapons for use against specific nations. This notion was reportedly communicated to then-President Vladimir Putin by the Federal Security Service (FSB), the successor of the KGB.¹⁴⁹ An article in the Russian newspaper *Kommersant* described the FSB report as containing "a wealth of fantastical details about the development of 'ethnically oriented' biological weapons capable of rendering Russia's population sterile and even killing it off."¹⁵⁰ The restriction on the availability of Russian biomaterials was intended to thwart the development of "anti-Russian biological weapons."¹⁵¹ (Russian media outlets quickly pointed out the absurdity of the ban, with one noting that "strictly speaking, any Russian travelling abroad is biological material."¹⁵² Aleksey Moshchan, the deputy director of the Federal Centre of Children Haematology and Oncology, described the genetic weapon explanation as "the silliest of all possible theories."¹⁵³) Nevertheless, the perception that such research is occurring in the West might prompt Russia's famously paranoid decision-makers to direct the country's considerable biomedical infrastructure to pursue its own genetic weapons.

4.2 Counter-Drivers

4.2.1 Biological Agents as Indiscriminate Weapons

Perhaps the most compelling argument against the use of biological weapons, and therefore the most operative counter-driver to their development, is the inability to confine outbreaks of disease to a discrete population (excepting, of course, non-transmissible pathogens such as anthrax). For example, in an offensive battlefield context, a military force that employed biological agents might risk exposing its own personnel. For this reason, a certain inexplicability has attached to state-run offensive biological weapons programs. Of course, indiscriminate infection is less troublesome for terrorists. Yet, even terrorist groups might be less inclined toward such weapons if they fully understood their implications. Indeed, in 2007, game theorist Thomas Schelling discussed several of the uncertainties surrounding terrorists' attraction to bioweapons. In particular, he wondered whether they understood the inability to contain the spread of certain viruses, a characteristic that made these weapons unattractive to military strategists during the Cold War:

Three years ago there was a lot of interest in, and concern about, the use of smallpox as a weapon. I was involved in a meeting that included a number of bioweapons experts, and after considerable discussion, I asked how long it would take for a smallpox epidemic deliberately started in the U.S. to spread around the world. The answer was "Not long." Then how practical are infectious diseases as bioweapons? Is it

¹⁴⁸ Svetlana Osadchuk, "Customs Blocks Export of Blood and Tissue," *Moscow Times*, May 31, 2007. See also Terry Macalister, "Russian Ban on Body Parts Exports Hits Drug Testing Firm," *Guardian*, June 5, 2007.

¹⁴⁹ Vasilij Vlassov, "Russian Clinical Research is Threatened by Ban on Export of Samples," *British Medical Journal*, Vol. 334, June 16, 2007.

¹⁵⁰ "Russian Federal Customs Service Halts Export of Human Biological Materials," *Moscow Kommersant* in English, May 30, 2007, OSC CEP20070530950003.

¹⁵¹ "Confusion surrounds reported Russian ban on human tissue exports," *NTV Mir Moscow* (Russian language) May 20, 2007, OSC CEP20070530950452. See also Yulia Taratuta, "40,000 Patients to Suffer due to Ban on Biomaterials Export," *Kommersant Moscow* (Russian language), May 31, 2007, OSC CEP20070531950031.

¹⁵² "Confusion surrounds reported Russian ban on human tissue exports," *NTV Mir Moscow* (Russian language) May 20, 2007, OSC CEP20070530950452.

¹⁵³ "Senior Russian medic condemns ban on human tissue export," *Moscow Vesti TV* (Russian language), May 31, 2007, OSC CEP20070531950505.

really likely that terrorists in the Middle East would use smallpox against a neighbor? Because of these considerations the interest in infectious diseases as weapons... has declined. But I was struck by the fact experts in bioweapons are not strategists, and by the thought that if *our* experts hadn't thought of this, could we be sure that others, including terrorist organizations, had?¹⁵⁴ [Emphasis in original].

Yet, it cannot be assumed that a full appreciation of the uncontrollable spread of biological agents would foreclose the option, even to a rational actor. A state or terrorist movement that has much less to lose than its more advanced enemy, or simply values human life less as a culture, may elect to use bioweapons in spite of the danger they pose to its own people.¹⁵⁵ As biophysicist Steven Block notes,

In the past it was argued that no one would want to release a contagious disease that killed a third of all the individuals on the planet. You'd be shooting yourself in the foot. But a country like Afghanistan loses a third of its population, and after mourning the loss of so many individuals, the country goes on pretty much as it did. An agrarian nation remains an agrarian nation. A developed country has farther to fall. Society as we know it would come to a grinding halt if we suffered such a significant loss of population. Therefore the release of an incredibly lethal contagious disease would perversely level the playing field. And in this new world order some of the undeveloped countries might have a better crack at the big time than they do under the current status.¹⁵⁶

In the case of ethnic-specific biological weapons, Jacob M. Appel notes that "the history of human migration and genetic mixing means that individual [genetic] markers rarely if ever are distributed entirely along racial or ethnic lines." Assuming that 100 percent selectivity cannot be achieved, the danger of self-inflicted injury to one's own people would therefore have to be considered. However, given what Appel calls the "unsentimental cost-benefit comparisons of military planners," an agent that kills 70 or 80 percent of an enemy force, while harming only 20 or 30 percent of the attacker's personnel, might still be deployed in dire circumstances.¹⁵⁷

4.2.2 Biological Agents as "Taboo" Weapons

Among the greatest inhibitions on the use of biological weapons is the historical "taboo" surrounding their use.¹⁵⁸ This prohibition seems to derive from the vague perception that casualties caused by living organisms are somehow more ghastly

¹⁵⁴ Michael Spence, "Mr. Counterintuition: America is Safer with Sophisticated Enemies," *Wall Street Journal*, February 17, 2007.

¹⁵⁵ The suggestion that certain cultures value human life less strongly than others is admittedly controversial. Further, historical episodes offered as evidence of a callous attitude toward human suffering (e.g., the famines in the USSR and China during the reigns of Stalin and Mao, respectively) may reflect the cruelty of a leader or political system rather than the humanity of the culture in question. Nonetheless, one can argue with some confidence that the casualty aversion of several eastern cultures simply does not approach that of the United States and other western European nations. A widely reported incident in 1996 appears to support this hypothesis. During a discussion with former Assistant Secretary of Defense Chas Freeman, several Chinese military officers suggested that China would be prepared to sacrifice "millions of men" and "entire cities" in a conflict over Taiwan and that the United States would not demonstrate similar resolve. See Patrick E. Tyler, "As China Threatens Taiwan, It Makes Sure United States Listens," *New York Times*, January 24, 1996. This threat was reminiscent of a remark by Saddam Hussein during a 1990 meeting with then-U.S. Ambassador April Glaspie, in which the dictator famously warned, "Yours is a society which cannot accept ten thousand dead in one battle." See Dan Reiter and Allan C. Stam, *Democracies at War*, Princeton University Press: 2002. pp. 21-22.

¹⁵⁶ Jon Cohen, "Designer Bugs," *Atlantic Monthly*, July/August 2002.

¹⁵⁷ Appel, op. cit.

¹⁵⁸ For a discussion of the biological weapons taboo, see Phillip M. McCauley and Rodger A. Payne, "The Illogic of the Biological Weapons Taboo," *Strategic Studies Quarterly*, Spring 2010.

than those resulting from flying bits of metal. Yet for the groups assumed to be most apt to conduct biological attacks—jihadists and other apocalyptic religious groups, deranged individuals, and possibly the most radical environmentalists—aversion to mass killing is not an operative concern. Alone among these groups, jihadists have something resembling a constituency—the global Muslim *ummah*, or “community of believers”—whose revulsion they may wish to avoid.

Jihadist propagandists have taken pains in recent years to underscore the religious legitimacy of indiscriminate killing. Clerical water carriers have produced a number of religious rulings to justify not only the killing of civilians but also the deaths of fellow Muslims in the course of attacks; these edicts require no special elaboration.¹⁵⁹ What is worth noting, however, is that some evidence indicates al-Qaeda’s growing sensitivity to popular disgust over civilian deaths. In 2007, an influential Egyptian jihadist known as Dr. Fadl released a lengthy manuscript denouncing jihadist violence.¹⁶⁰ Ayman al-Zawahiri was forced to defend al-Qaeda’s methods, which he admitted had not been “free of error.”¹⁶¹ Al-Qaeda’s acquisition of bio-weapons should therefore not be treated as synonymous with their use. Furthermore, there is reason to believe that the network would be mindful of the high risk of a backlash following the use of such weapons.

4.2.3 Lack of Necessity for Advanced Biological Weapons

An obvious disincentive to producing genetically engineered bioweapons is that many natural pathogens simply require no improvement. That is, they are sufficiently lethal in their unaltered state as to obviate the complicated processes required to produce enhancements. Consider, for example, the lethality of the smallpox virus. Since the World Health Organization declared smallpox eradicated in 1979, vaccinations have largely ceased among civilians around the world, and natural immunities have diminished.¹⁶² Consequently, the global population is highly susceptible to the virus. An outbreak anywhere would likely have catastrophic, global consequences, raising the question of what additional benefit terrorists would gain by making the virus even more virulent.¹⁶³ Of course, this logic did not dissuade Soviet leaders from ordering

¹⁵⁹ After several esteemed Islamists condemned the 9/11 attacks, al-Qaeda responded in 2002 with a religious justification for killing civilians. Like many jihadist rationalizations for such deaths, the document cites the Prophet Muhammed’s siege of Ta’if in 630, which involved the use of a catapult. According to al-Qaeda’s interpretation of this episode, it is “allowed for Muslims to kill protected ones among unbelievers when [the Muslims] are using heavy weapons that do not distinguish between combatants and protected ones...” See “A Statement from Qaidat al-Jihad Regarding the Mandates of the Heroes and the Legality of the Operations in New York and Washington,” April 24, 2002. Another widely quoted edict is a 2003 *fatwa*, believed to have been commissioned by al-Qaeda, that sanctions the killing of as many as 10 million “infidels.” See Nasir bin Hamid al Fahd, “A Treatise on the Legal Status of Using Weapons of Mass Destruction Against Infidels,” May 21, 2003.

¹⁶⁰ Lawrence Wright, “The Rebellion Within,” *New Yorker*, June 2, 2008. Other denunciations of jihadist slaughter have appeared with some regularity in recent years. In 2007, Saudi cleric Salman al-Ouda issued a scathing personal indictment of Osama bin Laden on a major Middle Eastern television network. “My brother Osama, how much blood has been spilt?” he asked. “How many innocent people, children, elderly, and women have been killed...in the name of al-Qaeda?” See Peter Bergen and Paul Cruickshank, “The Unraveling: The Jihadist Revolt Against bin Laden,” *New Republic*, June 11, 2008.

¹⁶¹ The florid full title of Zawahiri’s rebuttal is *The Exoneration: A Treatise Exonerating the Community of the Pen and the Sword from the Debilitating Accusation of Fatigue and Weakness*. See “Zawahiri Tries to Clear Name, Explain Strategy,” Transnational Security Issue Report, International Research Center, April 21, 2008.

¹⁶² “Smallpox,” World Health Organization fact sheet. Available at: <http://www.who.int/mediacentre/factsheets/smallpox/en/>

¹⁶³ Senior U.S. officials held a high-level biological attack simulation in June 2001 named “Operation Dark Winter,” which concerned a fictitious smallpox attack on three American cities. Worst-case projections for the total number of U.S. deaths resulting from this attack reached as high as one million. See also Tara O’Toole, Michael Mair, and Thomas V. Inglesby, “Shining Light on ‘Dark Winter,’” *Clinical Infectious Diseases*, Vol. 34, February 2002. For an overview of the exercise provided by the University of

the creation of a host of "boosted" biological agents. For example, Dr. Ken Alibek claims that Soviet scientists created several genetically-engineered variants of smallpox. Alibek remarked that the production of this capability was akin to the development of other preposterous weapons during the Cold War. "Why was it necessary to develop a 100-megaton bomb?" he asked. "If you've got a weapon, your next step [is] to develop a more sophisticated weapon. Smallpox is a fine weapon. But it could be more fine, just by adding some foreign genes."¹⁶⁴ Yet these improvements were the luxury of a lavishly funded state weapons program. Sub-state groups and individuals with more modest budgets may be less able to explore the upper bounds of lethality.

5. CONCLUSION: RELEVANCE TO DTRA MISSION

The *National Strategy for Countering Biological Threats* states that the United States must ensure that its policies are "fully informed by a robust and current awareness of advances in the life sciences and their potential impact upon the risk" to the nation.¹⁶⁵ The preceding analysis contributes to this requirement by improving DTRA's situational awareness of theoretical adversary capabilities on the far reaches of science.

While the threat of genetically engineered bioweapons has been appreciated for more than two decades, consideration of their potential effects has generally been confined to the prospect of mere enhancements to known capabilities. That is, next generation adversary capabilities are typically conceived of as simply more lethal or more contagious varieties of agents that are already well understood. Similarly, assumptions of adversary objectives with respect to bioweapon use tend to mirror those associated with traditional warfare and/or terrorism: incapacitate enemy personnel, kill civilians in large numbers, terrorize enemy populations, and so on. Even the more ambitious analysis concerning novel pathogens rarely departs from this conceptual template. The discussion of truly revolutionary bioweapon capabilities, which would allow adversaries to deliver completely unprecedented effects, is valuable precisely because it so seldom occurs. That these capabilities may be decades away from being achieved does not subtract from the value of considering their national security implications.

With respect to ethnic-specific biological weapons, because there is no scientific consensus on their plausibility, and, indeed, the weight of expert opinion seems to lean toward their being extremely difficult to achieve, a concerted effort on DTRA's part to prepare for them is probably not warranted. However, given the potentially enormous ramifications that would result from their development, DTRA would be well-advised to keep abreast of scientific advances in this arena. Various milestones in our understanding of human genetics would have to be achieved before these weapons become feasible, the most significant of which would be observable. The U.S. defense establishment will therefore have ample opportunities to assess the policies and capabilities that would be necessary to respond to this threat should it approach reality.

Pittsburgh Medical Center's Center for Biosecurity, see: http://www.upmc-biosecurity.org/website/events/2001_darkwinter/index.html

¹⁶⁴ "Interview with Dr. Kanatjan Alibekov," PBS Frontline, October 1998.

¹⁶⁵ "National Strategy for Countering Biological Threats," National Security Council, The White House, Washington, D.C., November 2009.

ADVANCED LASER ISOTOPE SEPARATION AND ENRICHMENT

JEFFREY R. COOPER

"Previous enrichment technologies—the calutron, gas centrifuge and advanced centrifuges—have all created proliferation risks over the past 50 years despite efforts to withhold the information."

— Francis Slakey and Linda Cohen,

"NRC Should Perform Non-Proliferation Assessment of Laser Enrichment Technology,"
Physics & Society, July 2010

I. TECHNOLOGY OVERVIEW

Acquisition of nuclear weapons depends on a supply of suitable fissile material, none of which occur naturally at the concentration levels required for making a weapon. Plutonium is not a naturally occurring element. Plutonium-239, the traditional fissile isotope, is a byproduct of fissioning uranium-238; it must first be created in a reactor and then must be separated from the uranium and other plutonium isotopes to be useful as material for weapons. While uranium-235, the fissile isotope, occurs naturally, it is present only at ~0.7%—far below the requirements of weapons-grade material—and must be concentrated, or "enriched," by one of several methods.

While there are many potential methods for the separation of isotopes and selective enrichment of desirable fissile ones, all of these depend on subtle differences (e.g., in weight) among the isotopes. Historically, gaseous diffusion was the foundational technology used for large-scale enrichment of uranium for both weapons and power grade applications by the United States, the Soviet Union, and other countries. Gaseous diffusion depends upon slight differences between the two isotopes (converted to a uranium hexafluoride gas) in their ability to diffuse through a specially designed porous barrier. More recently, high-speed centrifuges have provided another increasingly common path for large-scale separation activities, especially by states of potential proliferation concern. These machines use centrifugal force to

exploit the mass difference in order to skim a small fraction in each stage of both the enriched and depleted isotope streams and feed them to continue to amplify the separation fraction through a series of cascades. In both of these cases, although the actual mechanisms are quite distinctive, separation essentially depends on the slight mass difference between the U-235 and U-238 conducted recursively over many passes (or stages) to create the desired degree of enrichment. Because the degree of enrichment achieved in each pass is very small, these methods demand that the process be repeated a large number of times in a series of cascades. One result is that, although the science is known and the technology is available—and a substantial number of countries have mastered these industrial-scale technologies—the facilities are large and energy-intensive and create recognizable signatures for surveillance.

Among the many potential alternatives for isotope separation, there are some techniques with even more potential for proliferation concern because of scale, cost,

or efficiency that could significantly reduce the signatures, resources, or time required to produce material for weapons. Indeed, the enriched uranium used in the “Little Boy” device dropped on Hiroshima was produced in calutrons, essentially large-diameter electromagnetic mass spectrometers employing ion cyclotron resonance to exploit the slightly different mass and magnetic spin properties for separation of the two isotopes. Although calutrons have significantly lower energy efficiency than centrifuges, especially at scale, they require fewer separation stages, and facilities for small-scale production can therefore be considerably smaller.

The use of lasers is another, but fundamentally distinctive, route to isotope separation that relies instead in differences in induced chemical reactivity of the two isotopes.¹⁶⁶

Due to differences in absorption and resonance characteristics of different weight isotopes when illuminated by light of an appropriate frequency generated by lasers, they are subject differentially to both ionization and chemical reactivity effects. Each isotope of uranium absorbs laser energy at a slightly different frequency, and therefore a laser of appropriate wavelength can be used for selective irradiation and ionization; as the different isotopes absorb the laser energy, they exhibit sharply different chemical bonding characteristics; and these can then be exploited as the basis for isotope separation.¹⁶⁷ Moreover, because of the very substantial differences in the chemical characteristics of the irradiated isotopes, some laser techniques offer the potential to produce weapons-grade material in a single enrichment stage.¹⁶⁸ In addition to its obvious application for the enrichment of fuel- and weapons-grade uranium, laser isotope separation could also offer

¹⁶⁶ For an early overview on laser separation of uranium isotopes, see C.P. Robinson and R.J. Jensen, “Laser Methods of Uranium Isotope Separation,” in *Topics in Applied Physics: Uranium Enrichment*, New York: Springer-Verlag Berlin Heidelberg, 1979.

¹⁶⁷ For additional information, see John L. Lyman, “Enrichment Separative Capacity for Silex,” Los Alamos National Laboratories, (undated); and “Laser Isotope Separation Uranium Enrichment,” GlobalSecurity.org (undated).

¹⁶⁸ See Francis Slakey and Linda R. Cohen, “Stop Laser Uranium Enrichment,” *Nature*, Vol. 464, March 4, 2010; and Francis Slakey and Linda Cohen, “NRC Should Perform Non-Proliferation Assessment of Laser Enrichment Technology,” *Physics & Society*, July 2010.



advantages in the selective processing of other potentially exploitable radioactive isotopes.

In the late 1970s, the United States initiated a large, multi-pronged program to explore alternative laser separation techniques. Two different laser methods were initially selected for further research and development, one designed at Lawrence Livermore National Laboratory (LLNL) and the other at Los Alamos National Laboratory (LANL). In both cases, the size of the required facilities and the amount of energy used were calculated to be substantially smaller than with those facilities relying on traditional gaseous diffusion or even newer centrifuge technologies. Although neither method has moved into a full-scale production process, laser technology itself is a well-understood domain, with knowledge and technology available worldwide.

The key potential advantages of using lasers for separation and enrichment are size, cost, and efficiency of the process, reducing the need for cascades of thousands of sequential stages. Moreover, unlike the very large, high-energy lasers needed to drive inertial confinement fusion, lasers for enrichment are quite compact and use relatively little electricity; and for those methods that might produce sufficient enrichment in a single stage, they could offer outstanding efficiency that reduces both the cost and time to produce sufficient weapons grade material.

1.1 The Present Level of Accessibility

Gaseous diffusion facilities are massive due to the number of stages needed for enrichment to weapons-grade quality and the extremely large supplies of electric power they consume. By contrast, ultra-speed centrifuges offer a significantly more compact footprint and far lower use of electricity, although demanding a higher, more stable quality of power. However, such centrifuge cascades still represent very large, energy-intensive facilities, feasible only for states or very large organizations. The likelihood that surveillance might discover them or their component elements is increasingly high. Although the scientific and technical bases for both methods are known, both demand a high degree of technical, engineering, and industrial competence to make them work at necessary scale and reliability. These constraints have not stopped a growing number of countries from mastering the necessary capabilities to become potential proliferation sources. However, such capabilities (and the resources to support them) still appear to be beyond those available to most sub-state actors.

Studies conducted in the late 1960s and subsequently indicated quite clearly that the "secret" of the atomic bomb really was no longer secret; the real choke point was acquisition of fissile material, either in the form of uranium or plutonium.¹⁶⁹ As one result, surveillance of potential proliferators then started to emphasize the supply chain and production processes for special nuclear materials (SNM) and other

¹⁶⁹ Theodore Taylor, "Preliminary Survey on Non-national Nuclear Threats," *Stanford Research Institute Technical Note SSC-TN-5205-83*, September 17, 1967. See also Theodore Taylor, et al., "Non-National Nuclear Threats," International Research and Technology, Inc. under contract to the Advanced Projects Research Agency. As a graduate student in 1969-70, the author participated in this more detailed study effort, which demonstrated, first, that smart university undergraduates, yet untrained specifically in nuclear engineering, could design both a "not incredible" atomic weapon and, second, lay out a production and fabrication process with openly accessible tools and materials at reasonable cost, other than the SNM. (This study was funded by ARPA rather than the Atomic Energy Commission (AEC) because the AEC was then still contending that control of weapons design information represented the key to preventing proliferation.) Among other effects, this study helped lead to significantly more stringent controls at facilities possessing SNM.

specialized weapons components. The intelligence surveillance almost exclusively focused on three routes to SNM production: 1) reactors for plutonium, 2) gaseous diffusion, and 3) increasingly high-speed centrifuge technologies.¹⁷⁰ Attempts to focus intelligence collection and analysis on potential alternative routes to SNM production was strongly resisted by the Energy Research and Development Administration (ERDA) and the nuclear weapons laboratories "because we understand the efficient paths" in this area.¹⁷¹

However, the history of the Iraq atomic weapons program offers some cautionary notes concerning our ability to estimate accessibility of and choices among advanced technologies, even by countries under relatively close surveillance. One target of formerly high interest was Iraq. From the mid-1970s onward, surveillance of uranium enrichment within the Iraqi nuclear weapons program focused almost exclusively on gaseous diffusion and centrifuge technologies, ignoring electromagnetic separation technologies like the calutron, which had been used to actually produce weapons grade material. Yet in 1991, weapons inspectors in Iraq literally stumbled upon a series of large-diameter ring magnets for calutrons attempting to be removed from one of the previously secret Iraqi atomic weapons research facilities.¹⁷² While significantly less efficient than either gaseous diffusion or ultra-centrifuge cascades, they were relatively cheap, very easy to assemble with openly available technical information, and required only small facilities.

1.2 The Timeline for Development

While it is feasible based on U.S. experience to make estimates about the development path and time scale for the already identified laser enrichment techniques, it is more problematic to forecast whether alternative laser technologies or innovative separation methods exploiting selective absorption and ionization could offer dramatic improvements. Because of widespread academic and commercial interest in lasers and laser-assisted chemistry, possible breakthroughs in either area should not be ignored.

The story of the radio-frequency quadrupole (RFQ) should caution against confidence in estimating development timelines; in those instances where truly significant innovations can provide factor-order rather than incremental improvements in critical capabilities, such estimates can be wildly off the mark. The RFQ is a compact device now used as the front-end of high-energy particle accelerators as the injector. The concept was originally laid out in a 1968 Russian-language Soviet patent emphasizing the RFQ's advantages for beam stability and emittance quality. Yet it actually "represented the 'missing link'" to beams for high power particle accelerators, sharply increasing the efficiency "from 50% to more than 90%."¹⁷³ Such accelerators have many potential uses, some beyond academic research in particle physics or materials research. One such use is the free electron laser, based on

¹⁷⁰ Among other factors, from the mid-1970s onward, it was known that critical design, production, and operating technologies for centrifuges had leaked from Urenco, the European enrichment consortium, and were known to be in the possession of states of proliferation concern.

¹⁷¹ Starting in early 1977, the author served as the personal liaison between the Secretary of Energy-Designate and the National Security Agency (NSA) for creating the first "non-proliferation dictionary;" neither calutrons nor ion cyclotron resonance appeared in that dictionary due to resistance from laboratory experts.

¹⁷² For additional information on Iraq's use of calutrons, see Andre Gsponer and Jean-Pierre Hurni, "Iraq's Calutrons: Electromagnetic Isotope Separation, Beam Technology, and Nuclear Weapon Proliferation," Independent Scientific Research Institute (ISRI) Report ISRI9503, October 19, 1995, in Suren Erkman, et al., "The Origin of Iraq's Nuclear Weapons Program: Technical Reality and Western Hypocrisy," Independent Scientific Research Institute, October 20, 2008.

¹⁷³ Alessandra M. Lombardi, "Radio Frequency Quadrupole (RFQ)," CERN, Geneva, Switzerland.

similar technology, which also has potential for national security applications in beam weapons.

However, from the time of the original patent filing, it took nearly a decade for researchers in the United States to become aware (by happenstance) of this research and its overlap with then-emerging interests and engineering capabilities at Los Alamos. According to Alessandra M. Lombardi, only in 1977 was the RFQ concept published in the Western literature, which generated "strong interest" from LANL. Its scientists elected to test the RFQ principle for potential application in developing high-current low-emittance beams. Concurrently, a concerted effort was made to develop computer codes for the RFQ design.¹⁷⁴ A 1981 paper by a LANL team provides further details of this research: "In 1978 the Los Alamos Accelerator Technology Division initiated a program to develop improved low-velocity systems. The program was based on the RFQ linear accelerator that had been suggested by Kapchinski and Teplyakov in 1970."¹⁷⁵ As the LANL piece notes, "The success of this test and the advances in RFQ design procedures have led to the adoption of this linac for a wide range of applications," many with important defense as well as scientific research applications.¹⁷⁶

2. GAME-CHANGING QUALITIES

Compared even with modern centrifuge technologies, laser isotope separation and enrichment techniques potentially offer a further dramatic reduction in size and process efficiency as well as extremely substantial improvement in energy used. However, the two technical paths chosen by the U.S. for laser enrichment still represent very high-end technical capabilities demanding a large and sophisticated industrial infrastructure. To the extent that more efficient lasers with the proper wavelengths are developed or new methods for separation identified, there could be surprisingly rapid progress that allows relatively small groups, as opposed to nations or large organizations with significant industrial capabilities, to enrich uranium for weapons purposes.

A truly compact, frequency-stable laser that is tunable to the frequencies of interest for isotope separation could potentially allow many actors to exploit laser technologies for separation and enrichment. Coupled with innovative separation techniques based on differential responses (such as chemical bonding or spin) of the isotopes to the laser energy, these technologies could provide genuine breakthroughs with dramatic consequences for proliferation as they might offer truly unique capabilities such as single-stage enrichment and possess very small footprints and signatures.

It is important to note that one of the traditional assumptions often made in assessing future S&T advances is that because of our widespread technological leadership, the U.S. will be able to recognize important new developments that could become "game changers," often because it will be invented or developed in the United States. As the RFQ example illustrated above, the United States does not possess a monopoly on innovation. Moreover, there are numerous other examples, such as the "Caspian Sea Monster" and the Shkval torpedo, that illustrate the

¹⁷⁴ Lombardi, op. cit.

¹⁷⁵ R.H. Stokes, T.P. Wangler, and K.R. Crandall, "The Radio-Frequency Quadrupole—A New Linear Accelerator," *IEEE Transactions on Nuclear Science*, Vol. NS-28, No. 3, June 1981.

¹⁷⁶ Stokes, op. cit.

difficulty in recognizing truly innovative foreign technical developments.¹⁷⁷ Furthermore, new frontiers in science often produce surprises in the types or rates of advance that cannot be predicted beforehand, resulting in fundamentally new and different approaches to meeting existing objectives or creating new opportunities.¹⁷⁸

3. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY DEVELOPMENT

3.1 Drivers

The growing use of lasers for academic and industrial research in many possible areas of application significantly increases the chance that new, more efficient laser technologies will be developed. Furthermore, as cheap, compact lasers with the appropriate frequency capabilities and pulse characteristics become available, it is likely that researchers will discover additional approaches to exploiting laser chemistry. Some of these could lead to innovative separation methods based on selective absorption and ionization that would not currently be forecasted as possible. Furthermore, one area in particular that appears very ripe for rapid innovation involves manipulating chemical reactions on ultra-short timescales (such as femtoseconds) and the growing availability of lasers with these types of ultra-short pulse capabilities could enable truly revolutionary science.¹⁷⁹

3.2 Counter-drivers

The growing interest in biologically inspired or derived technologies for a wide range of chemistry applications could lead to the rapid development of alternatives to laser methods that might be more economically or commercially attractive and therefore skew the direction and priorities for future research.

4. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY ATTRACTIVENESS

There are potentially two very different sets of drivers that could affect the prospects for compact laser separation and enrichment. One set derives from top-down concerns over continued diffusion of proliferation-related technologies that could result in additional constraints being placed on relevant research and access to related technologies. The other set could arise from the emergence of fundamentally different alternatives for advanced chemistry and chemical engineering, especially for heavy-metal separation and sequestration such as bio-derived methods.

5. CONCLUSION: RELEVANCE TO DTRA MISSION

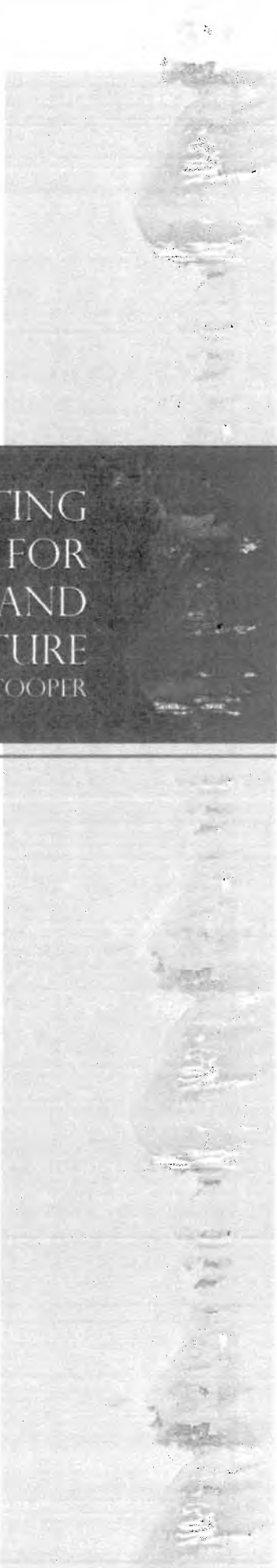
Advanced separation technologies that are low cost and compact could significantly expand the range of actors capable of producing fissile material usable for nuclear weapons. Even the newer centrifuge technology, although smaller and less costly than gaseous diffusion methods, requires the resources and capabilities of state-level actors. However, breakthroughs in compact laser technologies, akin to the type of leap in capability that occurred with accelerator technology as a result of the RFQ, could alter this situation rapidly.

¹⁷⁷ A large number of excellent examples highlighting this issue could be provided at the classified level. For a description of the Caspian Sea Monster, a Soviet Ekranoplan, or ground effect vehicle (GEV), see "Riding the Caspian Sea Monster," *BBC News*, September 27, 2008; for a description of the Shkval torpedo, see Patrick E. Tyler, "Behind Spy Trial in Moscow: A Superfast Torpedo," *New York Times*, December 1, 2000.

¹⁷⁸ Adrian Cho, "What Shall We Do with the X-ray Laser?" *Science*, Vol. 330, December 2010, 2010, pp. 1470-71.

¹⁷⁹ Revolutionary as in Kuhn's distinction between normal and revolutionary science: offering fundamental discrete leaps in knowledge and capability.

If such technologies were to emerge, a far wider range of players could become "actors of concern," requiring more intense surveillance and far greater expenditures of political capital. A critical first step in preventing such expansion concerns the recognition that one or more new separation and enrichment technologies have emerged that could be applied to isotope separation. One priority area for investment would be a far more intensive foreign S&T surveillance effort. Another priority area for investment would be a broader U.S. research and development effort on alternative enrichment methods in order to identify potential routes.



EMI MICRO-JAMMERS (EMJs): EXPLOITING ELECTROMAGNETIC INTERFERENCE FOR DISRUPTION OF CRITICAL NETWORKS AND INFRASTRUCTURE

JEFFREY R. COOPER

"We've arranged a civilization in which most crucial elements profoundly depend on science and technology. We have also arranged things so that almost no one understands science and technology. This is a prescription for disaster. We might get away with it for a while, but sooner or later this combustible mixture of ignorance and power is going to blow up in our faces."

— Carl Sagan, 1995

I. TECHNOLOGY OVERVIEW

Electro-magnetic interference (EMI) Micro-Jammers, referred to hereafter as EMJs, would exploit modern electronic, robotic, and nano-technologies to enable widespread disruption of critical information networks and societal infrastructures at low cost to the attacker.¹⁸⁰ EMJs could be distributed in a wide range of ways: by unsophisticated methods—such as simply scattering by hand or blown from moving vehicles—to more highly targeted emplacements by nano-bots or micro-flyers homing on specific radiated signals.

¹⁸⁰ Elsewhere in the literature, this threat is referred to as "Intentional electromagnetic interference (IEMI)" and also "EM Terrorism." See William Radasky and Edward Savage, "Intentional Electromagnetic Interference (IEMI) and its Impact on the U.S. Power Grid," Metatech Corporation report prepared for Oak Ridge National Laboratory. See also William A. Radasky, et al. "Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)," *IEEE Transactions on Electromagnetic Compatibility*, Vol. 46, No. 3, August 2004; and R.L. Gardner, "Electromagnetic Terrorism: A Real Danger," in *Proceedings of the 11th Symposium on Electromagnetic Compatibility*, Wroctaw, Poland, June 1998.

Unlike concerns about corruption of information content or widespread interruptions of communication flows by cyber attacks, disruption of specific waveforms and signals created by traditional electronic warfare (EW), or very destructive but localized effects from high-power pulse devices such as EMP, micro-EMI jamming would create a new niche in the threat taxonomy. This new threat would be produced by exploiting the increasing dependencies on these networks and infrastructures by



modern societies for mission-critical services at very high reliability factors. Attacks would be facilitated by the vulnerabilities of these systems due to inherent technical characteristics of modern electronics and the electronic environment. In particular, EMJs could portend serious threats to distributed communications systems (including supervisory control and data acquisition (SCADA)) and to certain important but lesser recognized functions of the Global Positioning System (GPS) system, such as timing.

1.1 A Short Course in EMI

All types of systems and devices operating in the electromagnetic spectrum, including critical networks

for communications and information transfer, are subject to disruptive effects from a variety of interference problems. While this interference may often be unintentional, it is no less problematic for the user. EMI, also known as radio-frequency interference (RFI), affects both systems that have tangible physical connections between components, such as circuit boards and conductively-wired networks, as well as those connected by propagation of radio-frequency signals through free space, such as WiFi or cellular telephone networks. Since the invention of devices that depend on signals propagated through the electromagnetic spectrum (EMS)—such as telegraph and radio—concerns about potential inference have existed. These problems, especially caused by unintentional sources of interference, can generally be mitigated in the design and with appropriate shielding of the equipment. Historically, EMI was considered to be a problem primarily for users dependent on radio-frequency (RF) signals such as radio or radar propagating through free space or from improperly routed or shielded communications wiring. Commonly occurring examples include “static,” affecting traditional radio or television reception, and “cross-talk” from inadequately shielded or segregated circuits, a frequent problem in traditional circuit-switched telephone networks.

There are many potential sources of EMI: some of these effects result from natural sources, such as solar flares or lightning during electrical storms; other sources are created by man-made machines because almost all electro-mechanical and electromagnetic devices (such as electric motors and spark plugs, respectively) emit RF transients during operations, especially during transient operations like switching. This interference results both from interactions within and between conductive electric/electronic circuits—such as in older wired telephone systems and

computers,¹⁸¹ as well as from radiated energy interacting with electromagnetic propagation through free space (as with radio, television, and radar), or even within circuit boards and black boxes.¹⁸² Devices that switch rapidly, including modern digital electronic circuits, can create local broad-band interference that can be difficult to eliminate through filtering once introduced into the receiver chain.¹⁸³

Thus, EMI can be introduced not only by effects from outside (whether natural or man-made, unintentional or with malevolent purpose) but also caused by components within devices and systems. Engineers generally distinguish between EMI or RFI that is radiated (through free space) and that which is conducted (within circuits), and they also distinguish between sources of narrow-band (within specific frequency bands) and broad-band interference. Within circuits, EMI from conductance was previously more common. EMI/RFI from inductance is increasingly likely as devices shrink and signal levels decrease, moving within the field patterns of neighboring devices.¹⁸⁴ Given that the infrastructures tying together the diverse and heterogeneous networks underlying modern societies include a very wide range of links and nodes, they are potentially subject to a wide range of interference effects—both from inside and outside their systems.

As noted above, most devices that rely on the electromagnetic spectrum are subject to both intentional and unintentional interference. However, as devices have become smaller and more densely packed, EMI/RFI issues arise within complex integrated systems at both board and box levels. Increasingly, semiconductors and integrated circuits have replaced large, high-voltage vacuum tubes and electronic circuits have replaced mechanical control linkages, with both changes increasing sensitivity to interference. And although photonic devices themselves are less subject to external interference, the components at nodes that rely on electronic devices for conversion, power supply, switching, and control circuits remain subject to EMI.¹⁸⁵

While it is often easy to eliminate sources of unintentional EMI by suppressing it at the emitter, it is often far more difficult to negate these effects when they are created intentionally for malevolent purposes and can exploit inherent characteristics of the devices and systems. However, especially with intentional sources of interference, combinations and interactions among these categories may occur as EMI effects that begin in free space may be introduced into circuits, especially as hybrid interconnected wireless/wired networks become increasingly common. Moreover, it is important to recognize that to disrupt networked communications systems, jammers do not necessarily have to actively “interfere” with particular communications by overriding or corrupting signals. With modern communications systems that do not

¹⁸¹ The problem is considerably reduced by systems that employ light and fiber optics rather than conductive wires.

¹⁸² Not unlike the problem of identifying weeds, it is impossible in the abstract to clearly distinguish “interference” or “noise” from useful signal without reference to context. Thus, a radar performing important air surveillance functions may be a source of interference with TV broadcasts.

¹⁸³ “Radio Frequency Interference – And What to Do About It,” *Radio-Sky Journal*, No. 4, March 2001.

¹⁸⁴ As devices shrink and power and signal levels also generally decrease, so do signal-noise ratios, making these devices more sensitive to interference.

¹⁸⁵ Links using optical fibers are themselves generally resistant to introducing or extracting signals by induction-coupling, thus minimizing one traditional source of interference, or entry-point for cyber attacks. As more WANS and even LANs, such as for Ethernet, employ fiber rather than the traditional conductive cables, the electronics at the connecting and processing nodes will become even higher priority targets for access and attack.

specifically reserve circuits for particular users,¹⁸⁶ jammers that can access the links and routing nodes and appear as legitimate users can merely use up available bandwidth, channels, or code division multiple access (CDMA) and time division multiple access (TDMA) slots in order to create effective disruption through pseudo-congestion.¹⁸⁷

Finally, in some cases, such as with receiving GPS signals in small portable devices with relatively low signal-noise margins, simple in-band “noise” can be seriously disruptive. This might represent only a minor annoyance for many non-mission critical navigation functions. However, GPS signals serve another critical role that is seldom recognized—along with its navigation signals, GPS also transmits high-precision timing signals that are used to set clocks in the communications networks and in increasingly common encryption/decryption devices such as RSA cards. These clocks serve as an essential synchronizing element that is necessary for proper system functioning. Widespread interference jamming of these signals would potentially disturb not only communications networks but also those payment, credit validation, and financial transaction networks that require time synchronization for their encryption/decryption security processing. As users carry out more and more financial transactions with small, low-power devices such as cell phones and personal digital assistants (PDAs), the importance of this function will increase dramatically.

	Radiated	Conduction/Induction
Narrow-Band	Cell phones, WiFi networks, radar, radio and TV broadcasts	Inductors, neighboring circuits
Broad-Band	Spark devices, motors, lightning	Switching circuits, transformers, capacitors

Table 1: Categorizing EMI/RFI

1.2 The Present Level of Accessibility

For the “do-it-yourself” attacker, in simplest terms, an EMJ needs only a few components: a transmitter at the correct frequency, an antenna, and a power supply. The potential for widespread availability of EMJs is enabled by the commercial applications of each of the three key components. More sophisticated devices might also require a scanning receiver to identify target frequencies or channels to be jammed, a frequency agile transmitter module, and an adaptive antenna that can optimize its signal coverage and reduce power demands for the same effectiveness.

However, because wireless systems, especially cellular telephones and WiFi systems, have increased dramatically in popularity, complete devices to exploit wireless (which are also capable of serving as jammers) have proliferated broadly. These devices now represent the fastest-growing segments for many parts of cyber/information networks and probably will for the foreseeable future. Unlike traditional broadcast

¹⁸⁶ Traditional communications systems addressed resource (bandwidth) scarcity and contention issues by pre-planned allocations of channels and time-slots, lacking flexibility to meet changing demands and using resources less efficiently. Modern adaptive systems (including those using Ethernet and TCP/IP routing) use resources more efficiently by real-time allocation to users as needed.

¹⁸⁷ Such contention issues often arise from unplanned “storms” of users responding to viral communications. However, it could also arise from jammers that create or “lose” packets, effectively forcing re-transmission of noise. This would result in situations quite similar to a distributed denial of service attacks on Internet nodes and links by loosely coordinated botnets.

radio or television, which for the bulk of consumers were mostly “one-way” technologies where “users” possessed what were simply receivers, many modern RF devices such as cell phones are fundamentally designed and intended for two-way communications. Moreover, for packet-switched systems, even those devices that are basically intended only to receive information, the digital devices possessed by users are both receivers and transmitters.¹⁸⁸ Therefore, complete devices capable of creating disruptive electromagnetic interference are widely available for a broad range of legitimate uses.¹⁸⁹

Thus, there is already widespread commercial availability of these newer small emitters that have the potential to disrupt the critical information linkages among many important networks through widely proliferated operations. Accessibility of the components needed for the simplest EMJs must therefore be assessed as high, even for relatively unsophisticated individuals or small groups. These individuals and groups would not need to build the key components but rather merely assemble EMJ devices from widely available components.

There is also widespread availability of the components needed for more sophisticated devices designed to home-in and jam particular frequencies or signal formats, and only moderate skill is needed to assemble these. Even EMJs intended for mobility in order to be more precisely positioned could be assembled from readily accessible components intended for hobbyists and children's toys. Components for EMJs intended to interfere specifically with GPS signals by noise jamming are less easily available, as they require transmitters less readily accessible because of the specific frequencies at which GPS operates. However, an increasing number of components with the capability to generate signals at these frequencies are commercially available and can be modified for these purposes.

Moreover, it is important to appreciate that jamming is a function of how a device is used or applied, and not necessarily an inherent characteristic of a mechanism. Not only does this have serious implications for the availability of such devices, but it also makes their identification potentially more difficult, as it is not necessarily the signal form or power that would mark their role as jammers. Devices that merely replicate and re-broadcast valid message packets could serve as effective jammers simply by creating congestion and bandwidth contention. Moreover, since these EMJs would operate close to their targets, they only need to emit low-power signals that would make them very difficult to locate against the very noisy background environment.¹⁹⁰

1.3 The Timeline for Development

The ability to wage effective EW that exploits EMI/RFI, or large-scale cyber attacks, was traditionally thought to be the province of technically sophisticated states and a few especially competent non-state actors. With the capabilities posed by EMJs and their relatively low level of needed technical input, there is nothing fundamentally constraining the creation of these devices now by small groups or individuals, much less by more sophisticated organizations or states.

¹⁸⁸ In networks like the Internet employing TCP/IP, receipt of transmitted packets must be acknowledged, requiring the recipient to broadcast an acknowledgement or else the packets are retransmitted by the source until a receipt acknowledgement is received or the gate times out. Cellular telephones broadcast location information when “on” even when not actively transmitting communications in order to let the network know where to reach them.

¹⁸⁹ An unfortunately good analogy is the ease of acquiring cell phones to use as triggers and control devices for improvised explosive devices (IEDs).

¹⁹⁰ One need only look at the website for Dust Networks, Inc. (www.dustnetworks.com) to appreciate how easy it would be to repurpose readily available components or devices of the right size and form factors.

2. GAME-CHANGING QUALITIES

Once considered quite distinct technical and warfare domains, EW and what is now generally called cyber operations (formerly known as “Information Warfare” or “Information Operations”) have begun to coningle and merge as target sets, and means of access have become conflated. Historically, EW focused on systems employing RF energy propagated through free space, such as radios and radars; cyber, on the other hand, generally focused on targeting computers and information systems and the networks that usually connected them through conductive wires or optical fibers.¹⁹¹ The present conflation results from the increasingly integrated nature of modern communications networks and information infrastructures that combine wireless RF systems with wired or fiber networks, largely driven by the need to service the rapidly growing mobile user market (for example, through cellular telephone systems) as well as by the ease and convenience of relying on WiFi links rather than wired ones for even local connectivity. As these previously separate systems became increasingly linked and networked, potential entry points and methods rapidly multiplied and criss-crossed these two domains.

Modern industrial and post-industrial societies depend on extraordinarily complex infrastructures for their efficiency and continued functioning—including for meeting the necessities of everyday life, as well as for maintaining the crucial social, political, and economic relationships that provide cohesion. These infrastructures, in turn, rely on seamlessly sharing information through highly integrated and complex networks. Unlike concerns about corruption of content, disruption of specific waveforms and signals created by traditional EW, or widespread effects such as EMP from high-power devices, micro-EMI jamming would occupy a new niche created by the increasing dependencies of modern societies on these critical information networks and control infrastructures.

Traditionally with broadcast analog radio and TV communications through free space, interference was a major concern for reliability and usability. Aside from appropriate design, the major thrust in reducing interference with broadcast signals was addressed by allocating and separating neighboring frequency users, controlling access to specific frequency bands, and licensing users. With the emergence of digital communications techniques with their inherent error-correcting coding, it was thought that traditional interference problems would largely disappear. While in the abstract, robust digital communications and the wide variety of resilient transmission techniques (e.g., CDMA, TDMA, etc.) appear to offer easy solutions like Parkinson’s Law, the explosive growth of digital users and devices has created serious competition for available bandwidth, resulting in frequent contention problems and constraining the ability to easily apply many of the usual methods to address EMI problems.¹⁹² Moreover, very few civilian or commercial networks were designed to cope with dedicated malevolent attacks traditionally considered in designing systems and networks for national security users.

Given that wireless devices have proliferated so broadly, small emitters have the potential to disrupt the critical information linkages among many important networks.

¹⁹¹ By the 1960s, even the traditional circuit-switched “plain old telephone system” (POTS) using wired networks began to incorporate both microwave and satellite RF links rather than depend solely on physically wired links where cost trades favored them.

¹⁹² There is a general trade-off between the effectiveness of an error-correcting code (ECC) and the amount of power consumed for processing, a high-priority design concern in increasingly compact mobile devices. Similarly, disruption of a channel’s timing by contention or by incompletely corrected errors introduced by noise increases the likelihood that packets will have to be re-transmitted, further aggravating the contention problem.

Although cellular phone networks are regulated and licensed, the problem has been greatly magnified in that much of the explosive growth of important capabilities for commercial and consumer use, such as WiFi, has occurred in systems operating in the unlicensed frequency bands (2.4Ghz, 3.6Ghz, and 5Ghz), which also have many other significant uses and users communities. These include, among others, medical devices, microwave ovens, burglar alarms, and older wireless telephone systems. As noise and errors increase in these systems, both latency and contention rise, further fueling the number of packets bouncing in the system.

Moreover, like the Internet, the majority of networks (including local area networks [LANs] and wide area networks [WANs]) today employ, and in the future will increasingly employ, stochastic routing methods and lack separate and centralized control channels. These control protocols are sensitive to traffic demands, the timing of packets, and the effects of contention; WiFi systems exhibit most of these characteristics as well. Because the information flows and protocols that tie these diverse infrastructures and networks together were designed in large measure to operate in relatively benign environments, they are sensitive to both unintended and intended interference. Often driven by advancing technologies and by purely competitive commercial considerations, the technical characteristics of many modern networks makes these infrastructures more susceptible to EMI. As electronic devices have become smaller, more tightly packed and integrated, lower power, and lower voltage, they may also be more subject to EMI problems.

As with the explosive growth of WiFi, worldwide cell phone usage has also grown extensively. The movement to lower-power "micro-cells" in order to exploit available bandwidth more efficiently and increase channel capacity has resulted in lower-power signals, often more subject to even low-power interference. It is likely that this continued movement toward even lower power devices to facilitate size reductions in portable devices and accommodate the increasing demand for mobile access will continue the drive toward lower signal strengths and smaller signal/noise ratios.

As discovered with Ethernet, high rates of competition for available bandwidth or time slots results in "contention," which in this context can be considered to be a form of EMI. Very similar effects have accompanied the explosion of WiFi, which operates in unlicensed bands and where devices are subject to relatively few restrictions. Especially as WiFi has transitioned from being merely a local access point for a LAN to being employed for widespread public access over large areas, the potential for interference and contention has increased dramatically.¹⁹³ Furthermore, often less appreciated, even more mundane systems are now subject to serious EMI problems as advanced electronics have been substituted for mechanical control and integrated into every-day household items. Recent problems with Toyota braking systems are now thought to be caused, at least in part, by EMI issues.

Perhaps of more direct concern, GPS has become an essential service, often in ways not generally recognized. While the location and navigation services of GPS are widely appreciated, the key role of the precision time-keeping system of GPS is often overlooked. The ultra-precise atomic clocks on GPS satellites provide synchronization signals that are essential to maintaining network communications. Moreover, those same timing signals are crucial for most real-time encryption

¹⁹³ Under the old POTS regime, "provisioning," although arcane, was recognized as an important aspect of service planning and was conducted by skilled professionals. Increasingly far less attention is paid when establishing user networks, especially when they are provided as an enticement for other services.

systems that rely on signals to synchronize pseudo-random number keys—and these are found in many financial transaction systems.

The ability to disrupt these networks by degrading their performance with cheap, easily available, widely dispersed small devices (what might be termed micro-EMI jammers) would create substantial new concerns for the ability of malevolent actors to stage significant disruptive acts that could strike at the very foundations of modern societies. At their most simple, a micro-EMI jammer would consist of a transmitter, an antenna, and a power source (most often a battery). For in-band transmitters operating in WiFi, cellular, or other popular bands, it might be exceptionally difficult to discriminate between signals from valid users and those generated by jammers. Given the small sizes of these devices, they could prove to be very difficult to detect, especially if they were only selectively activated. Operating in-band in an already cluttered environment, identifying jammers from legitimate devices could prove exceptionally difficult, especially in open-access areas with many transient users.

More sophisticated devices might also include: a tuner/receiver to identify nearby target signals and initiate jamming selectively so as to not waste power; a tunable directional antenna to increase effective radiated signal against targets; alternative power supplies, such as nano-scarvengers that can harvest energy from motion such as wind or vibration; and a C2 module for external control. Even without the ability of malicious actors to exert control of large-scale networks of such jammers in real-time, large numbers of sophisticated devices could create significant disruptions and service outages that could be difficult to remedy quickly. With the ability to control networks of such devices in real-time, effective countermeasures and remedies would be even more difficult to implement.

3. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY DEVELOPMENT

Consumer demands and commercial applications, often with new or significantly improved functionality, are fueling the rapidly spreading use of small mobile wireless devices relying on RF propagation (both cellular and WiFi technologies), often replacing larger fixed instruments connected by wire or fiber. These drivers have three important technical implications. First, these mobile devices will create increasing demands for RF bandwidth, magnifying allocation and contention issues, as well as likelihood of mutual interference. Second, mobile devices create a premium for small, low-power devices that are likely to be more subject to interference, whether unintentional or malevolent. Third, competitive cost pressures, especially for price-sensitive consumer products, tend to reduce the design margins available to address EMI/RFI problems. This includes pressures on physical shielding and more inherently robust ICs to choices among error correcting codes that reduce computational intensity (and therefore power consumption).¹⁹⁴

This expansion of demand for RF bandwidth occurs in two differently regulated regimes. Cellular-based technologies operate under a far more stringent set of regulatory controls than do systems like WiFi that operate in unlicensed bands; and these are experiencing the most explosive growth, especially as many cellular telephones now also have the ability to operate through local WiFi access points.

¹⁹⁴ This is not intended to place the blame only on the commercial sector for these choices. Similar choices to trade robustness and resiliency for cost have been made by the government for its own networks. Moreover, historically even with highly critical military systems such as satellites, hardening and EMI/RFI robustness have usually had lower priority than reduced system cost.

4. CONCLUSION: RELEVANCE TO DTRA MISSION

Given the pervasive availability of and ease of legitimate access to components and devices that could serve as EMJs, combined with the potential for serious disruption of critical networks and systems by the widespread use of EMJs, network surveillance and data fusion methods for recognizing such types of widely distributed, very low-power jamming exploits should be an investment priority. Further, investments in technologies needed to identify and locate specific jammer sources should also be considered a priority item. These represent significantly different and possibly more challenging problems for recognition and device identification than traditional jammers employing high-power or specific wave-forms.

CYBER TECHNOLOGY: BOTNET TECHNOLOGY AND CIRCUIT BOARD HACKING

STEPHEN J. LUKASIK, PH.D.

"People are the quintessential element in all technology... Once we recognize the inescapable human nexus of all technology our attitude toward the reliability problem is fundamentally changed."

— Garrett Hardin, 1976

I. TECHNOLOGY OVERVIEW¹⁹⁵

The terms cyber technology, information technology, and computer technology are used here synonymously, although in fact have somewhat different meanings. "Cyber" derives from the Greek κυβερνήτης (*kybernētēs*), referring to steersman, governor, or rudder. The subtitle of Norbert Wiener's *Cybernetics* is "*or Control and Communication in The Animal and The Machine*."¹⁹⁶ Information technology focuses on the creation, storage, and movement of information for practical ends of calculating and supporting business operations, with the International Business Machines Corporation (IBM) as its foremost icon. Computer technology as a scientific or engineering discipline is developed and taught in academic institutions with linkages to mathematics, logic, electrical engineering, signal processing, and intelligence, among others.

The DTRA mission derives from weapons—first nuclear weapons, and then broadened to WMD, understood in strategy and policy discussions to include chemical, biological, and radiological weapons. More recently, the term has included anything else that seems to promise *mass* casualties and destruction. In recent years DTRA

¹⁹⁵ This overview is intended to serve for both the botnet and the circuit board attack subjects discussed below.

¹⁹⁶ Norbert Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine*, Cambridge, Mass.: Massachusetts Institute of Technology Press, 1948.

has used the elasticity of the WMD term to refer to WME, where “effects” might be easier to argue than the “D” of death and destruction. Nevertheless, the invariant in DTRA’s formulation of its mission is *weapons*, that is, devices and techniques intended for use as an expression of political power and the mitigation of the threat they imply.



Cyber conflict and cyber weapons have received public attention only relatively recently compared to the much longer period of the development of information and computer technology.¹⁹⁷ Their origin dates to classified thinking in the national security establishment in the early 1990s, under the rubric of “software war,” the term itself being classified at the time.¹⁹⁸ Currently offensive “cyber war” is receiving much more visibility, under an opaque designation of “information operations” and the establishment of the U.S. Cyber Command subordinate to the Strategic Command.¹⁹⁹ The point of this is cyber technology, as DTRA would seem to have a mission related to it, rests not narrowly on technology or weaponization but on the larger issues of utility, intent strategy, and threat assessment. This said, the characteristics of cyber technology needed to appreciate future developments can only be understood by studying the longer period over which information and computer technology have developed, however unrelated they may have been to issues of threats and responses.



At this point an overview might be expected to turn to matters of science, engineering, and markets: processor speed, storage capacity, access time, semiconductor limits, transmission speeds, network connectivity, software complexity, ranges of applications and their strategic importance, national strengths in various areas, the likelihood of further innovation, and the like. The literature is awash in such inventories, and there is little benefit to DTRA in repeating it. Instead, this overview will focus on those matters that create both vulnerabilities and opportunities for states and sub-state groups to destabilize a cyber-based world.

There are four matters that determine one’s assessment of cyber-based national security developments:

- ▶ The “yin and yang” of cyber technology, the complementary opposites that dynamically interact within a greater system, and the importance of balance between them;
- ▶ The difference between cyber capabilities as weapons and threats and cyber capability as a strategy for balancing opposing forces;
- ▶ The limits of technological forecasting, and how that difficulty is exacerbated when dealing with rapidly changing technological and economic capabilities;

¹⁹⁷ In August 1995, a *Time* Magazine cover story on “Cyber War” declared, “The U.S. rushes to turn computers into tomorrow’s weapons of destruction. But how vulnerable is the home front?” See Mark Thompson and Douglas Waller, “Onward Cyber Soldiers,” *Time*, August 21, 1995.

¹⁹⁸ A successful CIA operation in the early 1980s to emplace “doctored” control software in a Soviet gas pipeline to Western Europe can be cited as an earlier example. But such one-off attacks are not easily repeatable and do not directly lead to its institutionalization as a new mode of warfare. See Thomas C. Reed, *At the Abyss: An Insider’s History of the Cold War*, New York: Random House, 2004. p. 269.

¹⁹⁹ For a few pointers into a large literature, see *Technology, Policy, Law, and Ethics Regarding the U.S. Acquisition and Use of Cyberattack Capabilities*, National Academies Press, 2009; Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Corporation report for the U.S. Air Force, 2009; and *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, 2010.

- The difference between trend extrapolation based on past events and extrapolation based the expectation of future discontinuities.

These matters are discussed in greater detail in the following sections.

1.1 The “Yin and Yang” of Cyber Technology

The recognition of information technology and computer science first emerged as an unblemished positive factor in the service of mankind. Computers were originally seen as mechanical or, later, electrical devices to do calculations. Originally the word “computers” was applied not to hardware but to the people who used these devices to perform calculations requested for analysis and management. As the hardware became more general purpose (i.e., “programmable”), the word was shifted to those who wrote the programs that directed computers to compute.

Starting with Herman Hollerith's work for the analysis of the U.S. census of 1880, and Thomas Watson when he became general manager of the Computing-Tabulating-Recording Company (CTR) in 1914 (renamed IBM in 1924), automatic computing had a utilitarian business purpose but hardly seemed to be an apparent precursor of “cyberwar.” While World War II introduced the need for automatic computing for weapon systems, nuclear weapon design, air defense, and cryptography, it remained a matter of rapid calculation. Its yang could, of course, be a tool to use for the execution of financial crimes. But for most of its 20th Century life, computing was an expensive tool entrusted to highly trained people intent on the purposes set by their employers and using mainframes affordable only by the largest enterprises.

The change came with the democratization and commoditization of the technology and the broad empowerment of what is now effectively everyone. The pace, driven by the Advanced Research Projects Agency (ARPA), the academic community, and Xerox PARC among many others, was rapid. Starting in 1970, the ARPANET demonstrated that computers could be connected to computers in a scalable way. Integrated circuits in the same period made personal computers smaller and widely affordable.²⁰⁰ In the 1980s, the Federal Communications Commission (FCC) adopted rules to allow communication capacity to be resold by unregulated carriers, and it authorized cellular telephony and spread spectrum technology to allow mobility of computer users.²⁰¹ The WorldWideWeb, HTML, and Web browsers allowed virtually universal access to such published information as its creators chose to make available.

The age of innocence ended with the Morris Worm in 1988, and beginning of the malware industry.²⁰² The impact of viruses and worms is less a function of the technology than it is the intentions of the technology's users. Irresponsible and playful users came first, followed by both distributed and centralized criminal groups, then by the development of cyber weapons, and finally became a global anxiety. Targeted marketing introduced personal privacy concerns; “phishing” led to identity theft, intellectual property losses, legal liability actions, and the disclosure of sensitive information. Distributed denial of service attacks on Web sites were first used against business rivals but have since become a means of both business interruption and political expression.

²⁰⁰ Stephen J. Lukasik, “Why the ARPANET Was Built,” *IEEE Annals of the History of Computing*, Vol. 32, No. 4, 2010.

²⁰¹ Stephen J. Lukasik, “Unleashing Innovation: Making the FCC User-Friendly,” *INFO*, Vol. 11, No. 4, 2009.

²⁰² Peter Gutmann, “The Commercial Malware Industry,” University of Auckland (undated).

1.2 Cyber Conflict, Mass Effects, and Cyber Force Balances

Cyber technology benefits all—all attackers and all defenders. As with strategic nuclear weapons, what is important is less absolute values than strategic force balances between potential adversaries. Unlike the case of strategic nuclear balances, we have yet to adopt the concept of cyber balances for security planning. The essence of a balance is the determination not of numbers on each side but, taking into account their differing characteristics, how offense compares with adversary offense, offense compares against adversary defense, and broader issues of geography, industrial base, and recovery potential. While we celebrate cyber technology's commercial attractiveness, we fail to understand how balances between capabilities, consequent vulnerabilities, and defensive measures impact a states strategic posture *vis-à-vis* another.

The mission of DTRA reflects a Cold War-era focus, on cyber technology as the immediate delivery of force: cyber attacks leaving destruction in their wake and concerns over mass effects. But cyber conflict is very different from kinetic conflict. With cyber techniques one can produce effects that are cumulative over long periods, amounting to damaging or subtracting from the productivity of an economy, or sectors of an economy, rather than its immediately perceived effects. A cyber weapon or cyber attack can be the functional equivalent of an explosive bomb planted in a computer remotely and activated at some later time, either as a single event or as a coordinated attack consisting of distributed events over time. A cyber weapon can impact not simply an economic metric but the rate of change of an economic metric.

Cyber weapons affect *information*, the raw material of perception and thus *de facto* reality. Influencing perceptions is not new, just the name is. This was previously described, accurately, as psychological operations. Pejoratively, it is called propaganda or deception. Cyber conflict can have a physical dimension as well, when the cyber malfunction occurs in the control systems of physical operations, where it can effect the destructive release of large amounts of kinetic, potential, or chemical energy. Such physical damage, thoughtfully planned, can result in the destruction of expensive and long lead-time physical facilities whose absence over long repair times is used to cause damage to an economy.²⁰³

Another route to wide damage from small cyber efforts can be through the selective attack of critical cyber nodes that have the greatest degree of connectivity, thereby affecting the reliability and responsiveness of communications.²⁰⁴ The most attractive targets are nodes in infrastructure systems providing universal service. These systems, when disabled, in turn impact into other critical systems that depend on them. Three such infrastructures that rise to the top of an attacker's target list are electric power, communication, and financial services.²⁰⁵

This approach to selecting cyber targets is the way to achieve mass effects. Yet unlike nuclear weapons, where the mass effect is achieved in a very short time, mass cyber effects can be produced both through critical node targeting and by persistent attacks over long periods of time. This is a very different perspective of an *attack* with a *weapon* than military forces have been trained to deal with. It has more in

²⁰³ Stephen J. Lukasik, "Natural Experiments Relating to the Destruction of Economies," SAIC report to DTRA for a Workshop on Economic Terrorism/Economic Warfare, January 5-6, 2006.

²⁰⁴ See Catherine A. Theohary and John Rollins, "Terrorist Use of the Internet: Information Operations in Cyberspace," Congressional Research Service report, March 8, 2011.

²⁰⁵ Stephen J. Lukasik, Seymour E. Goodman, and David W. Longhurst, *Protecting Infrastructures Against Cyber-Attack*, Adelphi Paper 359, International Institute for Strategic Studies, London, 2003.

common with Sun Tsu than with Clausewitz. Thus the question is, if the cyber domain is so very different, how can a state know where it stands *vis-à-vis* potential attackers? While states undertake net assessments of strategic nuclear postures, doing so for cyber force balances would seem to be impossible given that any mind with any computer can conceive and launch an attack, and many minds and many computers can launch large coordinated attacks. Thus a cyber *offensive force balance* is not meaningful. But if an offensive balance is *indeterminate*, it is possible to produce a *defensive force balance*. If one cannot prevent an attack, one can thwart an attack.²⁰⁶ There are three factors in cyber defense: the extent to which a state is "wired;" the extent to which a state has adopted networked automation for the operation of its economy; and outage statistics of its most critical economic systems.

Another net assessment metric is the *vulnerability production balance*. Automation and network enthusiasts aggressively pursue their visions, failing to recognize that two computers connected together pose more of a vulnerability than the same two computers not connected. Networking computers, especially when the networking is unlimited, leads to ever-increasing scales of complexity, and thus unintended consequences *produce* vulnerabilities. Adding protection, through any of several possible ways, reduces vulnerabilities. The ratio of the two production rates should be less than one.

This observation leads to another balance of strategic importance: the *connectivity balance*. Cyber conflict, at least between states, is measured by the net flow of attack packets between them. Unlike strategic nuclear weapons, attack packets are exchanged between all nodes continually. It is how cyber conflict would be undertaken, probing the cyber "order of battle," planting malware, harvesting the information obtained through malware, and testing vulnerabilities to determine if they have been modified in a way that calls for modifying weapons and attack plans. The structure of the international telecommunications networks is such that international gateways are regulated and each state has an agency responsible for overseeing its side of the interface. Thus data to assess connectivity balances are readily available in business and operational statistics.

Such a balance measures the degree of dependency of each state on the information resources of another state. Much like trade flows and capital flows, it can indicate a state's increasing or decreasing information strength and weakness. Cyber balances are dynamic, minute-to-minute (as in the May 6, 2010, stock market "instability,") or year-to-year.²⁰⁷ A global early warning system based on these cyber balances can provide a restoring force to keep the global cyber environment stable. Responses would be matters of both national and personal decisions.²⁰⁸

1.3 The Limits of Cyber Technology Forecasting

The time horizon of the subject study, 6-20 years, is an awkward fit for cyber technology. The usual starting point for cyber forecasting is to cite Moore's Law, which holds that the density of circuit elements on a chip doubles every 18 months. This technological trend is well established, despite periodic handwringing over the

²⁰⁶ Stephen J. Lukasik and Rebecca Givner-Forbes, "Deterring the Use of Cyber Force," December 14, 2009. Available at: http://www.cisip.gatech.edu/publications/files/cyber_deterrencev2.pdf

²⁰⁷ See "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, September 30, 2010.

²⁰⁸ Stephen J. Lukasik, "Reducing Threats to Users of the Global Cyber Commons," to be published by Communications of the Association for Computing Machinery, 2011.



end of Moore's Law and assurances that physical limits always spoil the fun.²⁰⁹ But cyber innovation continues and finds ways around these dire predictions, usually by changing the technological base, as from mechanical relays to electronic tubes to transistors to integrated circuits to opto-electronics to quantum dots.

By this line of argument, six years is four "generations" of doubling, a factor of 16. This is a rate of change unequaled in mechanical and chemical technology. Other rates such as storage density and transmission bandwidths, while relevant, benefit from the same cyber advances to reduce cost and automate production. Aside from technical measures, market innovation in consumer products, and the behavioral changes in attitudes influenced by social networks, increasing access and speed of market penetration mean that 20 years for cyber forecasting is unreasonable.

Between 1960 and 1980, computer development progressed from mainframes to personal computers. From 1990 to 2010, this evolution went from desktops and laptops to mobile wireless computing in smartphones.

Technology forecasters, in their preoccupation with the future, rarely look back to see how well they are doing. A study of technology forecasting in the 1890–1940 period presents a systematic (though by its nature not statistical) analysis of 1,556 public predictions in 18 areas of technology made by Americans concerning social, economic, and political effects.²¹⁰ The results were as follows:

Fulfilled	499	32%
In progress	121	8%
Not proven	420	27%
Refuted	516	33%

The study examined differences between experts and non-experts, and several other questions. The results are:

How well do predictors fare on their longer range efforts, those stretching ten or more years into the future?	They are right less than half the time (0.4)
Do experts predict better than non-experts?	Slightly, at best
Do some experts (non-experts) predict better than other experts (non-experts)?	No
Are predictions of the continuation of the status quo more accurate than predictions of change?	No
Can the effects of technological changes be predicted as accurately as can the changes themselves?	No

Since these dealt with technologies changing far less rapidly than cyber technology today, one must recognize that the answer to the first question is likely to be worse for cyber technology than the 0.4 reported. *Caveat emptor.*

²⁰⁹ For discussions of the limits of Moore's Law, see Victor V. Zhirnov, et al., "Limits to Binary Logic Switch Scaling—A Gedanken Model," *Proceedings of the IEEE*, Vol. 91, No. 11, November 2003; and Manek Dubash, "Moore's Law is Dead, says Gordon Moore," *Techworld*, April 13, 2005.

²¹⁰ George Wise, "The Accuracy of Technological Forecasts, 1890–1940," *Futures*, Vol. 8, Issue 5, October 1976.

1.4 Attempts to Predict Discontinuities

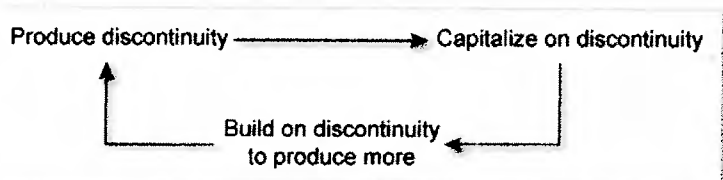
Studying the past, and given a deep understanding of technology, one is still at a loss to predict when a major change in a particular technology will occur, or even if one will occur at all. "Discontinuities" are often the result of crossovers in which the differing rates of rapidly changing quantities favor one process over another. Such game-changing events, which are so avidly sought for exploitation, are difficult (most would say impossible) to predict. Yet this need not leave one waiting for lightning to strike. If one cannot predict discontinuities, the most sensible approach is to set out to *produce* them. This approach has the leader benefitting from discontinuities before the followers, as well as the advantage of preparing the ground for their exploitation.

The process for producing discontinuities is simple in principle:

- ▶ Undertake as much R&D, public and private, as is economically sustainable;
- ▶ R&D can be both planned and controlled but also have a large uncontrolled component;
- ▶ Such innovation requires marketing the results;
- ▶ It thus depends on personal as well as organizational incentives;
- ▶ It requires adequate physical facilities and support services;
- ▶ It requires that venture capital, both public and private, be available;
- ▶ There must be economic and political freedom to distribute incentives to all levels;
- ▶ There must be a degree of personal empowerment;
- ▶ There must be a cultural acceptance of change over status quo;
- ▶ There must be a dragnet to attract people and ideas from everywhere.

That discontinuities are so rare is a result of these conditions rarely occurring together. And, while it is easy to summarize the necessary conditions, in practice the policy process is messy.

The process has an important element of feedback:



As an example of the process, a significant discontinuity occurred when the Soviet Union launched the Sputnik satellite in 1957. The United States capitalized on this event to rejuvenate its own moribund space program and in 1969 landed a man on the moon, leaving the USSR behind in the space race. In addition, it established an agency (ARPA) to produce discontinuities, the feedback loop in the diagram above. So discontinuities do not convey permanent leadership. To the winner this is a warning, and to the loser it is an opportunity to recover because it changes his bias away from sticking with the status quo.

One might, in analogy to Newton's laws of motion, suggest:

- ▶ To every disciplinary discontinuity there is an equal and opposite discontinuity;
- ▶ Disciplines at rest tend to remain at rest;
- ▶ Discontinuities are driving forces in disciplines. They occur when disciplines overlap.

Cyber technology is fruitful and dynamic because:

- ▶ Virtually all physical phenomena can be described digitally;
- ▶ Digital interfaces between devices and digital objects are easy to define and build;
- ▶ Easy interfaces facilitate connection of systems into larger systems of systems;
- ▶ Systems of systems are important to the extent they are scalable.

Thus, "cyber" is *not* a technology; it is a process of enormous generality. It is a game of leapfrog where all sides receive the benefit of discontinuities. But the benefits are not the exclusive property of anyone for very long. The essence of technological leadership is to build the next discontinuity before others can build their response to the first.

AI. BOTNET TECHNOLOGY

Botnets are the result of the easy scalability of systems of computers into larger systems of systems. Many computers are protected professionally, sequestered behind firewalls with strong encryption of robust user passwords required and maintained by having virus and intrusion protection software installed and updated. However, less protected machines, typically in homes, small businesses, and in mobile devices such as web-capable cell phones, tablet computers, and other mobile and autonomous devices, are not well-protected. Through "phishing," deceptive email with attachments containing executable code, or by clicking on an apparently reasonable link, malware can be downloaded into a computer. E-commerce depends on an interaction with a seller's website, and this can result in the installation of software to capture user actions, such as searching and purchases. Such information can be reported back to the seller. Use of Web browsers can result in unearthing sites one might otherwise never access, and this increases the chance of encountering malware. Even protected computers and sites can be overwhelmed by traffic sent from individual unprotected users. One recent development is to capture Facebook accounts for distributing spam. An alternative is to set up phony accounts. Both work. It is simply a matter of design tradeoffs.²¹¹

When captured, computers or accounts are used to send spam to the address lists in the device/service or using URLs and addresses sent to it. Such botnets can be used for distributed denial of service attacks when their transmission capacity is directed to target IPs or URLs.²¹²

²¹¹ Hongyu Gao, et al., "Detecting and Characterizing Social Spam Campaigns," ACM Internet Measurement Conference, November 1-3, 2010, Melbourne, Australia; reviewed in *M.I.T. Technology Review*, January-February, 2011. p. 89.

²¹² For additional information, see Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," Congressional Research Service report, January 29, 2008.

A1.1 The Malware Industry²¹³

The malware industry is spread across the globe and is heavily populated by technically-organized programmers from Russia and eastern Europe, often in league with organized crime syndicates. Malware is not, as many seem to assume, the work of high school students and programmers mischievously entertaining themselves. Rather, it is largely professionally organized. Malware stays in contact with its controller and can be changed as desired. It is thus an "insider," though without any employee relationship to the computer in which it resides. Updates are digitally-signed encrypted communications transmitted through Web-servers and newsgroups.

The participants in these criminal enterprises buy serious expertise: spam vendors employ professional linguists to bypass filters, and phishers use psychology graduates to scam victims. Employees can earn more than \$200,000 per year. Remote root zero-day exploits sell for \$50,000–\$100,000. There is an organized recruiting system. Russian script kiddies' activities are noticed by an Internet service provider (ISP), which reports them to a Russian mafia contact. The mafia visits the script kiddie and recruits him for profit or through coercion. As an illustration of the technological sophistication of these enterprises, Windows Vista attacks were available for \$50,000 one day before Vista was released. Malware is focused on the most popular software products. Microsoft Internet Explorer attacks are far more profitable (80% of the market) than Firefox attacks (20% of the market). Market share is the key malware targeting criterion.

Webmasters and adware vendors are paid to infect users with spyware, keystroke loggers, and trojans. A webmaster that allows his site to be used is generally paid 6¢ per infected machine. Adware can operate faster than Google can return a search, substituting a different product or directing the search to favor its products. Piggyback malware can collect credit card numbers, Social Security Numbers, usernames, and passwords. Try-before-you-buy deals offer 100 free visitors to infect before the malware supplier charges for use of the malware. Payments to malware vendors are done online but use a more secure Russian version of PayPal.

The malware industry outsources everything possible. A spammer pays for the use of botnets for a scam. He buys spam to lure victims. He buys drops to which victims' money is sent, and he pays to cash out the accounts. Carders collect personal information and sell it to other vendors to print fraudulent cards for sale wholesale, which are later resold retail. Malware vendors sell their work and outsource their products to others who verify that it will elude detection software. The system is highly decentralized, and this makes it fault-tolerant and difficult to contain. The money resides with the middleman, or as we put it in the defense business, the system integrators. It is a totally commercial, if illegal, business. Spammers have their own trade associations. Prices are openly published but are subject to private negotiation. There are eBay-style reputation rating systems. Funds are often moved through compromised bank accounts to launder them. Blocks of unassigned IP addresses can be purchased.

Malware depends for its operation on very smart people who are able to cover their trail and works because computer security is poor and, even when available, is not employed by the technically unsophisticated people who make up the bulk of Internet users. Consumer products labeled "smart" (e.g., phones, vehicles, and electric grids)

²¹³ This section is drawn from Peter Gutmann, *op. cit.*

are not as smart as advertised. The really smart can out-smart them. Only dumb people think such systems are smart. Among the dumb people are many managers. An abstract of a presentation at the Annual Computer Security Applications Conference 2010 reads: "Over the past year, we have systematically scanned large portions of the Internet to monitor the presence of trivially vulnerable embedded devices. We have identified over 540,000 publicly accessible embedded devices configured with factory default root passwords. This constitutes over 13% of all discovered embedded devices such as Voice over Internet Protocol (VoIP) adapters, routers, firewalls and enterprise equipment ... One important observation we make reveals a struggle between the efficiency of large-scale management of consumer devices and the security of those devices."²¹⁴ CNN carried a story of the 2011 Consumer Electronics Show about "smart" products including washing machines, refrigerators, ovens, and weight scales. Systems of systems opportunities would extend them to home energy management systems.²¹⁵ The dumb shall inherit the earth.

A1.2 Cyber Offense Systems

Just as the mafia took over the corner news stand numbers business in the United States and "organized" it through death threats, and then governments took it over and renamed it Lotto, a similar transition from cyber scrip kiddies to the malware industry to governments is underway. Russian attacks on Estonia and Georgia are cases in point.²¹⁶ The U.S. Cyber Command is an example of this phenomenon, with many other governments doing the same. The Stuxnet worm, plausibly attributed to a joint U.S.-Israeli operation against the Iranian nuclear program, is a possible instantiation.²¹⁷ "Stuxnet is the start of a new era," says Stewart Baker, former general counsel of the U.S. National Security Agency. "It's the first time we've actually seen a weapon created by a state to achieve a goal that you would otherwise have used multiple cruise missiles to achieve."²¹⁸



Consider a set of cyber weapons that may be as significant if they are built (if they have not already been) as were ICBMs carrying megaton nuclear weapons in the 1960s. If botnets are the distribution system of malware, and malware can, when scaled up, turn off or on what one does not wish turned off or on, such as electric power or one's stock portfolio, then the obvious culmination is the supersize botnet.

It is beyond the scope of this analysis to calculate the minimum size of a botnet adequate to turn off or on industries and economies. However, at some point, control of traffic on the Internet, because the net contains virtually all of the control signals that enable modern societies, even relatively undeveloped ones, to operate, is a powerful on-off capability. But is it capable of modulation? Can it turn off Iran's

²¹⁴ Ang Cui and Salvatore J. Stolfo, "A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan," Paper presented at the Annual Computer Security Applications Conference 2010, Orlando, Florida, December 6-10, 2010.

²¹⁵ John D. Sutter, "When refrigerators tweet and washing machines test," CNN, January 8, 2011.

²¹⁶ Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *New York Times*, May 29, 2007; and John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 13, 2008.

²¹⁷ William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

²¹⁸ Christopher Dickey, R. M. Schneidman, and Babak Dehghanpisheh, "The Shadow War," *Newsweek*, December 13, 2010.

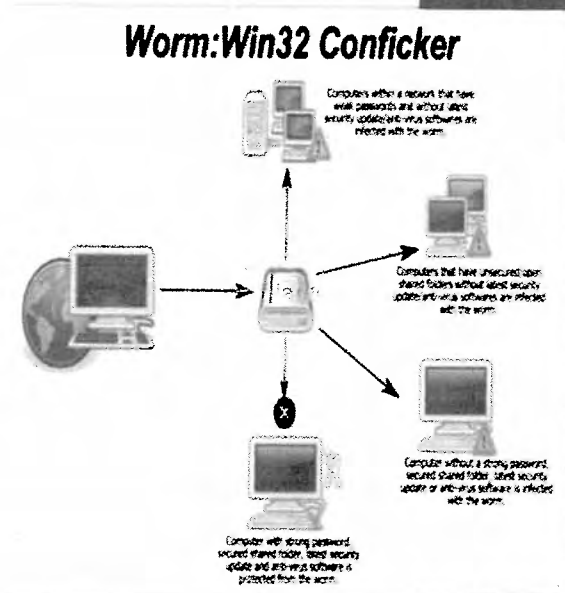
sector X without causing intolerable harm to another country's sector Y? Globalization and the interdependence of infrastructures makes this difficult to decide at this point in our understanding of economies.²¹⁹ But just as continuous aiming fire control systems improved naval gunnery and terminal guidance improved the accuracy of ordnance delivery, it is not unreasonable to expect that sophistication in macroeconomics will eventually result in mastering the art and science of cyber-enabled economic warfare.

Granting this, one will be led to large-scale offensive botnets for selective or global manipulation of social control systems. The question is simply one of the "fabrication" and "deployment" of large botnets. The largest botnet identified to date is that under control of the Conficker worm, which "infects" at least six million computers worldwide.²²⁰ If there are, say, three billion computer targets in the world that serve a world population of seven billion people, one might estimate that 100 million computer botnets could, if effectively used, tie up the Internet worldwide on demand, essentially closing or slowing it down when and where desired or threatening to do so to coerce a government or coalitions of states.

Large botnets can be constructed by states (or, equally worrisome, by sub-state groups) in two ways. The first is the way they are constructed now, computer by computer, by means of the malware techniques previously described. Following the mafia example, and probably the Russian and Chinese models, states would "enlist" their malware practitioners who are clearly doing "good" work. Or, an entity such as Cyber Command could undertake a similar program, aided in no small measure by U.S. legal, contracting, and regulatory authorities and influence.

The second approach is to build a large botnet *ab initio*. "Capturable" computers can be built and deployed in large server farms much as Google and other cloud operators have done. Such server farms could be used for all the purposes of large-scale computation that the government currently requires them for. Or one could lease commercial server farms for the relatively brief periods needed to conduct cyber offensive operations. This suggestion is not unique to the United States. While the costs are not like the costs of the U.S. nuclear forces and their supporting intelligence and weapon design components, it is probably a great deal less costly and certainly easier to conceal.

The construction of large botnets for offensive operations has a curious feature. A single captured computer can be used by more than one botnet (so states embarking on such national programs need not worry about running out of computers to



²¹⁹ In addition to Iran, the Stuxnet virus is known to have affected computers in Indonesia, India, Australia, Malaysia, Pakistan, the United Kingdom, and the United States. See Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec, Version 1.3, November 2010. Additionally, some concern was expressed after the Stuxnet attack that the virus could spread to Iran's Bushehr nuclear power plant and possibly cause a Chernobyl-like disaster. See, for example, Ramin Mostafavi and Robin Pomeroy, "Iran Says Stuxnet Claims Need Investigating," *Reuters*, February 4, 2011.

²²⁰ Mark Bowden, "The Enemy Within," *Atlantic Monthly*, June 2010.

capture.) Thus an early “theater of cyber operations” can be in each of our own home computers, where A’s botnet control software will have to struggle against B’s and C’s if several seek to use the computer simultaneously. Since operating systems are designed to contend with competition for computer resources, it is quite possible that each computer operating system will succeed in accommodating the needs of all the ongoing cyber conflict’s participants. This would be the equivalent of NATO and Warsaw Pact countries sharing airfields and maintenance facilities during a Soviet advance into Western Europe.

This description is intended simply to point out that cyber conflict is very different from conventional conflict, a point made earlier.²²¹

A2. GAME-CHANGING QUALITIES

The offensive side having been addressed above, the game-changing qualities of botnets depend on the degree to which defenses can be conceived and deployed. Defense can be preventative, such as deterrence, or it can involve hardening, to make malware difficult to transmit or emplace. It might also consist of real-time systems for situation awareness and enhanced defensive measures or counter-force responses, again all beyond to scope of this analysis but discussed in earlier references.²²²

Captured machines are difficult to diagnose because their capture does not impact their performance when the botnet operator is not actively using a machine. Since the captured machines are typically not owned by technical experts and thus are rarely serviced professionally, they are akin to a gun whose serial number has been obliterated.

Even relatively short network interruptions will be effective against time-sensitive connections such as:

- ▶ Financial transactions, which in automated trading can be “too late” if delays are of the order of usec, introducing a new weapon for economic warfare;
- ▶ Voice communication as VoIP becomes the dominant form of telephony and switching, critical for crisis responses and infrastructure operations;
- ▶ 911 service, medical diagnostics, delivery of therapy, remote surgery, and long-term health care;
- ▶ “Black start” after a regional power or other infrastructure interruption.²²³

Large botnets are assessed below through the lens of the “game-changing” qualities template described earlier in the report.

- ▶ **Reduced Barriers to Entry.** Barriers to entry are currently low to zero. Botnets are relatively easy to establish or build. One simply scans the Internet looking for unprotected machines to direct email with links that download the software to capture the machine.

²²¹ Lukasik and Givner-Forbes, op. cit.

²²² Stephen J. Lukasik, “A Framework for Thinking About Cyber Conflict and Cyber Deterrence, With Possible Declaratory Policies for These Domains,” *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policies*, National Academies Press, 2010.

²²³ “An Introduction to Black Start,” National Grid Company, PLC, February 2001.

- ▶ **System Integration.** There is no novelty here in the concept of botnets, which are ubiquitous and well understood. Estimates are that 20 percent of all computers today have been captured and are used in botnets.²²⁴ The novelty arises in the possibility of very large botnets and their virtually undetectable nature. The relevant tactical and strategic doctrine will require study.
- ▶ **Novel Delivery Means.** None. Botnets have been demonstrated by virtue of the plethora of spam. Spam is a very simple example of working on a target population psychologically. Enhancing one's self-image with a fake Rolex or one's physical performance through cosmetic surgery are quite elementary forms of the psychology of advertising. There are likely to be more sophisticated approaches developed to capitalize on the connectivity the Web offers. A number of cyber attacks that work against the morale of a state have been discussed elsewhere.²²⁵
- ▶ **Self-propagation.** The malware that "captures" a machine is the result of two voluntary actions by a user. The first is to choose not to prevent malware from loading, and the second is to click on a link or load software for which there is an expectation of non-malicious content. It is an open question whether a captured computer can capture others.
- ▶ **Novel Radical Empowerment.** This capability empowers individuals and sub-state groups, although fabrication of large botnets may remain the province of larger nations. However, as the cost of devices and bandwidth continue to drop, the pool of potential candidate nations and groups will grow.
- ▶ **Mitigation of Effects.** It is possible to build into application programs and operating systems limits on traffic and transmission rates

A3. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY DEVELOPMENT

A3.1 Driver

The chief driver of this technology is the easy exploitation of weak Internet security for cyber crime and cyber conflict.

A3.2 Counter-drivers

Development and wide adoption of strong network security technology. Conventions to make the exploitation of anonymity and of international jurisdictional differences more difficult would aid in the maintenance of law and order would help, however much they would be resisted. Another counter-driver would be international agreements to aid in detection, pursuit, apprehension and punishment of malicious actors

A4. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY ATTRACTIVENESS

Accessibility. Security always poses inconvenience to Blue users; there is also a lack of technical knowledge by the bulk of Blue users. U.S. government policies also

²²⁴ In 2008, analysts at the Georgia Tech Information Security Center estimated that botnet-affected computers comprised as many as 15 percent of online machines. See "Emerging Cyber Threats Report for 2009," Georgia Tech Information Security Center, October 15, 2008. Vint Cerf, often referred to as one of the "fathers of the Internet," estimates that as many as 150 million of the 600 million connected computers on the planet, or 25 percent, are part of botnets. See Tim Weber, "Criminals 'may overwhelm the web,'" BBC News, January 25, 2007.

²²⁵ Stephen J. Lukasik, "Mass-Effect Network Attacks: A Safe and Efficient Terrorist Strategy," SAIC report to DTRA, January 2007, pp. 24-33.

constitute Blue constraints, both in their failure to mandate security but also to minimize the use of security measures for reasons of cost and convenience. The technology is quite attractive to red at the lower levels of attack capabilities.

Signature. Detection of the presence of penetration is through observed operations and national losses due to lack of security. But this might be analogized to locking the barn door after the horse has been stolen. There is the possibility of detecting malware proactively during its installation and testing. It is difficult to identify attackers and their location if more than the state of origin is needed.

Ability to deploy. Presently it is relatively easy for attackers to deploy botnet attack technology. It is difficult and expensive for defenders to deploy large-scale defenses.

Efficiency. Captured computer botnets are cheap for attacker. Fabricated botnets are also relatively inexpensive, but there are non-trivial costs for scale-up. Defenses are likely expensive or difficult to deploy with high degrees of user cooperation, but not impossible.

A5. CONCLUSION: RELEVANCE TO DTRA MISSION

The relevance to DTRA's mission is unclear at this point. In discussions with a former DTRA director, the view emerges that other agencies (e.g., the National Security Agency, Department of Homeland Security, Defense Advanced Research Projects Agency, National Science Foundation, etc.) were the main actors in cyber defense, and DTRA would stay with its CBRN/WMD domain, where it has expertise. A substantial DTRA role in cyber matters would require some amount of internal discussion and planning before broaching such a proposal.

Cyber security is a delicate subject in the U.S. government at this point, and a "turf war" has been ongoing for at least a decade. This struggle is focused almost entirely internally and concerns matters of fundamental policy.²²⁶ For example, a broad DoD role in national cyber defense is unclear. Despite the lengthy period of study since cyber conflict became apparent, no substantive progress has occurred in improving national cyber protection broadly. In fact, quite the opposite is the case. Cyber security has experienced a monotonic decrease.

Much of this is due to the fact that advancing cyber technology that enhances its constructive use equally benefits those who use it destructively. The destructive users are small and highly effective groups while the constructive users are either large cumbersome groups or large numbers of uninformed individuals. This state of affairs is cheerfully ignored or downplayed by cyber technology enthusiasts whose motivations are to advance the power of information technology and to develop its business potential for organizational and personal benefit.

B1. CIRCUIT BOARD HACKING

B1.1 Outline of Circuit Board Electrical Power Vulnerabilities

The flow of information in a computer is controlled by changes in electronic states in its memory and logic elements as they operate on each byte of data during each

²²⁶ For additional information on current U.S. cyber defense policy, see Gregory C. Wilshusen, "Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems," Testimony before the House Committee on Homeland Security, Government Accountability Office report GAO-11-463T, March 16, 2011.

machine cycle. The 0/1 values of each bit correspond to ~0.1 volt at the physical level. The corresponding currents to effect these changes result in ohmic heating of resistors, board wiring, and interface connectors, and this constitutes a large part of the power consumption of a computer.

Internal voltage levels must be controlled to better than this to prevent statistical fluctuations in currents, called quantum noise, from randomly changing either data or program bits. Most importantly, too large a voltage will burn out a transistor on a chip. Internal voltage levels are controlled electronically, either at a facility power source, a work area power source, or its distribution point on the circuit board itself. Voltage levels, however provided, are controlled by programmable logic that can be hacked into through malware. Thus centers, computers, boards, and chips can be caused to destroy computing devices, rendering them inoperative. Proper power supply design assures that, absent malicious actions, this will not occur.

Some power malfunctions can be corrected by rebooting the device to continue processing. But burnout of a circuit element requires replacement, usually of the entire board. Maintaining adequate level of spares close by would impose enormous economic burdens to avoid a lengthy process of manufacturing and distribution through what is usually a global supply chain. While this supply chain always has some inventory in stock at all levels, replacement of large numbers of damaged devices takes time. If the circuit board attack is sufficiently widespread, as occurs when a server farm supporting cloud computing is attacked, the cumulative damage can overwhelm global supply chains.

BI.2 Channels for the execution of circuit board attacks

- ▶ Digital intervention at the program level, either by outsiders or insiders. This can include such attacks launched by botnet-distributed software;
- ▶ EMP, including implanted or embedded micro-size EMP generators;
- ▶ Physical attacks on inadequately redundant systems;
- ▶ Attacks on the power systems of automated production and logistics facilities;
- ▶ Stuxnet-type attacks on the control systems of the central power grid to produce wide area power fluctuations and failures.

Smart grid developments and smart home appliances will greatly increase the number of attack entry channels that can be utilized, thus increasing the risk of serious widespread system interruptions.

B.2 GAME-CHANGING QUALITIES

Destruction of basic functionality of “enough” computers will render information services inoperative and thus the physical operations and decision-making they support once the easily accessible supply of spare circuit boards is exhausted. Such interruptions can be lengthy ($\geq$ month) when damaged components have long lead times and are uneconomical to stockpile. An advanced attack might also target the supply chain computers used in automated production for ordering components and shipping products.

When global supply chains are examined, one finds that despite what appears to be intense competition, the competitiveness “necks down” at the level of critical components. For example, two companies in Taiwan supply basic components used in all personal computers. Simultaneous cyber, physical, or political attacks on these

sources will further add to global supply chain disruption. Such an attack is asymmetrical. Advanced states will be more susceptible than smaller, weaker, and lesser-wired states. Since many specialized targets such as infrastructure contain special purpose devices such as interfaces with field facilities having small supply bases, the scale of the attack needed will be less, and thus more feasible.

- ▶ **Reduced Barriers to Entry.** The barrier to entry to carry off such attacks can be small. Botnets are relatively easy to establish. Malicious software is relatively easy to write and costs little compared to the magnitude of the effects that it can produce. On the other hand, if the attack were to depend on implanted micro-EMP devices, the attack would be more complex and thus less feasible.
- ▶ **Novel Delivery Means.** Power supply failures are experienced but are seen as random failures: natural causes, accidents, or operator error. Concerted power supply attacks to deny the use of information technology to a state for a long period have not been reported in the unclassified literature.
- ▶ **Self-propagation.** At higher system levels, such attacks can be subject to cascading due to the heavy degree of integration and interdependence of systems in advanced societies.
- ▶ **Novel Radical Empowerment.** In principle, this capability empowers individuals and sub-state groups. However, as a practical matter, the most worrisome attack is more likely to involve advanced states that are capable of the substantial degree of planning required.
- ▶ **Mitigation of Effects.** The possibility of self-destructing boards has been mentioned in the technical discussions. Once mentioned, it is simple to adopt its avoidance as a design principle. But negation will be costly to redesign boards, reequip board production facilities, overcome market inertia, and change legacy systems. Market economies resist investments intended to protect against hypothetical events. Individuals are unlikely to be able to internalize the problem nor are they able to undertake sophisticated countermeasures, though they may be easily frightened into avoiding certain products. For this reason manufacturers are likely to talk down the issue, though they will quietly seek to avoid the problem without having to bear the burden of a costly product recall.

B.3 DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY DEVELOPMENT

B3.1 Drivers

Drivers will be rapid expansion of a part of the information technology market where both manufacturers and buyers are unsophisticated. Some of the smart domestic consumer products may be in this class. On the other hands, these markets focus on short product lifetimes, and constant changes in products to accommodate changing consumer choices.

B3.2 Counter-drivers

The chief counter-driver is the "Who cares?" attitude by both manufacturers and buyers as increasingly technical illiterate people base their lives around a dependence on technology they are unable to, or do not take the trouble to understand.

B.4 DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY ATTRACTIVENESS

Accessibility. As with many cyber attacks, there is an asymmetric character to them

because the manpower, basing, and capital costs are so low that being small is not disadvantageous. In fact, being small, particularly for sub-state groups, has an advantage because cyber aggression does not put their entire organization at risk.

Signature. The difficulty of attribution when sub-state groups mount cyber attacks makes attacker signatures difficult to establish. The current situation, with mainly sub-state actors in the malware business, points to the attractiveness of any cyber attack to Red. With Blue, cyber attacks have to be coordinated with larger diplomatic, political, economic, and military moves, all of which will leave further pointers to a Blue signature.

Ability to deploy. Currently terrorist use of cyber attacks is quite limited. But the skills are relatively easy to acquire, especially by next-generation terrorists who are currently teenagers. Blue already has massive skill upon which to draw.

Efficiency. The cost exchange ratios favor Red since the attacks are low cost and Blue has a great deal to lose but limited desire to protect itself.

B.5 CONCLUSION: RELEVANCE TO DTRA MISSION

While DTRA reluctance to jump into the cyber fight will be present, especially in the face of near-term expected reductions in the DoD budget and the need to protect their existing missions, the case for mass destruction and mass effects is much stronger for critical facilities than it is for national cyber defense in general.

QUANTUM COMPUTING APPLICATIONS

VICTOR OANCEA, PH.D.

"The machine does not isolate man from the great problems of nature but plunges him more deeply into them."

– Antoine de Saint-Exupéry, 1939

I. TECHNOLOGY OVERVIEW

In the early 1980s, Richard Feynman pioneered the idea that computing devices of atomic scale—"quantum computers"—could be constructed. According to the initial vision, a quantum computer would be able to perform tasks that no computers of current design could achieve. Its most powerful feature would be its "quantum parallelism," which would allow the execution of certain types of calculations in a fraction of the time that a standard computer requires.²²⁷

Quantum computing, which involves the use of individual atoms as switches (the quantum analogue of the classical bit is the "quantum bit," or the "qubit"), has significant implications for the expansion of network-based applications requiring powerful processors, high-density storage, and high-speed switching. For example, the average number of calculation steps that an existing computer requires to find an item in an unsorted list of say $N = 1,000,000$ entries (i.e., finding a name in a database) is of the order $O(N/2) \sim 500,000$. By contrast, a quantum computer takes only 1,000 steps to find a name in a similarly sized list. One qubit can simultaneously represent two different values, two qubits can represent four values (00, 01, 10, and 11, in binary notation), four qubits can represent 16 values, eight qubits can represent 256 values, and so on. Even a relatively small quantum

²²⁷ R.P. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics*, Vol. 21, 1982.

computer, one having a few tens of thousands of qubits, could simultaneously represent an enormous number of different values, thus reducing processing time by the same factor.

This paper explores the implications for DTRA that are associated with the capabilities that quantum computers may one day provide. The technical state of development of technologies through which quantum computation can be accomplished has been extensively covered in the literature and will not be summarized here.

Qubits can be the atoms, ions, photons or electrons, as well as specific control devices that correspond to the computer memory and the processor (e.g., the central processing unit [CPU]). Quantum computers encode information in the quantum-mechanical states (e.g., spin directions of electrons, polarization orientations of a photon, etc.), which might represent a 1 or a 0, a combination of zero and one, any state of the qubit between 1 and 0, or a superposition of many different states.

Hydrogen atoms could be used to store bits of information in a quantum computer. An atom in its ground state, with its electron in its lowest possible energy level, can represent a 0; the same atom in an excited state, with its electron at a higher energy level, can represent a 1. The atom's bit, 0 or 1, can be flipped to the opposite value using a pulse of laser light. If the photons have the same amount of energy as the difference between the electron's ground state and its excited state, the electron will jump from one state to the other.²²⁸

At the core of a quantum computer are quantum logic gates. A quantum logic gate, like a classical gate, is a very simple computing device that performs one elementary quantum operation (i.e., AND, OR, XOR), usually on two qubits, in a given time. Quantum information can be destroyed through interactions with the surrounding environment, referred to as decoherence. Because this effect is irreversible, it is a difficult engineering endeavor to keep the qubits' interactions isolated from the surrounding environment.

Qubits in quantum computers are set to one of their possible states by using control devices. Currently, several technologies are being explored that have the potential to support quantum computation, i.e. having low decoherence levels. Today simple quantum logic gates involving two qubits are being routinely realized in laboratories.²²⁹ Among the most used techniques to create logic gates are those that rely on trapped ions via atoms in an array of potential wells created by a pattern of crossed laser beams, or electrons in semiconductors. The most used quantum devices, which can control the state of the atoms, ions, photons or electrons used in quantum computing (i.e. qubits), are:

- ▶ **Ion traps:** use optical or magnetic fields (or a combination of both) to trap ions;
- ▶ **Optical traps:** use light waves to trap and control particles;
- ▶ **Quantum dots:** made of semiconductor material and used to contain and manipulate electrons;
- ▶ **Semiconductor impurities:** contain electrons by using "unwanted" atoms found in semiconductor material;

²²⁸ S. Lloyd, "Quantum-Mechanical Computers," *Scientific American*, 1997.

²²⁹ D. James, "Quantum Computing Technology," LANL/Quantum Institute, 2008.

- ▶ **Superconducting circuits:** allow electrons to flow with almost no resistance at very low temperatures.

A leading implementation of quantum computers uses the ion trap technique.²³⁰

Quantum computations are inherently prone to errors due to the imperfect isolation of quantum mechanical systems from the environment. As a result, several error correction schemes have been developed to allow quantum computations to be performed free of errors.²³¹

Realization of Quantum Computers

In quantum computing, a large number of 2^N parallel computations are performed, but only one of the corresponding output values will be measured. This type of calculation can be done only by specially designed "quantum" algorithms, which are able to exploit the innate quantum parallelism, and thus use exponentially fewer steps than is possible by classical computer algorithms.²³² Some of the best-known quantum algorithms are:

- ▶ **Shor's algorithm (1994):** Efficiently finds the prime factors of large integer numbers. For a classical computer algorithm, the time needed to decompose a large number into its prime factors increases exponentially with the length of the number (on this fact is based most of the current cryptographic codes). For quantum computing algorithms, this time increases only by polynomials, which makes some of the most used cryptographic algorithms prone to decode.
- ▶ **Grover's algorithm (1996):** Offers a quadratic speed-up for unstructured search problems.

The design of quantum algorithms is as important as their physical realization and can potentially be the limiting factor in the delivery of quantum computing capabilities. The following are the basic requirements for any quantum system to be adequate for building a practical quantum computer:²³³

- ▶ A scalable physical system with well-characterized qubits,
- ▶ Initialization of the qubits to a well-known state,
- ▶ A universal set of quantum logic gates,
- ▶ Read-out of the qubits, and
- ▶ Coherence times long compared to the typical gate duration.

It is a great challenge to satisfy these criteria, as one would need to access the qubits so that they can be initialized, manipulated, and their state read out, while at the same time, isolated from the environment as much as possible to maintain their coherence. Currently, due to these practical difficulties, most quantum computers have been built in laboratory environments; until now, they have only been used to solve trivial problems.

²³⁰ A group working on a project to build a quantum computer with 20 to 50 ions in one or more ion traps is currently funded by the Intelligence Advanced Research Projects Activity; the goal is to build such a quantum computer in five years.

²³¹ This is analogous to the use of error correcting codes (ECCs) to address noise and other errors in communications circuits.

²³² D. Bacon and W. Van Dam, "Recent Progress in Quantum Algorithms; What quantum algorithms outperform classical computation and how do they do it?" *Communications of the ACM*, Vol. 53 No. 2, pp. 84-93.

²³³ DiVincenzo, D., "Quantum computation," *Science*, Vol. 270, 1995, p. 255.

The largest quantum computer to date is made up of eight ions in an "ion trap," a device that uses an electric field to capture the ions.²³⁴ As of December 2010, the most advanced prototype quantum computer chip is built by D-Wave Systems in Burnaby, Canada; it is designed to handle 128 qubits of information. The data is stored in 128 superconducting niobium loops as either a clockwise or an anticlockwise current.

Quantum Computing Technology Development Timeline

As a point of comparison for quantum computing technology development, one can refer to the history of evolution of the classical computation: basic principles were set in early 1930s, early laboratory implementation occurred over the next 10 years, commercially viable devices were created within the next decade, and, roughly 50 years later, classical computation ascended to its dominant role in the world economy. To extrapolate a similar temporal evolution of a quantum computer, in 2004 there were 155 quantum computing research projects in the public domain.²³⁵ In 2004, the Quantum Information Science and Technology Experts Panel of the U.S. Advanced Research and Development Activity (ARDA), with contributions from experts of the U.S. Army, Air Force, Navy, and the National Science Foundation, estimated that large quantum computers could become practical in 10-20 years.^{236,237} In 2008, several experts estimated that the use of quantum information technologies in business computing will become possible in the next decade.²³⁸

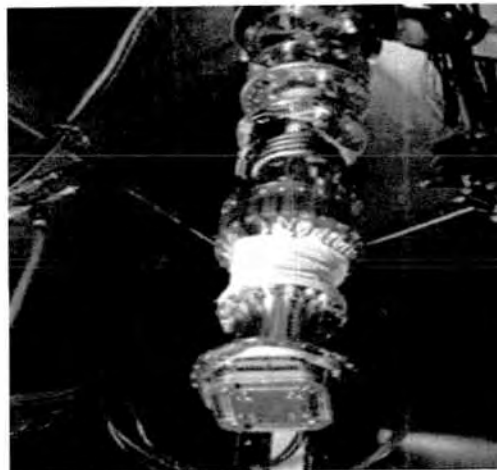


Figure 1: D-Wave 16-qubit quantum computer "Orion."

(Source: D-Wave Inc., "D-Wave quantum computers operating processors available today with 128 qubits, <http://www.dwavesys.com/index.php?page=quantum-computing>)

In summary, the objectives of the quantum computing roadmap can be accomplished within a decade, at least for a fault tolerant device on a small scale. For larger scales, reaching a reliable fault-tolerant regime would imply the ability to create registers of

²³⁴ D. James, op. cit.

²³⁵ A. Shields, "Quantum Cryptography breakthrough heralds un-crackable communication networks," Toshiba Research Europe Ltd., Cambridge Research Laboratory; April 19, 2010, Cambridge, UK.

²³⁶ "A Quantum Information Science and Technology Roadmap," ARDA, LANL LA-UR-04-1778, April 2, 2004.

²³⁷ Quantiki Contributor, "Introduction: the Major Visions and Goals of QIPC," December 2010. Available at: http://www.quantiki.org/wiki/Introduction:_the_major_visions_and_goals_of_qipc

²³⁸ S. Lloyd, "Riding D-Wave," MIT Technology Review, May/June 2008.

sufficiently many physical qubits to support logical encoding and to perform qubit operations within the fault-tolerant precision thresholds²³⁹.

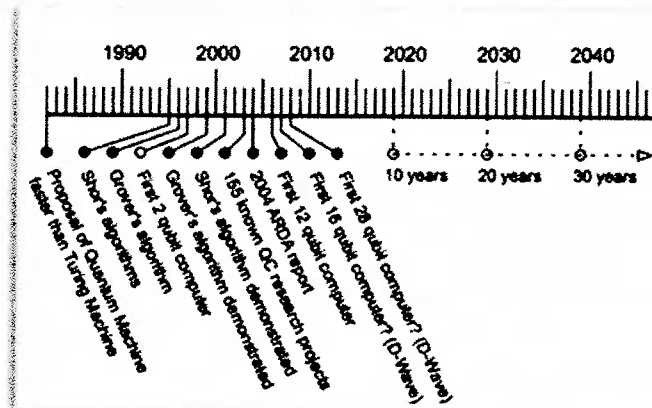


Figure 2: Development timeline of the quantum computers technology

(Source: R., Kelson and B., Gittins, *Proprietary Technologies to create 50-to-100 year including Post Quantum: Secure Communications Infrastructure and Secure Collaboration Applications such as e-mail, Instant Messaging, and VoIP*, Synaptic Laboratories; 2009)

Realization of small quantum computers of less than 50 qubits with fault-tolerant scalability, but still within the basic science regime, will require both experimental and theoretical advances, among which the following are the main components:

- ▶ Creating deterministic, on-demand quantum entanglement;
- ▶ Encoding quantum information into a logical qubit;
- ▶ Extending the lifetime of quantum information; and
- ▶ Communicating quantum information coherently from one part of a quantum computer to another.

Realization of larger quantum computers that are greater than 100 physical qubits and are able to perform real applications will require the technological ability to create registers of sufficiently many physical qubits to support logical encoding and the ability to perform qubit operations within the fault-tolerant precision thresholds. These benchmarks will be networked to extend quantum computers into the test-bed regime, which will allow for the experimental exploration of architectural and algorithmic issues. Such larger quantum computers would allow for quantum simulation as originally envisioned by Feynman—the implementation of distributed quantum computers in classically networked arrays advantageous for partial differential equation solutions, even though, compared with other quantum computing applications, no exponential or polynomial speed-up would be possible.²⁴⁰

In order to achieve the physical implementation of a quantum computer, several scientific approaches will emerge. Not all approaches will be successful; however, even those that do not ultimately contribute to the quantum computer will play important supporting roles by exploring different ways to implement quantum logic.

²³⁹ A. Shields, "Quantum Cryptography breakthrough heralds un-crackable communication networks," Toshiba Research Europe Ltd., Cambridge Research Laboratory; April 19, 2010, Cambridge, UK.

²⁴⁰ "A Quantum Information Science and Technology Roadmap," ARDA, LANL LA-UR-04-1778, April 2, 2004.

To date, small quantum computers have been developed in several laboratories around the world, and their evolution and the consequent cross-hybridization between various approaches to the quantum computing problem continues and advances.²⁴¹

2. GAME-CHANGING QUALITIES

Based on its potential applications, quantum computing technology is assessed to have the following “game-changing” qualities:

- ▶ **Reduced Barriers to Entry (into the regime of “really massive parallel processing”):** Access to quantum computers would give an adversary the capability to solve complex systems of multiple, highly non-linear equation systems for the simulation of physical processes from chemistry and solid state physics, biology, etc. Quantum computers also offer a polynomial “speed up” for other problems. If quantum computers become readily available, they could provide an adversary with easy access to novel engineering capabilities that can potentially become sources of technology surprise. However, a cautionary note is in order: the rapid rise of large-scale cloud computing and availability of massive computational capability as a commercial service by Amazon, Google, Microsoft, etc., “computation-by-the-yard,” suggest caution in over-stressing the impact of quantum computing on the issue of access to massive scale computation.
- ▶ **System Integration:** While parallel processing is no longer novel, quantum computers represent a significant degree of novelty. Quantum computing may result in the replacement of Moore’s law as a basis for technology forecasting with a new regime that is dependent not on the engineering of small “macro-structures” on chips but on atomic level engineering. While peripherals and human interfaces will still depend on conventional microelectronics, the computational power that those interfaces will control or respond to will be significantly greater.
- ▶ **Novel Delivery Means:** With the evolution of networked quantum computers, there will be the potential for significant changes in the delivery of conventional weapons since targeting and support of conventional weapons are highly dependent on central “back office” computing.
- ▶ **Self-propagation:** N/A
- ▶ **Novel Radical Empowerment:** In the hands of a competent adversary, quantum computing would provide the computing power necessary to exploit the security weaknesses of a highly networked world. The Internet is already a major enabler of commerce, learning, cooperative problem solving, and national security. Capabilities that previously would have been accessible only to the most intellectually and technologically resourceful state-level adversaries now have the potential to empower smaller sub-state entities. Some capabilities that would become possible for a previously less proficient adversary would be the ability to design new type of materials (e.g., explosives or biological agents such as synthetic pathogens) that can assist the adversary in achieving his goals. Quantum computing can address other fundamental problems such as the simulation of quantum systems, quantum effects in biological systems such as photosynthesis, physical chemistry, science of materials, and other fields.²⁴² It has the potential to

²⁴¹ T.D. Ladd, “Quantum Computers,” *Nature*, Vol. 464, 45-53, 4 March 2010.

²⁴² B. Testa, “Something Rich & Strange: Computing In The Quantum Realm,” *Processor*, Vol. 32 Issue 21, October 8, 2010.

increase our understanding of physics, to include the type of constraints that physics places on quantum technology itself.²⁴³

- **Mitigation of Effects:** Quantum computing arises out of scientific research that is broadly supported around the globe. Like all dual-use technology, it is difficult to see how it can be completely negated. As in the early days of computing, the United States will be able to enforce export controls on the technology, but past experience shows that export controls are only effective in slowing down—not preventing—technological diffusion when the technology becomes a commodity.

3. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY DEVELOPMENT

This section outlines the utility of quantum computing technology, the forces that will encourage investment in this area, and the factors that can slow down the development of the technology.

3.1 Technology Development Drivers

Quantum computers have the potential to be far more powerful than conventional machines because they exploit the rules of quantum mechanics to perform very large (2^N) calculations in parallel. One area of expected impact is new image and signal processing methods for data collection, image analysis, and signal processing of all kinds.²⁴⁴

Some rankings and priorities for U.S. S&T initiatives to address top national security threats are:²⁴⁵

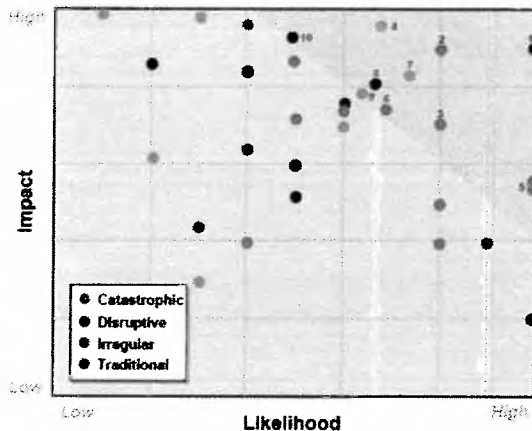


Figure 3 MIT Lincoln Lab. National Security Technology Study Threat Ranking of Critical National Security Threats (Lemnios 2009); the numbers in the figure identify the following national security threats: (1) Computer Network Attack/Exploit (2) Quiet Submarines (3) Unguided Battlefield Rockets (4) Chemical/Biological Attack (5) IED/Insurgents (6) Maneuvering Ballistic Missile (MaRV) Against Carrier Battle Group (CBG) (7) Containerized Nuclear Weapon (8) Anti-Satellite (ASAT) (9) Cruise or Short-Range Ballistic Missile Launch off Barge (10) Anti-cryptography (QC). (Source: Z.J. Lemnios, "Creating Capability Surprise," MIT Lincoln Laboratory; Department of the Air Force, FA8721-05-C-0002, 2009)

Quantum computing will have broad impacts, not only for national security but also for maintaining U.S. leadership in science and computing technologies. National security drivers have been responsible for networking, aeronautics and space,

²⁴³ SQIS, "A Federal Vision for Quantum Information Science," Subcommittee on Quantum Information Science (SQIS), Executive Office of the President, National Science and Technology Council, Washington, D.C., 2009.

²⁴⁴ David Robson, "Most powerful ever quantum chip undergoing tests," *NewScientistTech*, February 24, 2009.

²⁴⁵ Z.J. Lemnios, "Creating Capability Surprise," MIT Lincoln Laboratory; Department of the Air Force, FA8721-05-C-0002, 2009.

nuclear technology, and geophysical advances in the past. Currently commercial drivers supporting the interdependence of national economies and joint approaches to global problems of food, water, energy, education, poverty, and the environment are adding to the momentum of technology to address common problems.

Research towards achieving a quantum computing capability has deepened our understanding of the laws of quantum physics and consequently of the inner workings of matter. It has become evident that almost every physical object can become a quantum computer and therefore, through the application of an extrapolation from Turing's computing theory, a quantum computer will be able to model a wide range of physical process in nature. This inevitably leads one to consider the simulation the conscious thought. For now, this question remains an on-going philosophical debate, driven most recently by IBM's Watson and its Jeopardy success.²⁴⁶ Without wishing to depend on philosophy for justifying DTRA interest, it is likely that the ability of quantum computers to work on parallel "lines of thought" will aid in the realization of more powerful artificial intelligence applications.

3.2 Technology Development Counter-drivers

Achieving a robust quantum computer system that is immune from decoherence is a major challenge. Quantum information is fragile. Even weak interactions with the environment can change or destroy it. Currently, quantum entanglement has largely been limited to systems of two quantum objects, but for meaningful quantum processors, it will need to be spread among many quantum objects, even though the theoretical constructs for understanding entanglement are only beginning to be understood.

Quantum computing has the potential to solve certain classes of problems. Moreover, for practical implementation of a large scale quantum computer, significant theoretical and engineering challenges remain including:

- ▶ Loss of information due to quantum decoherence
- ▶ Limited communication distance due to signal attenuation
- ▶ Quantum communication protocols
- ▶ Need for larger numbers of quantum bits (Qubits) and control of their entanglement

Error correcting codes and fault tolerant schemes that could address the loss of information are other limitations of current technological capabilities, and efforts to replace them with more robust implementations are still in their infancy.

The greatest challenge in quantum computation today is the development of new quantum algorithms. The algorithms currently used in cryptography, i.e., factoring and discrete logarithm algorithms, will become less valuable as quantum computation becomes available for other applications. Finding new quantum algorithms is of paramount importance.

4. DRIVERS/COUNTER-DRIVERS OF TECHNOLOGY ATTRACTIVENESS

This section captures the factors that directly impinge on the adoption of quantum computing technology by Blue and Red, and the countermeasures available to each.

²⁴⁶ See John Markoff, "Computer Wins on 'Jeopardy!': Trivial, It's Not," *New York Times*, February 16, 2011.

4.1 Technology Attractiveness Drivers

The search for practical solutions to the barriers to quantum computing continues. The level of investment is still very high; in fact, it is prohibitively high for all but highly motivated major private organizations (e.g., IBM, Intel, Toshiba, NEC, etc.) or for states with solid information technology and quantum physics resources (e.g., the United States, certain western European countries, China, Russia, Israel, Singapore, etc.). It can be expected that special government needs will lead the technology development. Nonetheless, once the theoretical issues and engineering designs have been solved, quantum computing “chips” could become ubiquitous. If one assumes, however, that quantum computing will follow the trajectory of current computers, the first stage is likely to be a smaller number of large and expensive shared devices. This will enable both for technology issues to be demonstrated to the market and the creation of supporting industrial and networking infrastructure. These steps will presumably lead to cost reductions that will broaden the market to larger numbers of smaller users.

Quantum computing does not have an easily visible signature. However, once

connected to an exposed network, quantum computers would—by their nature—become visible as an enabler for a range of activities, first leading to broadening the market and becoming a commodity product and later leading to potential offensive uses. This inversion of government-early but weaponization-later should not be surprising. It is easier to sustain the broad use of a new technology, while weapon development, and the related development of necessary operational and strategic doctrine, consumes more time and effort.

Fortunately for Blue, any electronic device that connects to a network has a

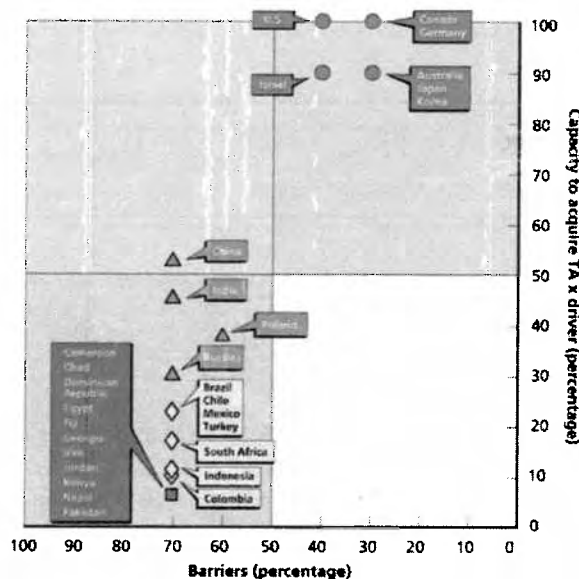


Figure 4: Countries with technological capacity to implement advanced technology applications (TA). The upper right-hand quadrant (blue) represents countries for which implementation of TAs is strongly driven by a high level of S&T capacity and the presence of many drivers but few barriers. The upper left-hand quadrant (green) represents countries for which implementation of TAs is strongly driven by a high level of S&T capacity and the presence of many drivers but for which many barriers are simultaneously present. The lower right-hand quadrant (yellow) represents countries for which implementation of TAs is not supported by a high level of S&T capacity and for which the number of both drivers and barriers is small. The lower left hand quadrant (red) represents countries for which implementation of TAs is not supported by a high level of S&T capacity and for which the number of barriers exceeds the number of drivers.

(Source: Richard Silbergliitt, et al., "The Global Technology Revolution 2020, In-Depth Analyses

Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications," RAND Corporation, 2006.)

"fingerprint" defined by the technical characteristics of the device itself. So, too, will technical feasibility be obvious, either directly from the market or, like nuclear weapons, through government use. In the case of quantum computing, today's technology dynamic has shifted from secret government development to market dynamics as states vie for leadership and economic strength while leveraging market capabilities.

The convergence of quantum computing and omnipresent Internet connections may drive cyber terrorism to become a more viable option for an adversary than traditional physical acts of violence.²⁴⁷ Nonetheless, quantum computing is even more of a game changer for Blue, which has the resources to take advantage not only of the huge, unprecedented computing power that quantum computing could provide, but more importantly, the potential new discoveries of a fundamental nature—regarding the micro-structure of matter, the fundamental forces that make the fabric of new quantum phenomena and new materials with revolutionary characteristics (e.g., superconductivity at wide range of temperatures, strong magnetic properties, electric capacitors, etc.).

At the most basic level, the tremendous computing power that even a medium-size quantum computer would provide could be used to integrate data and develop models of complex systems across multiple spatial and temporal scales. This would allow for modeling and simulation of complex natural or biological phenomena that would be difficult (if not impossible) to approach using today's computing capacities. These include modeling and simulation of new synthetic bio-materials and organisms (e.g., protein structure prediction, genomic sequencing, larger sets of dynamic events and chemical species); multi-phase biology (e.g., protein-nucleic acid recognition and assembly); and new composite and nano-materials.²⁴⁸

4.2 Technology Attractiveness Counter-drivers

While progress in quantum computing has been rapid over the past decade, there is not yet a convincing demonstration that it can become the next generation of computer technology. Some ideas simply do not come to fruition. For example, consider fusion power, space-based ballistic missile defense, and charged particle beam weapons. Such ideas do not fail suddenly. Instead, as an old Army ballad puts it, "Old soldiers, they never die; they just fade away."

A second counter-driver, and one that is characteristic of rapidly moving technology, is the "hotter biscuit" phenomenon. In other words, the "hot" idea of yesterday that fails to deliver instant gratification to supporting venture capitalists is abandoned to allow a resource shift to focus on a new idea.

5. CONCLUSION: RELEVANCE TO DTRA MISSION

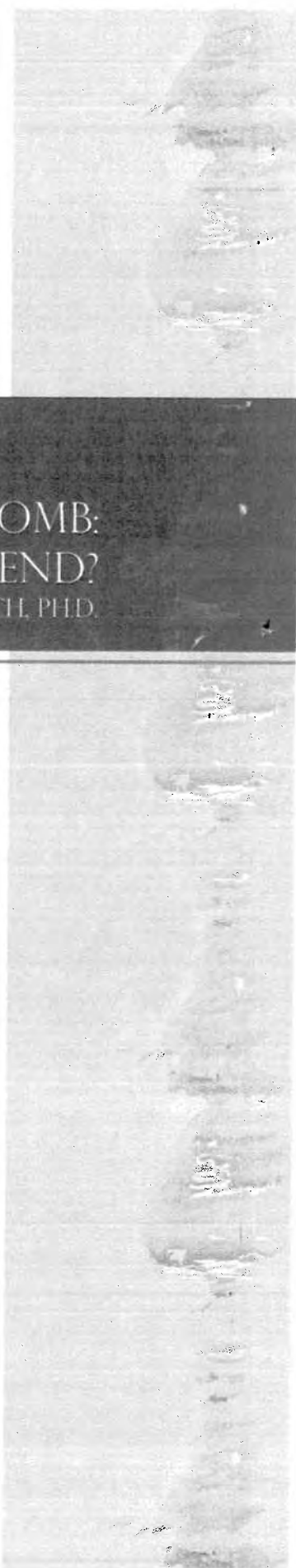
DTRA's area of responsibility is to combat threats posed by WMD. Over the years, WMD has proven to be a rather flexible umbrella covering a growing number of threats, each justified by its capability to produce first mass destruction, but more recently extended to include mass "effects." This is not unreasonable, since agencies of government exist to perform needed tasks, and an agency uniquely capable of assisting in a new important task can be expected to respond.

²⁴⁷ Bruce Tarter and Robert Nesbit, "Report on Advanced Computing," Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., March 2009.

²⁴⁸ Ibid.

While quantum computers are a good distance from being realized, it is clear that if their development occurs, they could have a tremendous impact on threats posed by Red, as well as Blue's ability to respond. It is therefore reasonable for DTRA to watch, study the implications of, and examine net Red/Blue balances. Quantum computing will not, in and of itself, pose a threat. However, it is a technology that enables many other threats that are of direct concern to DTRA.

Whether quantum computing falls within the 20-year timeframe addressed in this study is unclear. If no technical "show-stoppers" appear, a working quantum computer within 20 years is possible. Whether that development will pose a threat, as DTRA has come to define the term, is more problematic. A proper role for DTRA is to remain aware of U.S. and foreign progress in quantum computing, both accomplishments and difficulties. Additionally, the agency should consider how its programs and its assessments of current and future threats would have to be modified if the quantum computing possibilities outlined in this analysis come to pass.



THE E-BOMB: URBAN THREAT OR URBAN LEGEND?

GEORGE W. ULLRICH, PH.D.

"The next Pearl Harbor will not announce itself with a searing flash of nuclear light or with the plaintive wails of those dying of Ebola or its genetically engineered twin. You will hear a sharp crack in the distance. By the time you mistakenly identify this sound as an innocent clap of thunder, the civilized world will have become unhinged."

– Jim Wilson, "E-Bomb", *Popular Mechanics*, September 2001

INTRODUCTION

There has been considerable debate during the past 10 years regarding the threat that electromagnetic pulse (EMP) poses to U.S. civilian infrastructure, a debate fueled by the deliberations of a congressionally mandated commission charged with assessing the threat.²⁴⁹ While the EMP Commission focused exclusively on the consequences of high-altitude nuclear detonations, it is now widely recognized that similar but smaller-scale effects can also be created by non-nuclear EMP generators, sometimes referred to as "E-bombs." However, the distinction between the two is often blurred in media reports, leading to absurdly exaggerated claims regarding the aftermath of an E-bomb attack against modern electronics-based infrastructure. This paper examines the state of technology related to non-nuclear EMP generation and provides a realistic assessment of E-bombs as a readily accessible, game-changing technological threat to the United States.

²⁴⁹ The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack was established pursuant to title XIV of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (as enacted into law by Public Law 106-398; 114 Stat. 1654A-345). It was reestablished by Public Law 109-163, the National Defense Authorization Act for Fiscal Year 2006. The Commission completed its work in 2008. Throughout its seven-year tenure, it produced numerous reports and several of the Commissioners testified to various Congressional Committees on numerous occasions.

I. TECHNOLOGY OVERVIEW

I.1 Nuclear EMP

To better establish the distinction between nuclear and non-nuclear generated EMP, it is instructive to review the basic phenomenology of EMP generation from a high altitude burst (> 50 km). Prompt gamma rays generated by a high-altitude nuclear detonation interact with air molecules at mid-stratosphere (20-40 km) producing copious energetic electrons in a process known as Compton scattering.²⁵⁰ The Compton electrons then spiral down the Earth's magnetic field lines and collectively radiate an intense coherent electromagnetic pulse, which typically rises to its peak value in 5-10 nanoseconds and decays to half its peak value within about 100 nanoseconds. This so-called E1 pulse is characterized by peak electric field strengths up to tens of kilovolts per meter near the surface of the Earth. E1 can induce very high voltages in electrical conductors, exceed voltage breakdown thresholds, and circumvent ordinary lightning protection. It can couple directly into computers and communications equipment, frying microelectronic components. The E2 pulse follows closely behind E1 and lasts for about 1 second. It is created by Compton electrons from scattered gamma rays and delayed gammas generated by neutron capture. The E2 frequency domain is similar to lightning, as are its effects on electrical and electronic infrastructure. Accordingly, measures taken to protect against lightning are usually effective against E2, provided the protection devices survive the E1 pulse. The third and lowest frequency component of EMP is known as the E3 pulse. It is the result of the magneto-hydrodynamic heave of the Earth's magnetic field caused by the expanding ionized fireball. The magnitude of E3 is directly proportional to the yield of the weapon. Because of its long wavelength, E3 can couple significant energy into electrical transmission lines and propagate damaging current surges throughout the electrical grid, damaging transformers and other power conditioning equipment. It can also knock out copper-based communication links. The E3 damage mechanisms are similar to those caused by solar-induced geomagnetic storms.

The area affected by high-altitude nuclear EMP can be continental in scale, extending to the visual horizon as viewed from the burst point.²⁵¹ The damaging effects of EMP from a strategic nuclear warhead detonated at 500 km above Kansas would be felt across all 48 contiguous states. Because of the downward inclination of the Earth's magnetic field at higher latitudes, the maximum field strength will be concentrated in a U-shaped region extending southward from ground zero.

I.2 Non-nuclear EMP Devices

The literature is replete with monikers for non-nuclear EMP devices, among them High Power Microwave (HPM) weapons, Radio-Frequency (RF) weapons, directed RF energy weapons, weapons of electrical mass destruction, and E-Bombs. The terms are largely interchangeable, but for the purposes of this paper, the term E-Bombs will be reserved for EMP devices that are explosively driven using Flux Compression

²⁵⁰ Compton scattering is the inelastic scattering of photons by electrons. Part of the photon energy is transferred to the electron, which recoils and is ejected from its bound atomic state.

²⁵¹ The long reach of high-altitude EMP was first observed in connection with the 1962 Starfish Prime event, a 1.4 MT warhead launched aboard a rocket from Johnston Island in the Pacific Ocean and detonated at an altitude of 400 km. The detonation produced electrical disruptions in Hawaii, situated 900 miles from Ground Zero (GZ). Streetlights were darkened, burglar alarms were activated, and telephone microwave links were damaged. Less well known is that Starfish Prime also caused the demise of seven satellites in low Earth orbit within several months of the detonation, primarily from solar cell damage caused by residual energetic electrons trapped in the Van Allen radiation belts.

Generators; all other non-explosive devices will be referred to as HPM weapons.²⁵² A common feature among all non-nuclear EMP devices is that they radiate high peak-power bursts of electromagnetic radiation, not unlike the nuclear E1 pulse, at frequencies ranging from as low as several hundred kilohertz (KHz) to as high as several hundred gigahertz (GHz). The various sources are also distinguished as either narrowband, characterized by a relatively narrow output frequency spectrum around some center frequency, or ultra-wideband with an output frequency range from MHz to GHz. Generally speaking, narrowband HPM sources are analogous to lasers in their technical sophistication, whereas ultra-wideband sources are little more than high-power flashbulbs that generate a spatially compact electromagnetic pulse with a sub-nanosecond rise time. Narrowband sources can be configured to exploit a known resonance frequency in an electronic target. Ultra-wideband sources can be very compact (paint can size) and span the frequency spectrum from megahertz (MHz) to GHz. Such sources are very useful when little is known about the target vulnerability, but the energy coupled to the target in specific penetrating frequency bands is much reduced.

1.3 Electrically-Driven HPM Sources

Electrically driven, HPM sources are inherently narrowband. Essential components include a pulsed power system to convert prime power to a short, high-voltage pulse used to generate a relativistic electron beam (e-beam) in a vacuum electronic device.²⁵³ Once generated, the e-beam propagates in a radio-frequency interaction region where the electron kinetic energy is converted to coherent electromagnetic radiation. Most HPM research is focused on cross-field, vacuum devices, in which the electrons move across magnetic field lines produced by an external coil or permanent magnets. Cross-field devices include magnetrons and magnetically insulated line oscillators (MILO). They are capable of producing repetitive pulses at up to gigawatt (GW) peak power levels; pulse durations ranging from 10s to 100s of nanoseconds; operational repetition rates of up to 100 Hz; and a device-unique working frequency between 0.1-10 GHz. Other sources, such as gyrotrons, are tunable across a broad spectrum of frequencies and can operate in a continuous wave mode at megawatt (MW) class average power.²⁵⁴ The Virtual Cathode Oscillator, or Vircator, is a particularly interesting narrowband vacuum tube device since it is capable of generating pulses of tunable but well-defined frequencies at very high power levels (tens of GW). Such devices have significant advantages for enhancing energy coupling to targets with known resonant frequencies.

Packaging is a challenge for electrically driven HPM sources. Batteries and capacitors are bulky and heavy. The pulse-forming network, microwave tubes, and antennas also take up volume and weight. While it may not be possible to package such a system in a man-portable configuration, it is relatively straightforward to do so on an air platform or a large ground vehicle.²⁵⁵ The advantages of a vehicle-based electrically driven source over explosively-driven sources are several: 1) the ability to deliver multiple pulses and hence impact a larger area, 2) deep magazine, especially

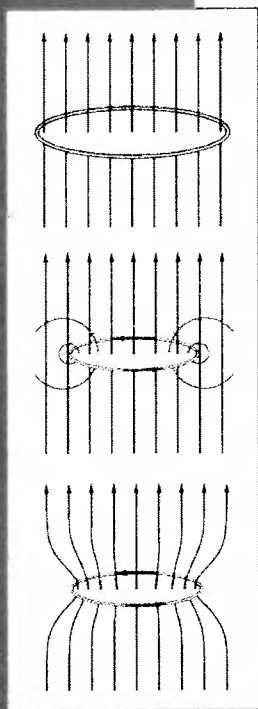
²⁵² Explosive or propellant driven Magneto-Hydro-Dynamic (MHD) generators will not be considered because that technology is not as mature as FCGs.

²⁵³ In typical mobile configuration, batteries are used to charge a capacitor bank (aka Marx bank) in parallel. Once charged, the capacitors are connected in series by fast-acting, spark gap switches, producing an output voltage that is n times the charging voltage, where n is the number of capacitors.

²⁵⁴ For a survey of HPM sources and their applications, see, for example: Edl Schamiloglu, "High Power Microwave Sources and Applications," IEEE Microwave Theory and Techniques Society, Fort Worth, TX, 2004.

²⁵⁵ The Air Force Research Laboratory has already prototyped a truck-based HPM counter-IED system, employing eight phase-locked, repetitively pulsed magnetrons, radiating at an average power of 2.5 MW.

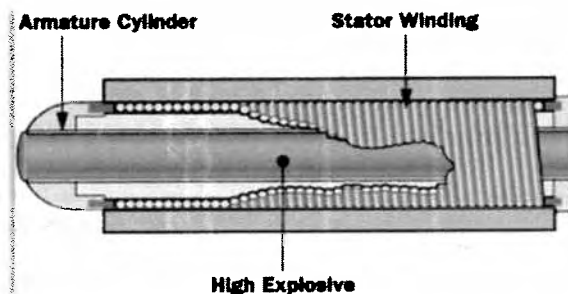
if the batteries can be recharged from the truck's prime power, 3) no explosive collateral effects, 4) inconspicuous attack, and 5) no forensic signatures.



1.4 Explosively-Driven EMP Sources

Explosively driven EMP sources rely on a device known as a magnetic Flux Compression Generator (FCG).²⁵⁶ FCGs are still the simplest, most compact, and most economical devices for generating a very short, high peak-power electromagnetic pulse. The principle of operation derives from Maxwell's equations, which require the magnetic flux (i.e., the amount of magnetic field passing through a surface) to remain constant if that surface is surrounded by a conductor. Consider the simplest case of a constant external magnetic field passing through a circular loop of copper wire. If the diameter of the wire is decreased, a current will be induced in the wire, which in turn will increase the magnetic field strength within the loop to keep the magnetic flux constant.

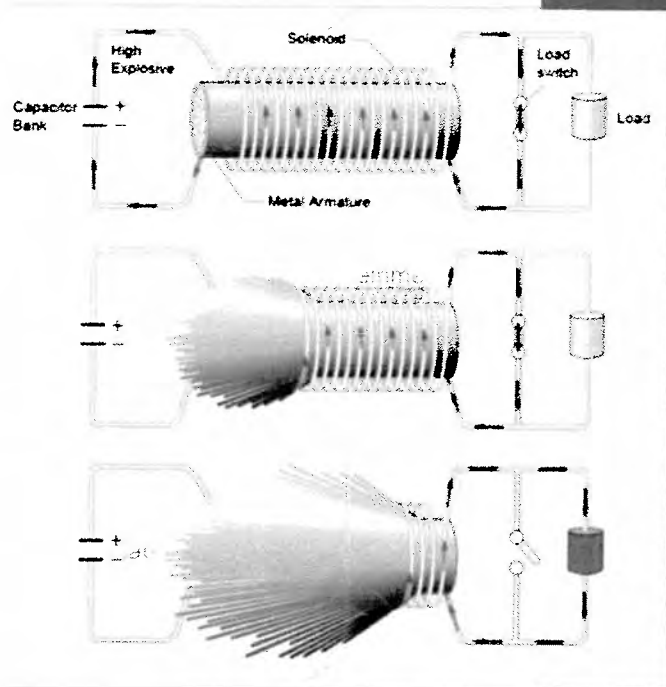
The schematic below depicts a simple coaxial FCG design based on this principle. The explosive is contained in a cylindrical metal tube which serves as the armature. The stator is a helically wound copper coil, surrounded by a thick structural jacket of



non-magnetic material to provide confinement and avoid premature structural failure of the device. The sequence of events is illustrated in the graphic below. A capacitor bank is discharged, sending a current through the coil and thereby creating a magnetic field in the annular region between the armature and the stator winding. At the moment of peak seed current in the coil, the explosive is initiated. As the detonation front propagates down the length of the cylinder, it expands the armature in a conical fashion forming a short circuit with the solenoid, thus isolating it from its seed current source and trapping the magnetic flux in the volume between the stator and the armature. The moving short circuit compresses the magnetic field while at the same time reducing the inductance of the coil. The combined effect induces a large current pulse in the remaining stator windings, peaking just before the device disintegrates in the tens of microseconds required to complete the explosive burn. At that point, a fast opening switch directs the current to a load, which could be an antenna or a microwave tube. Current amplification factors of up to 50x have been demonstrated. Seed currents of 0.1 to 1 MegaAmperes (MA) are easily achievable by cascading several FCGs, where a small FCG primes a larger one, resulting in a final peak current output of up to 100 MA and peak energies of tens of MegaJoules (MJ).

²⁵⁶ The Soviet VNIIEF (aka Arzamas 16) Center for Nuclear Research did much of the pioneering work on FCGs in support of nuclear fusion research in the 1950s. The early Soviet FCG design concepts were largely developed by Andrei Sakharov. Work on FCGs in the United States started in the late 1950s at the Los Alamos Scientific Laboratory (LASL) under the direction of Max Fowler.

FCGs are essentially impulse generators and thus intrinsically ultra-wideband. They self-radiate and generate RF energy on their own, typically at frequencies below 1MHz (limited by the burn time of the explosive). They can also drive an antenna. However, impulse antennas with any respectable gain and directivity are typically large and cumbersome. Another interesting application of FCGs is to drive an HPM generator. This would require special pulse power impedance matching techniques, using transformers and fast acting switches to shape the pulse. Such a hybrid E-bomb configuration requires considerable sophistication, and the packaging is only slightly less challenging than for non-explosively driven HPM sources. Also, as a one-shot device, it can be an expensive undertaking.



1.5 Accessibility to Non-Nuclear EMP Devices

Since the technology underpinning non-nuclear EMP devices has been around for well over 60 years, it should be no surprise that the components needed to fabricate such devices are all commercially available. HPM vacuum tubes of various types can be purchased from a number of vendors. In fact, the German company Rheinmetall Defense, in cooperation with fellow defense contractor Diehl, is marketing complete "High Power Electro-Magnetic (HPEM)" systems.²⁵⁷ They offer a variety of products ranging from a fully integrated system for defeating IEDs to a briefcase-sized ultra-wideband source capable of generating repetitive pulses that cover the entire frequency range from MHz to GHz. Russia and China also have active research programs pertaining to both nuclear and non-nuclear EMP sources. Russia has been actively marketing FCG technology since the dissolution of the Soviet Union. Both countries have state-of-the-art pulse power programs, supporting research in magnetic fusion as well as the development of HPM weapon systems.

FCGs can virtually be fabricated from Radio Shack components at a cost of several hundreds to thousands of dollars, depending on the size and complexity. But while conceptually simple, the detailed information required to construct efficient FCG sources, and the associated pulse forming networks required to link them to antennas or microwave tubes, is not available in open source literature.

1.6 Timelines for Development

Simple non-nuclear FCG-based EMP devices can be purchased or developed essentially in real time. But such systems will have a very limited range for electronic defeat that is not likely to exceed 10 meters or so. Packaging a high-power system that is man-portable or configured as a weapon payload in a bomb body or cruise missile is a challenging undertaking that could take years to come to fruition. A truck-based system affords the volume to accommodate the batteries, the capacitor

²⁵⁷ See, for example: <http://www.rheinmetall-defence.com/index.php?lang=3&fid=3756>

bank, the pulse forming network, the HPM tube, and the antenna required for a non-explosively-driven EMP source, but the integration of all components is non-trivial and will require seasoned engineering skills. Nonetheless, an operational system could likely be configured within a year from the start of development.

2. GAME-CHANGING QUALITIES

Since 2004, the EMP Commission has been sounding the alarm on the nation's vulnerability to a high-altitude nuclear EMP attack, citing the potentially widespread and long-lasting consequences to U.S. critical infrastructure. The Commission was particularly concerned about the strong interdependence of infrastructure (e.g., electric power, telecommunications, financial systems, and so on) and the potential for a failure of one infrastructure to trigger cascading failures of others. In this regard, electrical power and telecommunications are among the most critical given the dependence of virtually all of the others on them. Both of these sectors feature exploitable vulnerabilities that could lead to catastrophic failure. For example, the U.S. electric power grid depends on regional 500 KV transformers, which mediate the power distribution from high voltage transmission lines to the consumer. The Commission argued that the simultaneous failure of several such transformers, caused by an EMP-induced current surge, could bring down the entire grid. Spares are seldom available, and each is custom tailored to meet regional distribution needs. Additionally, most such transformers are manufactured overseas with normal delivery times of over a year.

The infrastructure failure scenarios considered by the EMP Commission were all predicated on a simultaneous EMP insult across a wide geographical area, as is the case for a high-altitude nuclear detonation. In making its arguments public, the EMP Commission has exposed some glaring vulnerabilities in various infrastructure components. Could these vulnerabilities be exploited on a smaller scale with distributed, synchronized non-nuclear electronic attacks to achieve a similar result? If so, are there advantages to an electronic attack over a simpler high explosive attack, relying solely on blast damage to achieve component failure?

Repetitively pulsed HPM sources at GW-class peak power levels can upset or damage electronic equipment with sensitive, high-density semiconductor devices at ranges of a few hundred meters and, for some devices, perhaps as far as a kilometer. Single-pulse, FCG-based EMP devices will generally exhibit a somewhat reduced range. By comparison, the amount of explosive needed to impart sufficient blast damage at 100 m to physically destroy such electronic equipment is about eight tons of TNT.²⁵⁸ An E-bomb that uses anywhere from 1-100 kg of high explosive is clearly a more plausible way of holding such electronic targets at risk, particularly when stand-off is enforced with physical barriers. In principle, a synchronized attack against distributed vulnerable infrastructure nodes using E-bombs is possible and preferable over alternative explosive means. But as will be discussed, target response to EMP is highly uncertain and for the most part unpredictable.

It is not necessary to bring down an entire infrastructure to impart a major blow to our modern urban existence. Virtually every job, every public service, and every element of commerce is dependent on electronic equipment, especially computers and the servers that connect them to the Internet. Perhaps less noticeable are the Supervisory Control and Data Acquisition (SCADA) systems that serve as silent

²⁵⁸ This assumes that the electronic equipment is housed in a building that can withstand up to 5 psi blast overpressure.

sentries, monitoring and controlling all industrial processes, facility functions, and infrastructure elements. Purposeful disruption or destruction of such systems, even on a local basis, could wreak havoc, confusion and turmoil and bring commerce to a near standstill.

To compare non-nuclear EMP devices against other futuristic technology threats being considered in the broader ASCO study, it is useful to address the game-changing potential of each in terms of the following qualities:

- ▶ **Reduced Barriers to Entry:** The barriers to entry for non-nuclear EMP devices are already low. The technology has been developed and refined over decades of research and many of the components are commercially available. The challenge lies in compact packaging and design refinements that maximize the power output at frequencies conducive to electronic defeat.
- ▶ **Novel Use:** Novel use equates to opportunistic use, e.g., an electronic attack on Wall Street during a global financial crisis, or on hospitals during a major disease outbreak, or on satellite receiver ground stations during a global security crisis. An electronic attack could also be conducted as an adjunct to a major cyber attack. The combined effects of malware and hardware disruptions could considerably exacerbate the consequences of execution and delay recovery.
- ▶ **Novel Delivery Means:** For military applications airborne delivery via penetrating bombs or cruise missiles would be preferred. For terrorist attacks in an urban environment, truck-based systems would appear to be the most unobtrusive. In both cases non-explosively driven devices that can be repetitively pulsed would be more effective than explosively driven single-shot devices. However, explosively driven devices that are also man-portable, wideband, and short-range would likely be the choice of Special Forces assigned to neutralize an electronic target without inflicting any human casualties or causing other undesired collateral effects.
- ▶ **Self-Propagation:** Some specially designed, low-frequency, pulse-power EMP devices can couple significant energy into the local facility power and telephone lines. Any electronic devices connected to those lines could experience damaging current surges and high voltage spikes, far exceeding those created by lightning. In such a way damaging effects could propagate to electronic systems well beyond the range of influence of the initial EMP pulse.
- ▶ **Novel Radical Empowerment:** Our increasing dependence on advanced electronic systems and the perceived lack of resilience of these systems to EMP insults makes such an attack an attractive asymmetric option, especially to non-peer adversaries. It is tantamount to the Biblical underdog bringing down the giant with a mere slingshot. Many critical vulnerabilities of our urban infrastructure are widely known, the means to exploit them are inexpensive, and the attack can be executed with virtual impunity. The only aspect of the scenario that might not appeal to the terrorist psyche is the lack of prompt human carnage.
- ▶ **Negation of Effects:** The lethality of EMP devices against electronic components is difficult if not impossible to predict. One could take two identical items of consumer electronics using the same semiconductor chips and they would likely fail at different field strengths because of minor variations in feature size or overall electrical topology introduced during the fabrication process. Additionally, the electrical state of the electronic system at the time of the EMP insult plays a major role in type and level of damage

or upset. Electronic equipment can also be hardened against EMP effects. Well established hardening protocols, such as Faraday cages, have been demonstrated to be effective against electronic attack. However, retrofitting hardness into existing electronic systems can be an expensive proposition.²⁵⁹

3. DRIVERS AND COUNTER-DRIVERS OF TECHNOLOGY DEVELOPMENT

3.1 Drivers

The *drivers* for developing non-nuclear EMP sources by our adversaries are clear. Pulse power technology and HPM sources have matured to the point where practical electrically driven EMP devices and explosively driven E-bombs are within reach. Meanwhile, the U.S. civil and military infrastructures have become increasingly imbedded with advanced electronic components that are highly vulnerable to EMP effects. This poses a classic asymmetric opportunity where a relatively minor investment by an unsophisticated adversary can hold hostage the world's largest economy and its only superpower. Because of uncertainties in the vulnerability of the electronic target and the coupling efficiency into the target, it makes sense to build the largest and most powerful FCG or the highest peak-power microwave tube. However, this requires a level of sophistication and technical know-how that likely will elude a third world adversary or a non-state terrorist organization.

3.2 Counterdrivers

The *counterdrivers* are largely related to packaging. An FCG is the most compact EMP source and hence most amenable to packaging as a man-portable system. However, because it is a relatively low frequency, wideband source, it will either require a large, cumbersome antenna along with a high power coupling transformer to match the low impedance FCG to the much higher impedance antenna, or it must be placed very close to the target with total reliance on the near-field EMP environment produced by the FCG winding. Alternatively, the output of the FCG could be impedance matched to a microwave source, such as a vircator. However, this would require advanced knowledge and special skill sets that are not readily available.

As the level of device sophistication increases, so do the costs. The Air Force Research Laboratory (AFRL) has demonstrated that research guided by highly developed physics codes running on supercomputers is far superior to the more traditional "cook and look" approach. However, such an approach is not available to our less sophisticated adversaries. The time and investment needed for an effective EMP source together with the uncertainties concerning effectiveness may, in the final analysis, frustrate the developer to the point of abandoning the technology.

4. DRIVERS AND COUNTER-DRIVERS OF TECHNOLOGY ATTRACTIVENESS

The technology attractiveness of HPM sources and E-Bombs is perhaps best discussed in the context of drivers and counter-drivers across the following domains:

Accessibility: As mentioned previously, access to materials and components required to fabricate a primitive E-bomb are readily available. However, such devices would likely have extremely limited range and effectiveness. Some commercial vendors

²⁵⁹ A Faraday cage is an electrically conductive enclosure that prevents an electromagnetic field from penetrating the protected equipment. However, any breaks in the cage (e.g., for cable penetration) provide potential leakage paths for some spectral components of the EMP pulse.

offer full-up HPM systems for sale, but they tend to be designed for special purpose applications and may not provide the sufficient flexibility to address a variety of targets. They are also expensive to purchase, operate and maintain. Some components, such as an efficient, compact, and affordable impulse-radiating antenna to focus ultra- wideband pulses are simply not available and continue to elude even the top researchers in the field. In the final analysis, the challenge of fabricating an effective HPM source or E-Bomb lies not so much in acquiring the hardware but rather in the engineering skills needed to integrate all of the essential components—prime power, pulse forming network, EMP generating device, and antenna—into a reliable, turn-key system.

Signatures: One of the attractive features of HPM sources is their lack of detectable signatures. A mobile, truck-mounted source can be designed to not have any external distinguishable features²⁶⁰ and blend in with routine traffic. There are no human casualties, no smoking holes, and by the time realization of the attack sets in, the source vehicle is gone. However, it may be possible after the fact to identify potential source vehicles within range at the time of the attack, using traffic cameras or the many other ubiquitous cameras that operate continuously in today's urban environment. The more often such an attack is conducted, the more likely it will be that the source vehicle will be found and interdicted. FCG-based E-bombs may not be discovered prior to detonation but they will leave a distinct signature. While the amount of explosive in such devices is typically on the order of several kilograms, it is sufficient to cause injuries and even death to those in the immediate vicinity of the explosion. Also the explosion will leave behind forensic clues regarding the origin of the device and its perpetrators.

Ability to Deploy: For Blue on Red military applications, the preferred delivery system would be a cruise missile or an unmanned air vehicle. For difficult targets, such as hardened underground command posts, the preferred package would be an EMP source in a penetrating bomb body. The packaging for any such systems requires unique capabilities found only in countries sponsoring advanced HPM research with extensive experience in weapon system integration. For a Red on Blue urban electronic attack, the preferred delivery means would be a vehicle-mounted HPM system capable of repetitive pulsing. Less desirable, but perhaps easier to deploy, would be an FCG-based, explosively-driven, single-shot, wideband devices. Such devices are man-portable. Several would have to be deployed in extreme proximity to the target to achieve the same effect as a more distant narrowband HPM source. This poses an increased risk of detection and interdiction.

Efficacy: The efficacy of execution with a non-nuclear EMP source is perhaps the most significant counter-driver towards the development and use of such devices. Modern commercial electronics all depend on high-density semiconductor devices that are very sensitive to high voltage transients, resulting in permanent damage (burn-out) or temporary upsets (e.g., latch-up). However, there is considerable variability in the electromagnetic hardness of electronic equipment, even in identically manufactured components. Some critical systems have hardened components; others are fully protected by a Faraday cage. There is also considerable uncertainty in how much RF energy is actually coupled to the target from an EMP source. Front door coupling refers to the normal pathway that an electronic device receives RF energy, e.g., a radar or communications antenna. An HPM device can be tuned to maximize front door penetration. While this may be an efficient pathway for

²⁶⁰ This assumes that the antenna would be mounted internal to the truck body.

the power flow to the device, many devices use protective measures, such as isolation transformers and surge arrestors to prevent or limit the damage from front door insults. Back door coupling refer to unintended leakage pathways to the electronic device through openings such as cable penetrations, etc. Since these pathways are not usually known *a priori*, a wideband source is the more appropriate choice to exploit such vulnerabilities, but the coupled energy in the penetrating frequency band may not be enough to do damage. For all of these reasons, the efficacy of an electronic attack can be highly variable and largely unpredictable.²⁶¹

5. CONCLUSION: RELEVANCE TO DTRA MISSION

HPM sources and E-bombs appear to have attributes highly desirable for Blue-on-Red engagements, including stealth, non-attribution, speed of light, tunable lethality, deep magazine (for HPM sources), non-lethality to humans, and low collateral consequences. Such a capability clearly complements the offensive capability of the U.S. military, providing more options to the commander in the field when lethal force may be inadvisable or unacceptable. The case for Red-on-Blue engagements is less compelling, especially for terrorist attacks in urban settings. Such adversaries do not share the U.S. obsession with minimal collateral effects. To the contrary, they would prefer to maximize collateral consequences of execution. This impulse, coupled with the unpredictable nature of the efficacy of electronic attacks, makes it less likely that terrorists will pursue such a course of action.

DTRA's mission space includes the hardening of strategic and tactical systems to nuclear radiation effects, including EMP. It would therefore be advisable for DTRA to follow the foreign developments in HPM systems and E-bombs, as well as to consider expedient preemptive measures that would mitigate or negate the efficacy of such weapons should they be deployed against U.S. systems. DTRA should also collaborate with DHS/S&T to conduct a realistic assessment of the efficacy of E-bomb attacks against the U.S. urban infrastructure.

²⁶¹ As a point of interest, while U.S. doctrine during the Cold War called for the employment of precursor EMP attacks in the Single Integrated Operations Plan (SIOP), the overall damage expectancy did not take into account any contribution from EMP-related damage, as there were no reliable prediction methods.

CONCLUDING OBSERVATIONS ON S&T THREAT ANALYSIS

STEPHEN J. LUKASIK, PH.D.

1. THE AWKWARD MATTER OF TIME FRAME

The Lewis Mumford quote on the first page of this report makes an important point, though it may leave technical readers uncomfortable with its definiteness on “nothing.” If one allows Mr. Mumford some license, and relaxes mathematical rigor, he would have agreed that what happened after 1934 justified his use of “nothing”: a city-destroying nuclear weapon, manned and unmanned missions to explore the solar system, synthetic life, computer-networked intelligence, a computer defeating an International Master in chess, and detection of radiation from the beginning of the universe. When Mumford died in 1990, he must have felt quite satisfied with his earlier observation.

The first of these “impossibles” occurred within ten years of 1934, well within the 20-year time frame of this study. Whether we have identified any similarly stunning technologies here will require waiting for 10-20 years to know. Most “impossibles” of future importance will probably lie outside of our time frame; the half-dozen fields identified here are not especially audacious in their scope. We have tried to follow DTRA’s *current* mission, ignoring its history going back to the Manhattan Engineer District and the Armed Forces Special Weapons Project of 1947. But hewing to the agency’s present focus does not account for S&T developments that may occupy its attention 20 years hence.

In technical fields that evolve over time, the initial conditions, where one starts to look, are more important than the precise nature of an unforeseeable endpoint. The idea of predicting the future is quixotic anyway—the consumers of such predictions in government and industry tend to try to change the projected future. But better than attempting to predict the future is to invent it. Agencies such as DTRA can do that to some extent.

An alternative view to either predicting or inventing the future might be called "trying to make oneself less uncomfortable." Problems do not stand still until "solutions" can be contrived. The technologies that can contribute to both problems and solutions change. Every change in technology or perceived need redefines the problem as attempts at fixes produce greater or less comfort to defenders and change adversary perceptions. Just as systems move to minimum energy configurations, one can view the sequence of state adjustments resulting from political events and judgments of technical need seeking new states of less "discomfort." In this view it is not the future state to focus on but the path followed as actors seek a global state of minimum discomfort. Consequently, the relatively short 6-20 year timeframe of this study works well. The ideas presented here represent a set of developments that are offered as representing "reasonable" initial conditions. Nathan Leites, in "The Operational Code of the Politburo" quotes Napoleon as saying, "One must start a serious engagement and then see what happens."²⁶²

2. THE IDIOSYNCRATIC NATURE OF EFFORTS OF THIS TYPE

Other groups of people like ourselves would come up with different choices of what DTRA might look into. With many such sets or recommendations, one might look at frequencies and commonalities, rather like seeking the "wisdom of crowds."²⁶³ This points to the utility of DTRA integrating the numerous inputs that it continually receives from its contractors identifying trends, averages, and most importantly, interesting outlier ideas.

It is of interest in this regard to see what our group did and did not select. Five papers examine electromagnetic phenomena: lasers, electromagnetic interference, and electronic computing devices, all well within the limits of current science. Two have a particular concern for the mass effects that can be produced by degrading the infrastructures on which developed countries depend. Two papers do poke at the limits of science. One addresses the engineering feasibility of synthetic pathogens; the other, on quantum computing, points to the world first suggested by Richard Feynman in 1959 in his paper, "There's Plenty of Room at the Bottom."²⁶⁴ Chemistry, including nanoscale phenomena, receives little attention. Mass effect casualties are described in terms of human casualties, although plant and animal targets to attack food chains can cause more economic havoc.

The focus here on weapon technologies and weapon effects mirrors DTRA's history, but is not completely representative of defense threats when the targets are minds and social systems rather than physical entities. Psychological warfare, information operations, terrorism, and strategic deception are examples.

3. WHERE ARE THE NEW "IMPOSSIBLES"?

None of the technologies discussed in this analysis appear clearly impossible on their face. People do not generally spend their time on "impossible" matters unless driven to do so by need. We might therefore have looked more heavily at needs. The new science of fission was applied to weapons because of the fear that Germany might

²⁶² Nathan Leites, "The Operational Code of the Politburo," RAND Corporation monograph, 1951.

²⁶³ See James Surowiecki, *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies, and Nations* (New York: Random House, 2004).

²⁶⁴ Richard Feynman, "There's Plenty of Room at the Bottom," Lecture to an American Physical Society meeting at Caltech, December 29, 1959.

develop them first. The attempt to put a man on the Moon was driven by the desire to demonstrate that the Soviet Union did not have the upper hand in space.

Without serious prodding, government agencies and their technical experts tend not to make bold calls for the impossible. Neither do legislatures, although social networks may become such a source in the future. Visionaries, think tanks, public scholars, and educational leaders also have audiences capable of amplifying novel ideas. Thus, an alternate approach to finding Mumford's impossibles would be to start with world needs and select from them technologies consistent with DTRA's threat reduction charter.

4. RED-BLUE PERSPECTIVES IN ASSESSING TECHNOLOGY

This examination of future S&T threats explored Red and Blue assessments, both in terms of how technologies would develop and the relative attractiveness of the technologies. But this template was applied to a technology list *created by Blue*. That is, it reflected the assumptions, biases, and general worldview of U.S. analysts. Groups, states as well as sub-state groups, will see technology differently, in terms of their particular security needs, their technology capabilities, and the balance they seek between offense and defense. Some groups may simply want to be left alone. Others may seek to redress relatively local grievances, while others may have global agendas. The set of technologies addressed here are examined from the viewpoint of developed states. The technology needs of the Afghan Taliban, or the North Koreans, may be different.

While the United States has invested heavily in dissuading states from launching nuclear warheads against New York City, the events of September 11, 2001, surprised virtually everyone in the national security establishment. We had not designed and deployed an ABDS (Anti-Box-cutter Defense System) nor an FTVS (Flight Training Validation System.)

R&D leaders see technology, and its threat potential, in terms of strategic balances and technology surprise. Others, less enthralled by technology, see technology simply as something to help them achieve their objectives, and the less of it and the simpler and less expensive it is, the better.

5. ROLES, MISSIONS, AND THE PROBLEM OF BEING TOO ORGANIZED

Another dimension of the Red-Blue problem, when one is big, is managing government to minimize wasteful competition and turf fights between its parts. This problem is one of both the Executive and Legislative branches of government and is complicated by differing federal and state authorities. The United States and other developed states have a bureaucratic place for everything—everything, that is, except the things no one has thought of because they are seen as impossible or so improbable as to amount to the same thing.

To the extent that new technologies are not dependent on government action, they are more likely to be pursued because the decision criteria are simpler. The national security establishment relies on such independently established capabilities, and this is widely seen as an asset. But from the standpoint of this study, they will likely miss threats that have no commercial analogs. So security agencies have difficulty in exploring impossibles absent clear and present dangers.

Computer software discussed in this study serves the defense establishment well, but it has trouble matching its political and bureaucratic processes to the pace of commercial developments. New functionalities are rapidly brought to market, but national vulnerabilities receive little attention.

6. EXPLORING A SPARSE MULTIDIMENSIONAL SPACE OF IMPOSSIBLES FOR POSSIBLES

The space of impossibles is a large multidimensional space and is difficult to explore given the numbers of things that are genuinely not possible. Buried among these “really” impossible things are a few that, on careful examination, may in fact be possible.

The national security establishment, including an agency like DTRA, needs a systematic way to explore the multitudes of the impossible to find the novel but possibly workable. It is a signal processing problem that there is little guidance on how to do the filtering. The same problem is true of DARPA, and the set of ARPA-Xs springing up in the U.S. government, but their approach is to invent the future.²⁶⁵ A useful ASCO initiative would be to join forces with those agencies in their search for novelty, replacing random walks through the space of the impossible by ones that follows advanced technology leads developed by its colleagues in government.

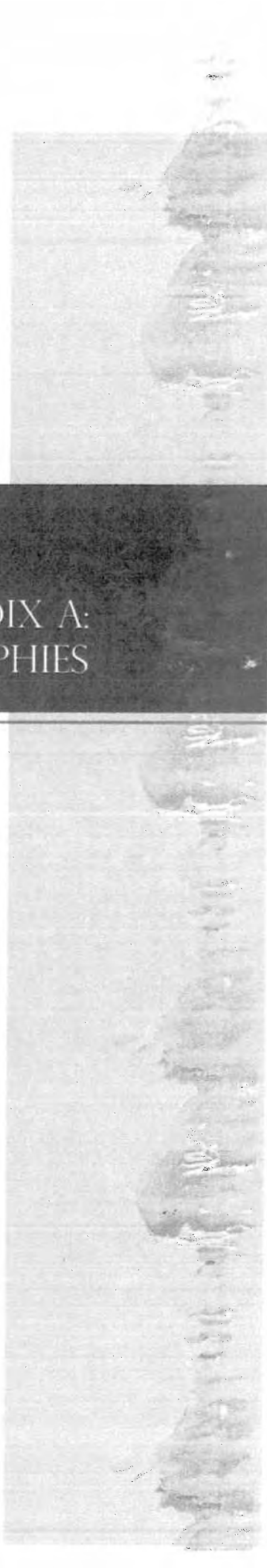
7. TECHNOLOGY DOES NOT THREATEN PEOPLE, PEOPLE THREATEN PEOPLE

Because we have no confidence in our ability to assess the willingness of a person to act, we must assume they will do so and proceed on this worst, but safe, basis. This ignores the possibility that a science of the mind might be a fruitful technological frontier, a next impossible to examine. “Game changing” includes both the rules of the game and the players. The foundations of a science of the mind lie in cultural anthropology, history, abnormal psychology, and group dynamics. Newly developed approaches to experimental economics and philosophy can provide useful entry points.

Such an approach looking at people rather than things may offer some efficiency in search. The space of impossibles is large, but the space of decision-makers is much smaller. The decision process itself may offer a starting point. “Decision-maker” implies a top-down process, but in fact decisions arise from the meeting of top-down and bottom-up initiatives. The latter, because of changes in global communication capabilities, are more easily examined, not only to learn of the results of decisions, but to measure *inputs* to decisions. Such an orientation to threat reduction, from the what to the who, may be feasible.

The methodology of the operational code, first established in Nathan Leites’ ground-breaking study of the principles guiding the decisions of the Soviet Politburo, provides a promising starting point. This approach, listening to what is said publicly from tweets, blogs, and ubiquitous video can be used to guide analysis of the new flows of information available, coupled with increasingly powerful search and analytical engines, is an unexploited window into the minds of public actors. Studying the science of the mind is not simply about understanding threats. The mind is also a target, and thus its vulnerability is a weapon effect.

²⁶⁵ The U.S. does not have a monopoly on ARPAs. The ARPA approach to technology management has not been ignored by other countries.



APPENDIX A: TEAM MEMBER BIOGRAPHIES

LISA ANDIVAHIS, PH.D.

Dr. Lisa Andivahis is a National Security Policy Analyst with SAIC. A physicist by training, she received her undergraduate and graduate degrees in Physics from The American University and later a Master of Science in Foreign Service from the Walsh School of Foreign Service at Georgetown University. She began her career as a research assistant at the Stanford Linear Accelerator Center, a DOE national research lab, performing experiments to study nuclear structure. She subsequently acquired 12 years of experience as a systems engineer for ballistic missile defense systems and anti-submarine warfare programs for which she provided technical system performance analysis as well as program management. Most recently she performs nuclear policy analysis. Her areas of expertise include nuclear technology and policy, ballistic missile defense technology and policy, radar and sonar signals analysis, and methods of radiation detection. Dr. Andivahis is the author/coauthor of over 20 scientific journal publications and a contributor to numerous policy studies.

DALLAS BOYD

Mr. Dallas Boyd is a National Security Analyst with SAIC. He received a B.A. degree in History from The Citadel and a Master in Public Policy degree from Harvard University's John F. Kennedy School of Government. Boyd performs research and analysis within SAIC's CBRNE Effects Analysis and Modeling division. His past work for DTRA/ASCO has involved research on terrorism, U.S. counterterrorism policy, nuclear deterrence, and adversary decision-making. Boyd served as the Principal Investigator of a DTRA/ASCO study concerning China's strategies to acquire advanced technology as part of its military modernization effort. He has also

performed research and analysis for DHS' Domestic Nuclear Detection Office related to the detection and interdiction of terrorist nuclear weapons. Prior to joining SAIC, Boyd served as a senior legislative aide to a member of the U.S. House of Representatives. His work has been published in the *Washington Quarterly*, *Bulletin of the Atomic Scientists*, and *Studies in Conflict & Terrorism*.

JEFFREY R. COOPER

Mr. Jeffrey Cooper is Vice President for Technology, SAIC Technical Fellow, and Chief Innovation Officer in SAIC's Intelligence, Reconnaissance, and Surveillance Group. He received his undergraduate and graduate education at The Johns Hopkins University, where he was later Professorial Lecturer in Arms Control and Defense Analysis at the School of Advanced International Studies (SAIS). In addition to long-standing focus on strategic analysis and military transformation, his core interest is using information to improve intelligence analysis, decision-making, and operational effectiveness in order to enhance U.S. national security. He is a founding member of the Highlands Forum, an OSD-sponsored program to identify cutting-edge technological developments that affect national security, and has been a member of numerous Defense Science Board Task Forces and Summer Studies. Cooper's recent focus has largely concerned intelligence matters, with particular emphasis on analytic failures and methods to improve all-source analysis capabilities. Cooper's monograph "Curing Analytic Pathologies" was published by CIA's Center for the Study of Intelligence in December 2005 and has been disseminated widely throughout the Intelligence Community. He was a recipient of the Secretary of Energy's Exceptional Service Medal.

STEPHEN J. LUKASIK, PH.D.

Dr. Stephen Lukasik received a B.S. in physics from Rensselaer Polytechnic Institute and a Ph.D. in physics from the Massachusetts Institute of Technology. While a member of the Advanced Research Projects Agency (ARPA), he was responsible for research in support of nuclear test ban negotiations and subsequently served as Deputy Director and then Director of the agency. Later government service was as Chief Scientist of the Federal Communications Commission, where he was responsible for advising the Commission on technical issues in communication regulation and for the management of non-government use of the electromagnetic spectrum. He is the author of numerous analyses concerning national strategies for cyber defense and international approaches to the protection of information systems against cyber threats. Lukasik is currently a consultant to SAIC, where his recent work has involved the vulnerabilities of industrialized societies to terrorism, nuclear smuggling, and the interdiction of terrorist attacks. Lukasik is also the author of a series of reports dealing with Red Team methodology, needed software tools for Red Teams, likely organizational structures for al-Qaeda, and terrorist uses of advanced technologies in attacks. Most recently he has studied concepts of operations for defensive systems, strategies for imposing costs on terrorists, and potential threats to the U.S. economy.

VICTOR OANCEA, PH.D.

Dr. Victor Oancea received his B.S., M.S., and Ph.D. degrees from Bucharest University. Oancea has over 20 years of technical experience in data mining, data

modeling and analysis, and software development in FORTRAN, Matlab, and VBA. His work experience includes risk analysis, systems engineering, complex modeling of mass casualty events, statistical analysis, and technology optimization for LIDAR atmospheric measurements. Additional experience includes: technology development risk analysis and risk analysis and modeling for critical asset protection. Oancea acted as deputy Principal Investigator for security needs assessment projects for several mass-transport jurisdictions. He also has experience with environmental hazard identification and risk assessment, risk control planning, implementation and review of control measures (atmospheric radionuclide transport, environmental risk mitigation), System Dynamics modeling for systems engineering analysis, and portfolio optimization for technological and business processes. Dr. Oancea's previous experience includes positions at the Massachusetts Institute of Technology and Romania's National Institute of Meteorology and Hydrology.

GEORGE W. ULLRICH, PH.D.

Dr. George Ullrich holds B.S., M.S., and Ph.D. degrees in physics from Drexel University. A former member of the federal Senior Executive Service, Ullrich held numerous senior positions in the Department of Defense, including Deputy Director of the Defense Nuclear Agency (later renamed the Defense Special Weapons Agency) and Director for Weapons Systems in the Office of the Secretary of Defense. In the latter position, Ullrich was responsible for the technical leadership, policy guidance, and management oversight of programs totaling approximately \$3 billion, spanning air, sea, and ground platforms; conventional weapons; directed energy weapons; advanced payloads and materials; and nuclear weapons technologies. Ullrich later held the position of Senior Vice President for Advanced Technology Programs at SAIC. He currently serves as the Chief Technology Officer of Schafer Corporation. Dr. Ullrich is a recipient of the Secretary of Defense Distinguished Civilian Service Medal.

REVOLUTIONS IN S&T

110

APPENDIX B: LITERATURE—GENERAL

2010

- ▶ National Research Council, “Persistent Forecasting of Disruptive Technologies – Report 2,” Committee on Forecasting Future Disruptive Technologies, National Academies Press, Washington, D.C., 2010. Available at: http://www.nap.edu/catalog.php?record_id=12834
- ▶ National Security Strategy, The White House, Washington, D.C., May 2010. Available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
- ▶ “Capability Surprise, Volume II: Supporting Papers,” Report of the Defense Science Board 2008 Summer Study, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., January 2010. Available at: <http://www.acq.osd.mil/dsb/reports/ADA513074.pdf>
- ▶ Quadrennial Defense Review, Office of the Secretary of Defense, The Pentagon, Washington, D.C., February 2010. Available at: http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf
- ▶ “Annual 10 Emerging Technologies,” MIT Technology Review, 2010. Available at: <http://www.technologyreview.com/tr10/>

2009

- ▶ National Research Council, “Persistent Forecasting of Disruptive Technologies,” Committee on Forecasting Future Disruptive Technologies, National Academies Press, Washington, D.C., 2009. Available at: http://www.nap.edu/catalog.php?record_id=12557

- ▶ “S&T for National Security,” JASON Defense Advisory Panel Report, JSR-OB-146, May 2009. Available at: <http://www.fas.org/irp/agency/dod/jason/sandt-full.pdf>
- ▶ “Capability Surprise, Volume I: Main Report,” Report of the Defense Science Board 2008 Summer Study, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., September 2009. Available at: <http://www.acq.osd.mil/dsb/reports/ADA506396.pdf>
- ▶ Brian A. Jackson and David R. Frelinger, “Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About?” RAND Corporation Occasional Paper, 2009. Available at: http://www.rand.org/pubs/occasional_papers/OP256/

2008

- ▶ *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*, New York: Vintage Books, 2008. Available at: http://www.preventwmd.org/static/docs/report/worldatrisk_full.pdf
- ▶ “Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025,” National Intelligence Council, April 2008. Available at: <http://www.fas.org/irp/nic/disruptive.pdf>
- ▶ Victor A. Banuls and Jose L. Salmeron, “Foresighting Key Areas in the Information Technology Industry,” *Technovation*, Vol. 28, 2008.
- ▶ Michael Moodie, “Reflections on the Implications of Terrorism Campaigns,” in Lewis A. Dunn et al., “Next Generation Weapons of Mass Destruction and Weapons of Mass Effects Terrorism,” McLean, Virginia: Science Applications International Corporation, January 31, 2008.

2007

- ▶ “21st Century Strategic Technology Vectors—Volume I: Main Report,” Defense Science Board 2006 Summer Study, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., February 2007: <http://www.acq.osd.mil/dsb/reports/ADA463361.pdf>
- ▶ “21st Century Strategic Technology Vectors—Volume II: Critical Capabilities and Enabling Technologies,” Defense Science Board 2006 Summer Study, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., February 2007: <http://www.acq.osd.mil/dsb/reports/ADA464370.pdf>
- ▶ “21st Century Strategic Technology Vectors—Volume IV: Accelerating the Transition of Technologies into U.S. Capabilities,” Defense Science Board 2006 Summer Study, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., April 2007: <http://www.acq.osd.mil/dsb/reports/ADA467596.pdf>
- ▶ “Reducing Vulnerabilities to Weapons of Mass Destruction—Volume I: Main Report,” Defense Science Board 2005 Summer Study, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., May 2007. Available at: <http://www.acq.osd.mil/dsb/reports/ADA471566.pdf>
- ▶ Mark Foulon and Christopher A. Padilla, “In Pursuit of Security and Prosperity: Technology Controls for a New Era,” *The Washington Quarterly*, Vol. 30, No. 2, Spring 2007. Available at: http://www.twq.com/07spring/docs/07spring_foulon-padilla.pdf

2006

- ▶ Christopher Spencer. "Knowledge: Its Preeminent Role; Education; Technology—A Guide to Facts and Views on Major or Future Trends, from Global Issues of the 21st Century and United Nations Challenges," May 12, 2006.
- ▶ Marina Gorbis and Alex Pang, et al., "Science & Technology Outlook: 2005–2055," Institute for the Future, Technology Horizons Program, May 2006. Available at: http://www.iftf.org/system/files/deliverables/TH_SR-967_S%2526T_Perspectives.pdf
- ▶ Richard Silbergliitt, et al., "The Global Technology Revolution 2020, In-Depth Analyses," RAND Corporation monograph. Prepared for the National Intelligence Council, 2006. Available at: http://www.rand.org/pubs/technical_reports/2006/RAND_TR303.pdf
- ▶ "21st Century Strategic Technology Vectors—Volume III: Strategic Technology Planning," Defense Science Board 2006 Summer Study, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., February 2006: <http://www.acq.osd.mil/dsh/reports/ADA469283.pdf>

2005

- ▶ "Avoiding Surprise in an Era of Global Technology Advances," Committee on Defense Intelligence Agency Technology Forecasts and Reviews, National Research Council, National Academies Press, Washington, D.C., 2005. Available at: www.nap.edu/catalog/11286.html
- ▶ T.A. Brooks et al., "Science and Technology Requirements for Naval Warfare 2015-2020," Naval Research Advisory Committee (NRAC) Report 05-03, August, 2005.
- ▶ International Science and Technology Strategy for the United States Department of Defense, DoD Defense Research and Engineering, April 2005.
- ▶ "The National Plan for Research and Development in Support of Critical Infrastructure Protection 2004," Office of Science and Technology Policy, Executive Office of the President, April 8, 2005.

2004

- ▶ "Mapping the Global Future," Report of the National Intelligence Council's 2020 Project, December 2004. Available at: <http://www.foia.cia.gov/2020/2020.pdf>
- ▶ "Foresight Analysis: Report of the CSPR," Committee on Scientific Planning and Review, International Council for Science, July 2004. Available at: http://www.icsu.org/Gestion/img/ICSU_DOC_DOWNLOAD/371_DD_FILE_Foresight_Analysis.pdf
- ▶ Dennis M. Gormley, "On Not Confusing the Unfamiliar with the Improbable: Low-Technology Means of Delivering Weapons of Mass Destruction," Weapons of Mass Destruction Commission study, October 24, 2004. Available at: <http://www.wmdcommission.org/files/No25.pdf>
- ▶ Paul Bernstein, et al., "Future Technology Concepts," Science Applications International Corporation report for the Defense Threat Reduction Agency/Advanced Systems and Concepts Office, May 2004.
- ▶ "Science and Technology Foresight Clusters & Convergence," Office of the National Science Advisor, September 2004. Available at: <http://www.tci->

network.org/media/asset_publics/resources/000/000/502/original/JSmith-foresight.pdf

- ▶ Richard Garwin, "Can Science and Technology Help to Counter Terrorism?" The Indo-U.S. Workshop on S&T to Counter Terrorism, Goa, India, January 12-14, 2004.

2002

- ▶ "Identification of Key Emerging Issues in Science and Society: An International Perspective on National Foresight Studies," International Council for Science, 2002. Available at: http://www.icsu.org/Gestion/img/ICSU_DOC_DOWNLOAD/22_DD_FILE_SPR_U0702-Report.pdf
- ▶ *National Strategy to Combat Weapons of Mass Destruction*, The White House, Washington, D.C., September 17, 2002. Available at: <http://www.fas.org/irp/offdocs/nsdp/nsdp-wmd.pdf>
- ▶ "Defense Science and Technology," Defense Science Board 2006 Summer Study, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., May 2002. Available at: <http://www.acq.osd.mil/dsb/reports/ADA403874.pdf>
- ▶ National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, Committee on Science and Technology for Countering Terrorism, Washington, D.C.: National Academies Press, 2002. Available at: <http://www.nap.edu/openbook.php?isbn=0309084814>
- ▶ "Making the Nation Safer; the Role of Science and Technology in Countering Terrorism," Committee on Science and Technology for Countering Terrorism, National Research Council, National Academies Press, Washington, D.C., 2002. Available at: http://www.nap.edu/catalog.php?record_id=10415
- ▶ Rex R. Kiziah, "Assessment of the Emerging Biocruise Threat," in Jim A. Davis and Barry R. Schneider, eds., *The Gathering Biological Warfare Storm*, USAF Counterproliferation Center, Air War College, Maxwell AFB, 2002.
- ▶ John Matsumura, et al., "Preparing for Future Warfare with Advanced Technologies: Prioritizing the Next Generation of Capabilities," RAND Corporation monograph, 2002. Available at: http://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP215.pdf
- ▶ M.B. Wallerstein, "Science in an Age of Terrorism," *Science*, Vol. 297, No. 5590, September 27, 2002. Available at: <http://www.sciencemag.org/cgi/content/summary/297/5590/2169>

2001

- ▶ Philip S. Antón, Richard Silbergliitt, James Schneider, "The Global Technology Revolution: Bio/Nano/Materials Trends and Their Synergies with IT by 2015," RAND National Defense Research Institute. Prepared for the National Intelligence Council, 2001. Available at: http://www.dni.gov/nic/PDF_GIF_research/globtechrev/rand.pdf
- ▶ Eileen Vergino, "Tracking the Global Spread of Advanced Technologies," *Science and Technology Review*, Lawrence Livermore National Laboratory, September 2001. Available at: https://www.llnl.gov/str/September01/pdfs/09_01.4.pdf

- ▶ Trace Gunsch, "The Next 20 Years," U.S. Army Technology Integration Center, September 12, 2001.
- ▶ J.S. Katz and S. Stewart, "Science Foresight Project Final Report, Volume 1," Defence Science and Technology Laboratory, Ministry of Defence (United Kingdom), October 2001. Available at: <http://www.sussex.ac.uk/Units/spru/foresight/SFP-documents/SFPfinal.pdf>
- ▶ "Technology Timeline," BTextact Technologies, November 12, 2001.

1999

- ▶ "Strategic Technologies for 2020," Batelle, November 30, 1999. Available at: http://www.battelle.org/SPOTLIGHT/tech_forecast/technology2020.aspx
- ▶ Hariolf Grupp and Harold A. Linstone, "National Technology Foresight Activities Around the Globe: Resurrection and New Paradigms," *Technological Forecasting and Social Change*, Vol. 60, 1999.

1998

- ▶ William E. Halal, et al., "The GWU Forecast of Emerging Technologies: A Continuous Assessment of the Technology Revolution," *Technological Forecasting and Social Change*, Vol. 59, September 1998. Available at: <http://home.gwu.edu/~halal/Articles/TC.tfsc.pdf>

1997

- ▶ Joseph F. Coates, John B. Mahaffie, and Andy Hines, *2025: Scenarios of U.S. and Global Society Reshaped by Science and Technology*, Greenville, North Carolina, Oakville Press, 1997.

1995

- ▶ Air Force Scientific Advisory Board, *New World Vistas, Air and Space Power for the 21st Century*, Washington, D.C.: The Department of the Air Force, The Pentagon, 1995.

1994

- ▶ Hamish McRae, *The World in 2020: Power, Culture and Prosperity: A Vision of the Future*, London: HarperCollins Publishers, 1994.

1992

- ▶ *STAR 21—Strategic Technologies for the Army of the Twenty-First Century*, Board on Army Science and Technology, Commission on Engineering and Technical Systems, and National Research Council, Washington, D.C.: National Academy Press, 1992. Available at: http://www.nap.edu/catalog.php?record_id=1888



APPENDIX C: LITERATURE—ULTRAFAST LASER TECHNOLOGY

- ▶ Jason Mick, "WickedLasers Unveils "Lightsaber" Powerful Enough to Set People on Fire" (undated). Available at:
<http://www.dailytech.com/WickedLasers+Unveils+Lightsaber+Powerful+Enough+to+Set+People+on+Fire/article18681.html>
- ▶ "ABL YAL 1A Airborne Laser, USA" (undated). Available at:
<http://www.airforce-technology.com/projects/abl/>

2010

- ▶ "National Space Policy of the United States of America," The White House, June 28, 2010. Available at:
http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf
- ▶ Michael K. Rafailov, "Ultrafast Bandgap Photonics Semiconductor Phenomenology: Response to Ultra-short Pulse Laser," International Society for Optics and Photonics, Proc. SPIE, 7780, August 26, 2010.

2009

- ▶ Jie Shan and Charles K. Toth, eds., *Topographic Laser Ranging and Scanning: Principles and Processing*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2009.
- ▶ Hamid Hemmati, ed., *Near-Earth Laser Communications*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2009. pp. 362-374.

2008

- ▶ Martin Richardson, Timothy McComb, and Vikas Sudesh, "High Power Fiber Lasers and Applications to Manufacturing," Conference Proceedings 1047, Laser and Plasma Applications in Materials Science, edited by E.H. Amara, S. Boudjemai, and D. Dournaz, American Institute of Physics, 2008.
- ▶ Philippe Roy, et al., "Optical Fiber Design and Fabrication: Discussion on Recent Developments," Conference Proceedings 1055, "1st Workshop on Specialty Optical Fibers and Their Applications," edited by C.M.B. Cordeiro and C. J. S. de Matos, American Institute of Physics, 2008.
- ▶ S. Sauteret, et al. "Generation of 20-TW pulses of picosecond duration using chirped-pulse amplification in a Nd:glass power chain," *Opt. Lett.* 16 (4), p 238, 1991.
- ▶ Madelyn I. Sawyer and John P. Sullivan. "Laser Weapons: An Emerging Threat," FBI Law Enforcement Bulletin, Quantico, VA, pp 18-21, April 2008.
- ▶ Bruce W. MacDonald, "China, Space Weapons, and U.S. Security," *Council of Foreign Relations Report*, No. 38, Council of Foreign Relations, September 2008.
- ▶ T. Eidam, et al., "57 W, 27 fs pulses from a fiber laser system using nonlinear compression," *Applied Physics B-Lasers and Optics*, Vol. 92, 2008. pp. 9-12.
- ▶ Robert J. Bunker and Dan Lindsay, "Laser Weapons: An Emerging Threat," FBI Law Enforcement Bulletin, Quantico, VA, April 2008. pp 2-7.
- ▶ David Alexander, "Advances in Electromagnetic/Directed Energy Weapon Systems," *Military Technology*, September 2008.

2007

- ▶ "The Defense Science Board Task Force on Directed Energy Weapons," Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., December 2007. Available at: <http://www.acq.osd.mil/dsb/reports/ADA476320.pdf>

2005

- ▶ Latika Becker, "Current and Future Trends in Infrared Focal Plan Array Technology," *Proc. SPIE* Vol. 5881, 2005.
- ▶ Adrian Carter and Bryce Samson, "New Technology Advances Applications for High-power Fiber Lasers," *Military and Aerospace Electronics*, February 1, 2005. Available at: http://www.nufern.com/article_detail.php/13
- ▶ S.L. Chin, et al. "The propagation of powerful femtosecond laser pulses in optical media: physics, applications, and new challenges," *Canadian Journal of Physics*, Vol. 83, 2005.
- ▶ John Keller, "Laser Pointer or Terrorist Threat," Editor's Notebook, Optoelectronics Watch, *Military and Aerospace Technology*, February 2005. p. 16.

2002

- ▶ S.K. Sundaram and E. Mazur, "Inducing and probing non-thermal transitions in semiconductors using femtosecond laser pulses," *Nature Materials*, Vol. 1, December 2002. Available at: <http://www.pnl.gov/main/highlights/Sundaram.pdf>

1992

- ▶ D. Wright, et al., "Laser Beam Width, Divergence and Beam Propagation Factor—An International Standardization Approach," *Optical and Quantum Electronics*, Vol. 24, 1992.

1987

- ▶ "Report to the APS of the Study Group on Science and Technology of Directed Energy Weapons: Executive Summary and Major Conclusions," *Physics Today*, May 1987. pp. S3-S13.

1985

- ▶ Strickland, D. and G. Mourou, "Compression of amplified chirped optical pulse," *Optics Communications*, Vol. 56, 1985.

1961

- ▶ Elias Snitzer, "Proposed Fiber Cavities for optical masers," *Journal of Applied Physics*, Vol. 32, No. 1, 36, 1961.

1960

- ▶ Theodore H. Mainman, "Optical and microwave optical experiments in Ruby," *Physical Review Letters*, Vol. 4 No. 11, 1960. pp. 564-566.

APPENDIX D: LITERATURE—ADVANCED BIOLOGICAL WEAPONS

- ▶ Human Genome Project Information, *Ethical, Legal, and Social Issues*, U.S. Department of Energy (undated). Available at: www.ornl.gov/sci/techresources/Human_Genome/elsi/elsi.shtml

2010

- ▶ *New Directions: The Ethics of Synthetic Biology and Emerging Technologies*, Report of the Presidential Commission for the Study of Bioethical Issues, Washington, D.C., December 2010. Available at: <http://www.bioethics.gov/documents/synthetic-biology/PCSBI-Synthetic-Biology-Report-12.16.10.pdf>
- ▶ "Common Elements of Project Coast," Nuclear Threat Initiative, January 2010. Available at: http://www.nti.org/e_research/profiles/Safrica/common_elements_project_coast.html
- ▶ Malcolm Dando, "Synthetic Biology: Harbinger of an Uncertain Future?" *Bulletin of the Atomic Scientists*, August 16, 2010. Available at: <http://www.thebulletin.org/web-edition/columnists/malcolm-dando/synthetic-biology-harbinger-of-uncertain-future>
- ▶ Katie Drummond, "Pentagon Looks to Breed Immortal 'Synthetic Organisms,' Molecular Kill-Switch Included," *Wired*, February 5, 2010. Available at: <http://www.wired.com/dangerroom/2010/02/pentagon-looks-to-breed-immortal-synthetic-organisms-molecular-kill-switch-included/>
- ▶ Nicholas Wade, "Researchers Say They Created a 'Synthetic' Cell," *New York Times*, May 20, 2010. Available at: <http://www.nytimes.com/2010/05/21/science/21cell.html>

- ▶ Maggie Fox, "Artificial life? Synthetic Genes 'Boot Up' Cell," *Reuters* May 20, 2010. Available at: <http://www.reuters.com/article/idUSTRE64J5RY20100520>
- ▶ Daniel G. Gibson, et al., "Creation of a Bacterial Cell Controlled by a Chemically Synthesized Genome," *Science*, Vol. 329, No. 5987, May 20, 2010. Available at: <http://www.sciencemag.org/content/329/5987/52.abstract>
- ▶ Mildred K. Cho and David A. Relman, "Synthetic 'Life,' Ethics, National Security, and Public Discourse," *Science*, Vol. 329, July 2, 2010. Available at: <http://cirge.stanford.edu/documents/ChoRelman2010.pdf>
- ▶ Thomas Douglas and Julian Savulescu, "Synthetic Biology and the Ethics of Knowledge," *Journal of Medical Ethics*, Vol. 36, October 8, 2010. Available at: http://www.bep.ox.ac.uk/_data/assets/pdf_file/0020/17516/Douglas.Savulescu_Synthetic.Biology_JME.2010.pdf

2009

- ▶ "National Strategy for Countering Biological Threats," National Security Council, The White House, Washington, D.C., November 2009. Available at: http://www.whitehouse.gov/sites/default/files/National_Strategy_for_Countering_BioThreats.pdf
- ▶ "Department of Defense Biological Safety and Security Program," Report of the Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., May 2009. Available at: <http://www.acq.osd.mil/dsb/reports/ADA499977.pdf>
- ▶ Jacob M. Appel, "Is All Fair in Biological Warfare? The Controversy over Genetically Engineered Biological Weapons," *Journal of Medical Ethics*, Vol. 35, 2009.
- ▶ Erik Parens, Josephine Johnston, and Jacob Moses, "Ethical Issues in Synthetic Biology: An Overview of the Debates," Synthetic Biology Project, June 2009. Available at: <http://www.synbioproject.org/process/assets/files/6334/synbio3.pdf>

2008

- ▶ Andrew Pollack, "Scientists Take New Step Toward Man-Made Life," *New York Times*, January 24, 2008. Available at: <http://www.nytimes.com/2008/01/24/science/24cnd-genome.html>
- ▶ Jerome A. Singh, "Project Coast: Eugenics in Apartheid South Africa," *Endeavour*, Vol. 32, No. 1, March 2008.
- ▶ A. Balmer and P. Martin, *Synthetic Biology: Social and Ethical Challenges*, University of Nottingham Institute for Science and Society, Nottingham, UK, 2008.

2007

- ▶ Alexander Kelle, "Synthetic Biology & Biosecurity Awareness In Europe," Bradford Science and Technology Report No. 9, November 2007. Available at: http://www.synbiosafe.eu/uploads///pdf/Synbiosafe-Biosecurity_awareness_in_Europe_Kelle.pdf
- ▶ Michele S. Garfinkel, Drew Endy, Gerald L. Epstein, and Robert M. Friedman, "Synthetic Genomic: Options for Governance," October 2007. Available at:

<http://www.icvi.org/cms/fileadmin/site/research/projects/synthetic-genomics-report/synthetic-genomics-report.pdf>

- ▶ Barry Kellman, "The Potential Dark Side of Genetics," *San Francisco Chronicle*, July 8, 2007. Available at: http://articles.sfgate.com/2007-07-08/opinion/17251564_1_genetic-testing-disease-ethnic-groups
- ▶ "Navigating Towards our Future: Third Scanning Report," Report of "The Navigator Network" on Emerging Issues in Biotechnology and Nanotechnology, New Zealand Ministry of Research, Science & Technology, February 2007. Available at: <http://www.morst.govt.nz/Documents/work/biotech/Navigator-Network-scanning-report-Feb-2007.pdf>

2006

- ▶ National Research Council, *Globalization, Biotechnology, and the Future of the Life Sciences*, Washington, D.C.: The National Academies Press, 2006. Available at: http://www.nap.edu/catalog.php?record_id=11567
- ▶ "Navigating Towards our Future: First Scanning Report," Report of "The Navigator Network" on Emerging Issues in Biotechnology and Nanotechnology, New Zealand Ministry of Research, Science & Technology, June 2006. Available at: <http://www.morst.govt.nz/Documents/work/biotech/Navigator-Network-scanning-report-June-2006.pdf>
- ▶ "Navigating Towards our Future: Second Scanning Report," Report of "The Navigator Network" on Emerging Issues in Biotechnology and Nanotechnology, New Zealand Ministry of Research, Science & Technology, November 2006. Available at: <http://www.morst.govt.nz/Documents/work/biotech/Navigator-Network-scanning-report-Nov-2006.pdf>
- ▶ Joby Warrick, "Custom-Built Pathogens Raise Bioterror Fears," *Washington Post*, July 31, 2006. Available at: <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/30/AR2006073000580.html>
- ▶ Hans Bügl, et al., "A Practical Perspective on DNA Synthesis and Biological Security," International Consortium for Polynucleotide Synthesis, December 4, 2006. Available at: <http://dspace.mit.edu/bitstream/handle/1721.1/40280/PPDS.pdf?sequence=1>
- ▶ Ronald Atlas and Malcolm Dando, "The Dual Use Dilemma for the Life Sciences: Perspectives, Conundrums, and Global Solutions," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, Vol. 4, No. 3, 2006.
- ▶ Julie E. Fischer, *Stewardship or Censorship: Balancing Biosecurity, the Public's Health, and the Benefits of Scientific Openness*, Washington, D.C.: Stimson Center, 2006. Available at: <http://www.stimson.org/images/uploads/research-pdfs/Stewardship.pdf>

2005

- ▶ "Biotechnologies to 2025," Prepared for New Zealand Government Agencies by the Ministry of Research, Science and Technology, January 2005. Available at: <http://www.morst.govt.nz/Documents/work/biotech/FutureWatch-Biotechnologies-to-2025.pdf>

- ▶ Chandré Gould, *South Africa's Chemical and Biological Warfare Programme 1981-1995*, Doctoral dissertation, Rhodes University, August 2005. Available at: <http://eprints.ru.ac.za/240/1/Gould-PhD.pdf>
- ▶ Gary A. Ackerman and Kevin S. Moran, "Bioterrorism and Threat Assessment," Weapons of Mass Destruction Commission study No. 22, 2005. Available at: <http://www.wmdcommission.org/files/No22.pdf>
- ▶ Milton Leitenberg, "Assessing the Biological Weapons and Bioterrorism Threat," Strategic Studies Institute, U.S. Army War College, December 2005. Available at: <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB639.pdf>
- ▶ Daryl J. Hauck, "Pandora's Box Opened Wide: UAVs Carrying Genetic Weapons," Occasional Paper No. 47, Center for Strategy and Technology, Air War College, Air University, Maxwell AFB, Alabama, November 2005. Available at: http://www.au.af.mil/au/awc/awcgate/cst/bugs_ch08.pdf
- ▶ Ronald Bailey, "Open Secrets of Biosecurity: Preventing the Life Sciences from Becoming the Death Sciences," *Reason*, July 6, 2005. Available at: <http://www.reason.com/news/show/34983.html>
- ▶ T.M. Tumpey, C.F. Basler, P.V. Aguilar et al., "Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus," *Science*, Vol. 310, No. 5745, October 7, 2005. Available at: <http://www.sciencemag.org/cgi/content/short/310/5745/77>

2004

- ▶ British Medical Association, *Biotechnology, Weapons, and Humanity II*, BMA Professional Division Publications, October 2004.
- ▶ Mark Wheelis, "Will the New Biology Lead to New Weapons?" *Arms Control Today*, July/August 2004.
- ▶ Vincent M. Sarich and Frank Miele, *Race: The Reality of Human Differences*, Boulder: Westview Press, 2004.²⁶⁶
- ▶ R.L. Frerichs, et al., "Historical Precedence and Technical Requirements of Biological Weapons Use: A Threat Assessment," SAND2004-1854, Albuquerque, NM: Sandia National Laboratories, 2004.
- ▶ Milton Leitenberg, *The Problem of Biological Weapons*, Swedish National Defense College, August 2004.
- ▶ National Research Council, *Biotechnology Research in an Age of Terrorism*, Washington, D.C.: The National Academies Press, 2004. Available at: http://www.nap.edu/catalog.php?record_id=10827#toc
- ▶ National Research Council, *Seeking Security: Pathogens, Open Access, and Genome Databases*, Washington, D.C.: National Academies Press, 2004. Available at: http://www.nap.edu/catalog.php?record_id=11087

²⁶⁶ The inclusion of this highly controversial work in this report is not meant to suggest the author's endorsement of its content. Sarich and Miele's book has been listed as a reference due to their discussion of the possibility of a "genetic bomb" being created as a result of research such as the Human Genome Project. For critiques of the authors' work, see Morris W. Foster, "Book Review—Race: The Reality of Human Differences," *Journal of Clinical Investigation*, Volume 113, Issue 12, June 15, 2004. Available at: <http://www.jci.org/articles/view/22151>. See also Mark Nathan Cohen, "Race and IQ Again," *Evolutionary Psychology*, Vol. 3, 2005. Available at: <http://www.epjournal.net/filestore/ep03255262.pdf>

2003

- ▶ "The Darker Bioweapons Future," Central Intelligence Agency, Office of Transnational Issues, (unclassified), November 3, 2003. Available at: <http://www.fas.org/irp/cia/product/bw1103.pdf>
- ▶ Chandré Gould and Peter Folb, "Project Coast: Apartheid's Chemical and Biological Warfare Programme," United Nations Institute for Disarmament Research, February 2003. Available at: <http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-144-0-en.pdf>
- ▶ David Whitehouse, "DNA Databases 'No Use to Terrorists,'" BBC News Online, January 15, 2003. Available at: <http://news.bbc.co.uk/2/hi/science/nature/2660753.stm>
- ▶ James B. Petro, Theodore R. Plasse, Jack A. McNulty, "Biotechnology: Impact on Biological Warfare and Biodefense," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, Volume 1, No. 3, September 2003.

2002

- ▶ Michael J. Ainscough, "Next Generation Bioweapons: The Technology of Genetic Engineering Applied to Biowarfare and Bioterrorism," Counterproliferation Papers, Future Warfare Series No. 14, USAF Counterproliferation Center, Air University, Maxwell AFB, Alabama, April 2002. Available at: <http://www.au.af.mil/au/awc/awcgate/cpc-pubs/ainscough.pdf>
- ▶ Jeronimo Cello, Aniko V. Paul, and Eckard Wimmer, "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template," *Science*, Vol. 297, No. 5583, August 9, 2002. Available at: <http://www.sciencemag.org/cgi/content/abstract/1072266>
- ▶ Jon Cohen, "Designer Bugs," *Atlantic Monthly*, July/August 2002. Available at: <http://www.theatlantic.com/past/docs/issues/2002/07/cohen-j.htm>

2001

- ▶ Claire M. Fraser and Malcolm R. Dando, "Genomics and Future Biological Weapons: the Need for Preventive Action by the Biomedical Community," *Nature Genetics*, Vol. 29, Vol. 3, 2001. Available at: <http://cmbi.bjmu.edu.cn/2001/insight-anthrax/feature/Genomics%20and%20future%20biological%20weapons.pdf>
- ▶ Stephen F. Burgess and Helen E. Purkitt, "The Rollback of South Africa's Chemical and Biological Warfare Program," USAF Counterproliferation Center, Air War College, April 2001. Available at: <http://www.au.af.mil/au/awc/awcgate/cpc-pubs/southafrica.pdf>
- ▶ Erik Baard, "The DNA Bomb: Modified Crops Are In The Crosshairs Now. You May Be Next," *Village Voice*, May 15, 2001. Available at: <http://www.villagevoice.com/2001-05-15/news/the-dna-bomb/>
- ▶ Gerald L. Epstein, "Controlling Biological Warfare Threats: Resolving Potential Tensions among the Research Community, Industry, and the National Security Community," *Critical Reviews in Microbiology*, Vol. 27, No. 4, 2001.

2000

- ▶ Chandré Gould and Peter I. Folb, "The South African Chemical and Biological Warfare Program: An Overview," *Nonproliferation Review*, Fall/Winter 2000. Available at: <http://cns.miis.edu/npr/pdfs/73gould.pdf>
- ▶ Mark Wheelis and Malcolm Dando, "New Technology and Future Developments in Biological Warfare," *Disarmament Forum*, No. 4, 2000. Available at: <http://www.unidir.org/pdf/articles/pdf-art115.pdf>
- ▶ Jonathan B. Tucker, ed., *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, Cambridge: The MIT Press, 2000. Available at: http://cns.miis.edu/books/toxic_terror_toc.htm

1999

- ▶ "Genetic Engineering and Biological Weapons," *GeneWatch UK*, Briefing Number 6, June 1999. Available at: <http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/brief6.pdf>
- ▶ Ethirajan Anbarasan, "Genetic Weapons: A 21st Century Nightmare?" *UNESCO Courier*, March 1999. Available at: <http://unesdoc.unesco.org/images/0011/001151/115117e.pdf>
- ▶ Tom Mangold and Jeff Goldberg, *Plague Wars: The Terrifying Reality of Biological Warfare*, New York: St. Martin's, 1999.
- ▶ British Medical Association, *Biotechnology, Weapons, and Humanity*, Amsterdam, Netherlands: Harwood Academic Publishers, 1999.
- ▶ Malcolm Dando, Appendix 13A. "Benefits and Threats of Developments in Biotechnology and Genetic Engineering," in *SIPRI Yearbook 1999: Armaments, Disarmament and International Security*, Oxford University Press: Oxford, 1999. Available at: <http://www.sipri.org/yearbook/1999/13>
- ▶ K.P. Kavanaugh, "Biological Warfare: Genetically-Engineered Weapons Cannot Be Excluded," *Public Interest Report* (Federation of American Scientists), Volume 52, Number 2, March/April 1999. Available at: <http://www.fas.org/faspir/v52n2.htm#weapons>
- ▶ Ken Alibek with Stephen Handelman, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World, Told from the Inside by the Man Who Ran It*, New York: Random House, 1999.

1998

- ▶ David Rotman, "The Next Biotech Harvest," *MIT Technology Review*, September/October 1998. Available at: <http://www.technologyreview.com/biomedicine/11759/>
- ▶ "Interview with Dr. Daan Goosen," PBS Frontline, October 1998. Available at: <http://www.pbs.org/wgbh/pages/frontline/shows/plague/sa/goosen.html>
- ▶ Uzi Mahnaimi and Marie Colvin, "Israel Planning 'Ethnic' Bomb as Saddam Caves In," *Sunday Times*, November 15, 1998. Available at: http://www.bibliotecapleyades.net/sociopolitica/esp_sociopol_depocu17a.htm
- ▶ "Interview with Dr. Christopher Davis," PBS Frontline, October 1998. Available at: <http://www.pbs.org/wgbh/pages/frontline/shows/plague/interviews/davis.html>

- ▶ "Interview with Michael Osterholm," PBS Frontline, October 1998. Available at:
<http://www.pbs.org/wgbh/pages/frontline/shows/plague/interviews/osterholm.html>
- ▶ W. Seth Carus, "Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900," Center for Counterproliferation Research, National Defense University, Washington, D.C. August 1998. Available at:
<http://www.fas.org/irp/threat/cbw/carus.pdf>

1997

- ▶ S. Koonin, et al., "Human Genome Project," JASON Defense Advisory Panel Report, JSR-97-315, October 7, 1997. Available at:
http://www.ornl.gov/sci/techresources/Human_Genome/publicat/miscpubs/jason/index.html

1996

- ▶ Leonard A. Cole, *The Eleventh Plague: The Politics of Biological and Chemical Warfare*, New York: W. H. Freeman, 1996.

1995

- ▶ "Biotechnology for the 21st Century: New Horizons," Biotechnology Research Subcommittee, Committee on Fundamental Science, National Science and Technology Council, July 1995.

1988

- ▶ Charles Piller, and Keith R. Yamamoto, *Gene Wars: Military Control over the New Genetic Technologies*, New York: William Morrow, 1988.

APPENDIX E: LITERATURE—ADVANCED LASER ISOTOPE SEPARATION AND ENRICHMENT

- ▶ Alessandra M. Lombardi, "Radio Frequency Quadrupole (RFQ)," CERN, Geneva, Switzerland, (undated). Available at: <http://cdsweb.cern.ch/record/1005049/files/p201.pdf>
- ▶ John L. Lyman, "Enrichment Separative Capacity for Silex," Los Alamos National Laboratories, (undated). Available at: <http://www.fas.org/sgp/othergov/doe/lanl/docs4/silex.pdf>
- ▶ "Laser Isotope Separation Uranium Enrichment," GlobalSecurity.org (undated). Available at: <http://www.globalsecurity.org/wmd/intro/u-laser.htm>

2010

- ▶ Adrian Cho, "What Shall We Do with the X-ray Laser?" *Science*, Vol. 330, December 10, 2010, pp. 1470-71.
- ▶ Francis Slakey and Linda R. Cohen, "Stop Laser Uranium Enrichment," *Nature*, Vol. 464, March 4, 2010. Available at: <http://www.nature.com/nature/journal/v464/n7285/full/464032a.html>
- ▶ Francis Slakey and Linda Cohen, "NRC Should Perform Non-Proliferation Assessment of Laser Enrichment Technology," *Physics & Society*, July 2010. Available at: <http://www.aps.org/units/fps/newsletters/201007/slakey.cfm>
- ▶ Richard Harris, "Laser Nuclear Technology Might Pose Security Risk," National Public Radio, April 12, 2010. Available at: <http://www.npr.org/templates/story/story.php?storyId=125787318>
- ▶ Elaine M. Grossman, "Agency Forgoes Proliferation Review of New Nuclear Technology, Despite Worries," *Global Security Newswire*, July 30, 2010. Available at: http://gsn.nti.org/gsn/nw_20100730_6449.php

- ▶ Elaine M. Grossman, "New Enrichment Technology Offers Detectable 'Signatures,' Advocate Says," *Global Security Newswire*, August 2, 2010. Available at: http://gsn.nti.org/gsn/nw_20100802_4907.php
- ▶ "GE Laser Enrichment Facility Licensing," U.S. Nuclear Regulatory Commission, October 20, 2010. Available at: <http://www.nrc.gov/materials/fuel-cycle-fac/laser.html>

2009

- ▶ Jonathan Fahey, "Riches in Enrichment," *Forbes Asia Magazine*, November 16, 2009. Available at: <http://www.forbes.com/global/2009/1116/outfront-nuclear-power-uranium-ge-riches-in-enrichment.html>
- ▶ M. D. Laughter, "Profile of World Uranium Enrichment Programs—2009," Oak Ridge National Laboratory, April 2009. Available at: <http://info.ornl.gov/sites/publications/files/Pub15166.pdf>
- ▶ "Letter to Nuclear Regulatory Commission on Laser Enrichment Facility in North Carolina," Center for Arms Control and Non-Proliferation, September 30, 2009. Available at: http://armscontrolcenter.org/policy/nuclearweapons/articles/100209_letter_nrc_laser_enrichment_north_carolina/
- ▶ James M. Acton, "Nuclear Power, Disarmament and Technological Restraint," *Survival*, August/September, 2009. Available at: www.carnegieendowment.org/files/acton_survival_aug20091.pdf
- ▶ William Mathews, "Laser Enrichment Plan Draws Critics," *Defense News*, December 7, 2009. Available at: <http://www.defensenews.com/story.php?i=4406853>

2008

- ▶ Suren Erkman, et al., "The Origin of Iraq's Nuclear Weapons Program: Technical Reality and Western Hypocrisy," Independent Scientific Research Institute, October 20, 2008. Available at: http://arxiv.org/PS_cache/physics/pdf/0512/0512268v4.pdf

2006

- ▶ Michael Goldsworthy, "Inquiry into Developing Australia's Non-Fossil Fuel Energy; Case Study: The Strategic Importance of Australia's Uranium Resource," SILEX, Presentation to the House of Representatives Standing Committee on Industry and Resources, February 6, 2006. Available at: <http://www.silex.com.au/public/uploads/announce/House%20of%20Reps%20Presentation%20090206.pdf>
- ▶ Petr A. Bokhan, et al. *Laser Isotope Separation in Atomic Vapor*, Wiley-VCH, Berlin, August 2006.

2005

- ▶ Charles D. Ferguson and Jack Boureston, "Laser Enrichment: Separation Anxiety," *Bulletin of Atomic Scientists*, March/April 2005. Available at: http://www.cfr.org/publication/7876/laser_enrichment.html
- ▶ "Nuclear Power and Proliferation Resistance: Securing Benefits, Limiting Risk," Report by the Nuclear Energy Study Group of the American Physical Society Panel on Public Affairs, May 2005. Available at:

<http://www.aps.org/policy/reports/popa-reports/proliferation-resistance/loader.cfm?csModule=security/getfile&PageID=6826>

2004

- ▶ Charles D. Ferguson and Jack Boureston, "Focusing on Iran's Laser Enrichment Program," FirstWatch International, June 17, 2004. Available at: <http://www.iranwatch.org/privateviews/First%20Watch/perspex-fwi-Laser.pdf>

2000

- ▶ Steven Hargrove, "Laser Technology Follows in Lawrence's Footsteps," *Science & Technology Review*, May 2000. Available at: <https://www.llnl.gov/str/Hargrove.html>

1995

- ▶ Andre Gsponer and Jean-Pierre Hurni, "Iraq's Calutrons: Electromagnetic Isotope Separation, Beam Technology, and Nuclear Weapon Proliferation," Independent Scientific Research Institute (ISRI) Report ISRI9503, October 19, 1995. Available at: http://arxiv.org/PS_cache/physics/pdf/0512/0512268v4.pdf

1993

- ▶ R.M. Feinberg and R.S. Hargrove, "Overview of Uranium Atomic Vapor Laser Isotope Separation," Lawrence Livermore National Laboratory, August 1993. Available at: <http://www.osti.gov/bridge/servlets/purl/10102839-PDTP1e/native/10102839.pdf>

1987

- ▶ L.J. Radziemski, R.W. Solarz, and J.A. Paisner, eds., *Laser Spectroscopy and its Applications*, New York: Marcel Dekker, 1987.

1981

- ▶ R.H. Stokes, T.P. Wangler, and K.R. Crandall, "The Radio-Frequency Quadrupole—A New Linear Accelerator," *IEEE Transactions on Nuclear Science*, Vol. NS-28, No. 3, June 1981. Available at: http://accelconf.web.cern.ch/Accelconf/p81/PDF/PAC1981_1999.PDF

APPENDIX F: LITERATURE—EMI MICRO-JAMMERS

- ▶ John Merrill, "Department of Homeland Security (DHS) GPS Interference Detection and Mitigation (IDM)," Department of Homeland Security (undated). Available at: www.pnt.gov/advisory/2009/05/merrill.ppt
- ▶ Captain Curtis L. Dubay, "Domestic Space-Based PNT Interference Detection and Mitigation," DHS Positioning, Navigation and Timing Work Group (undated). Available at: www.gps-world.biz/pdfs/GAARDIAN_Generic_Briefing_Presentation.pdf

2011

- ▶ "Navy Electronic Interference System Could Target Nuke Facilities," *Global Security Newswire*, January 21, 2011. Available at: http://www.globalsecuritynewswire.org/gsn/nw_20110121_2166.php

2010

- ▶ A. Brown, R. Edwards, B. Bockius, "Using JLOC (GPS Jammer Detection and Location System) to Support the Warfighter," Joint Navigation Conference 2010, Session A1: Warfighter Requirements & Solutions, June 7-10, 2010. Available at: <http://www.jointnavigation.org/abstract.cfm?meetingID=29&pid=52&t=A&s=1>
- ▶ William Radasky and Edward Savage, "Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid," Metatech Corporation report prepared for Oak Ridge National Laboratory, January 2010. Available at: http://www.futurescience.com/emp/ferc_Meta-R-323.pdf

- ▶ "GPS Jamming and Interference Conference," Royal Institute of Navigation / Digital Systems KTN, Teddington, London, United Kingdom, February 23, 2010. Available at: http://www.insidegnss.com/node/1979#Baseband_Technologies_Inc
- ▶ Alan Grant, GPS Jamming and its Impact on Maritime Navigation, Royal Institute of Navigation, May 10, 2010. Available at: www.gla-rnav.org/file.html?file=086cf9eb1dc18399eb2432a9ae9d7fe2
- ▶ Charles Curry, "GPS Interference Detection & Mitigation," Chronos Technology, January 25, 2010. Available at: http://www.gps-world.biz/pdfs/GAARDIAN_Generic_Briefing_Presentation.pdf
- ▶ Peter Whitehead, "Jamming of GPS signals threatens vital services," *Financial Times*, February 23 2010. Available at: <http://www.ft.com/cms/s/0/4fa1c68a-2094-11df-9775-00144feab49a.html#axzz1BgRhWA5u>
- ▶ Charlie Sorrel, "Car Thieves Use GPS Jammers to Make Clean Getaway," *Wired*, February 24, 2010. Available at: <http://www.wired.com/gadgetlab/2010/02/car-thieves-use-gps-jammers-to-make-a-clean-getaway/>

2009

- ▶ David Last, "Expert Advice: GPS Forensics, Crime, and Jamming," *GPS World*, October 4, 2009. Available at: <http://www.gpsworld.com/defense/security-surveillance/expert-advice-gps-forensics-crime-and-jamming-8986>
- ▶ David Last, "GPS Jamming Trials," Newcastle, November 30–December 4, 2009. Available at: www.professordavidlast.co.uk/cms_items/f20100108163025.ppt
- ▶ "Global Positioning System: Significant Challenges in Sustaining and Upgrading Widely Used Capabilities," Government Accountability Office report GAO-09-670T, May 7, 2009. Available at: <http://www.gao.gov/new.items/d09670t.pdf>

2008

- ▶ "Positioning, Navigation, and Timing (PNT) Interference Detection and Mitigation (IDM) Plan," Department of Homeland Security, April 2008. Available at: <http://www.pnt.gov/public/docs/2008/idmpublicsummary.pdf>
- ▶ "PNT Interference Detection and Mitigation (IDM) Plan Fact Sheet," Department of Homeland Security, April 2008. Available at: <http://www.pnt.gov/public/docs/2008/idmfactsheet.pdf>

2004

- ▶ William A. Radasky, Carl E. Baum, and Manu W. Wik, "Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)," *IEEE Transactions on Electromagnetic Compatibility*, Vol. 46, No. 3, August 2004. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1325784>
- ▶ D.V. Giri and F. Tesche, "Classification of Intentional Electromagnetic Environments (IEME)," *IEEE Transactions on Electromagnetic Compatibility*, Vol. 46, August 2004. pp. 322-328.

- ▶ Jeffrey G. Lewis, "Iraq and GPS Jamming," *ArmsControlWonk.com*, September 15, 2004. Available at: <http://lewis.armscontrolwonk.com/archive/39/iraq-and-gps-jamming>

2003

- ▶ Richard B. Langley, "Iraq and GPS: Some Frequently Asked Questions," Department of Geodesy and Geomatics Engineering, University of New Brunswick, March 13, 2003. Available at: http://www.globalsecurity.org/military/library/report/2003/iraq-and-gps_faq.pdf
- ▶ Stephen Trimble, "In Iraq, GPS Is Surviving Jamming Threat, Pentagon Says," *Aviation Week & Space Technology*, March 25, 2003. Available at: http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=aerospacedaily&id=news/gps.xml
- ▶ Anne Marie Squeo, "Leading the News: U.S. Studies Using 'E-Bomb' in Iraq—Electromagnetic Weapon Can Permanently Damage Telecom, Power Systems," *Wall Street Journal*, February 20, 2003.

2001

- ▶ Jim Wilson, "E-Bomb," *Popular Mechanics*, Vol. 178, No. 9, September 2001, pp. 50–53. Available at: <http://preppug.com/files/EMP/E-Bombs%20And%20Terrorists.pdf>
- ▶ W.A. Radasky, M.A. Messier, and M.W. Wik, "Intentional Electromagnetic Interference (EMI)—Test and data implications," in *Proceedings of the Zurich EMC Symposium*, Zurich, Switzerland, February 2001.
- ▶ "Radio Frequency Interference—And What to Do About It," *Radio-Sky Journal*, No. 4, March 2001. Available at: <http://www.radiosky.com/journal0901.html>

1998

- ▶ R.L. Gardner, "Electromagnetic Terrorism: A Real Danger," in *Proceedings of the 11th Symposium on Electromagnetic Compatibility*, Wroctaw, Poland, June 1998.
- ▶ Ira W. Merritt, "Proliferation and Significance of Radio Frequency Weapons Technology," testimony before the Joint Economic Committee, February 25, 1998
- ▶ David Schriener, "The Design and Fabrication of a Damage Inflicting RF Weapon by 'Back Yard' Methods," testimony before the Joint Economic Committee, February 25, 1998.

1997

- ▶ Eric Rosenberg, "New Threat: Electronic Warfare; Radio Frequency 'Guns' Can Cripple Computers," *Hearst Newspapers*, June 22, 1997.
- ▶ Robert Schweitzer, "RF Weapons and the Infrastructure," submitted to the House Joint Economic Committee on June 17, 1997. Available at: <http://www.house.gov/jec/hearings/espionag/schweitz.htm>

APPENDIX G: LITERATURE—BOTNET TECHNOLOGY AND CIRCUIT BOARD HACKING

- ▶ “Comprehensive National Cybersecurity Initiative,” The White House, Washington, D.C.:
<http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>
- ▶ Peter Gutmann, “The Commercial Malware Industry,” University of Auckland (undated). Available at:
www.cs.auckland.ac.nz/~pgut001/pubs/malware_biz.pdf

2011

- ▶ James Kanter, “E.U. Closes Emissions Trading System After Thefts,” *New York Times*, January 19, 2011. Available at:
<http://www.nytimes.com/2011/01/20/business/global/20iht-carbon20.html>
- ▶ Stephen J. Lukasik, “Reducing Threats to Users of the Global Cyber Commons,” to be published by Communications of the Association for Computing Machinery, 2011.
- ▶ Peter Sommer and Ian Brown, “Reducing Systemic Cybersecurity Risk,” Organisation for Economic Cooperation and Development, OECD/IFP Project on “Future Global Shocks,” January 14, 2011. Available at:
<http://www.oecd.org/dataoecd/3/42/46894657.pdf>
- ▶ William J. Broad, John Markoff, and David E. Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay,” *New York Times*, January 15, 2011. Available at:
<http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>
- ▶ John D. Sutter, “When refrigerators tweet and washing machines test,” CNN, January 8, 2011. Available at:
www.cnn.com/2011/TECH/innovation/01/07/internet.connected.appliances/index.html

2010

- ▶ Stephen J. Lukasik, "Why the ARPANET Was Built," *IEEE Annals of the History of Computing*, Vol. 32, No. 4, 2010. Available at: <http://www.cistp.gatech.edu/publications/files/ARPANETv8.pdf>
- ▶ *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, 2010. Available at: http://www.nap.edu/catalog.php?record_id=12997
- ▶ Stephen J. Lukasik, "A Framework for Thinking About Cyber Conflict and Cyber Deterrence, With Possible Declaratory Policies for These Domains," *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policies*, National Academies Press, 2010. Available at: http://www.nap.edu/catalog.php?record_id=12997
- ▶ Ang Cui and Salvatore J. Stolfo, "A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan," Paper presented at the Annual Computer Security Applications Conference 2010, Orlando, Florida, December 6-10, 2010. Available at: <http://www.cs.utexas.edu/~aseehra/botnets/papers/paper-acsc.pdf>
- ▶ Christopher Dickey, R. M. Schneidman, and Babak Dehghanpisheh, "The Shadow War," *Newsweek*, December 13, 2010. Available at: <http://www.newsweek.com/2010/12/13/the-covert-war-against-iran-s-nuclear-program.html>
- ▶ Hongyu Gao, et al., "Detecting and Characterizing Social Spam Campaigns," ACM Internet Measurement Conference, November 1-3, 2010, Melbourne, Australia; reviewed in *M.I.T. Technology Review*, January–February, 2011. p. 89. Available at: <http://www.cs.ucsb.edu/~ravenben/publications/pdf/fbspam-imc10.pdf>
- ▶ Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec, Version 1.3, November 2010. Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- ▶ William J. Broad and David E. Sanger, "Worm Was Perfect for Sabotaging Centrifuges," *New York Times*, November 18, 2010. Available at: <http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html?hp>
- ▶ "Securing Critical Infrastructure in the Age of Stuxnet," Hearing of the Senate Committee on Homeland Security and Governmental Affairs, November 17, 2010. Available at: http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=954c3149-042e-4028-ae23-754868902c44
- ▶ Seymour M. Hersh, "The Online Threat: Should we be worried about a cyber war?" *New Yorker*, November 1, 2010. Available at: http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?currentPage=all
- ▶ Farhad Manjoo "Don't Stick It In: The Dangers of USB drives," *Slate*, October 5, 2010. Available at: <http://www.slate.com/id/2270003/>
- ▶ William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010. Available at: <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>

- ▶ "Cyberspace Operations: Air Force Doctrine Document 3-12," July 15, 2010. Available at: <http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf>
- ▶ Mark Bowden, "The Enemy Within," *Atlantic Monthly*, June 2010. Available at: <http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/>

2009

- ▶ Stephen J. Lukasik and Rebecca Givner-Forbes, "Deterring the Use of Cyber Force," December 14, 2009. Available at: http://www.cistp.gatech.edu/publications/files/cyber_deterrencev2.pdf
- ▶ Stephen J. Lukasik, "Unleashing Innovation: Making the FCC User-Friendly," *INFO*, Vol. 11, No. 4, 2009. Available at: http://www.cistp.gatech.edu/publications/files/UNLEASHING_INNOVATIONv3.pdf
- ▶ *Technology, Policy, Law, and Ethics Regarding the U.S. Acquisition and Use of Cyberattack Capabilities*, National Academies Press, 2009. Available at: http://www.nap.edu/catalog.php?record_id=12651
- ▶ Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Corporation report for the U.S. Air Force, 2009. Available at: http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf
- ▶ Elaine M. Grossman, "U.S. General Reserves Right to Use Force, Even Nuclear, in Response to Cyber Attack," *Global Security Newswire*, May 12, 2009. Available at: http://gsn.nti.org/gsn/nw_20090512_4977.php

2008

- ▶ John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 13, 2008. Available at: <http://www.nytimes.com/2008/08/13/technology/13cyber.html>

2007

- ▶ Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *New York Times*, May 29, 2007. Available at: <http://www.nytimes.com/2007/05/29/technology/29estonia.html>
- ▶ Carolyn Duffy Marsan, "Lessons learned from Internet root server attack," *Network World*, February 8, 2007. Available at: <http://www.networkworld.com/news/2007/020807-internet-root-server-hack.html>

2003

- ▶ *National Strategy to Secure Cyberspace*, The White House, Washington, D.C., February 2003. Available at: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
- ▶ Victor V. Zhirnov, Ralph K. Cavin, III, James A Hutchby, and George I. Bourianoff, "Limits to Binary Logic Switch Scaling—A Gedanken Model," *Proceedings of the IEEE*, Vol. 91, No. 11, November 2003. Available at: <ftp://download.intel.com/technology/silicon/Bourianoff-Proc-IEEE-Limits.pdf>
- ▶ Stephen J. Lukasik, Seymour E. Goodman, and David W. Longhurst, *Protecting Infrastructures Against Cyber-Attack*, Adelphi Paper 359, International Institute for Strategic Studies, London, 2003.

APPENDIX H: LITERATURE—ADVANCES IN QUANTUM COMPUTING

- ▶ R. Alléaume, et al., “SECOQC White Paper on Quantum Key Distribution and Cryptography,” (undated). Available at:
http://www.secoqc.net/downloads/secoqc_crypto_wp.pdf
- ▶ D. Bacon and W. van Dam, “Recent Progress in Quantum Algorithms; What quantum algorithms outperform classical computation and how do they do it?” *Communications of the ACM*, Vol. 53 No. 2. pp. 84-93, (undated). Available at: <http://cacm.acm.org/magazines/2010/2/69352-recent-progress-in-quantum-algorithms/fulltext>
- ▶ Internet World Stats, “Internet Usage Statistics: The Internet Big Picture,” (undated). Available at: <http://www.internetworldstats.com/stats.htm>
- ▶ D-Wave Inc., “D-Wave quantum computers operating processors available today with 128 qubits,” (undated). Available at:
<http://www.dwavesys.com/index.php?page=quantum-computing>

2010

- ▶ RSA Labs, “Public-Key Cryptography Standards (PKCS),” 2010; Accessed at <http://www.rsa.com/rsalabs/node.asp?id=2165>
- ▶ “Quantum Cryptography,” Wikipedia, 2009. Retrieved on December 2010. Available at: http://en.wikipedia.org/wiki/Quantum_cryptography
- ▶ Erico Guizzo, “Loser: D-Wave Does Not Quantum Compute,” *IEEE Spectrum*, January 2010. Available at:
<http://spectrum.ieee.org/computing/hardware/loser-dwave-does-not-quantum-compute>
- ▶ G. Gross, “Feds say new online privacy rules needed,” IDG News Service, December 16, 2010. Available at:
<http://www.computerworld.com/s/article/9201405/>

Feds say new online privacy rules needed? source = CTWNLE nlt security 2010-12-17

- ▶ C. Biever, "Cryptographers chosen to duke it out in final fight," *New Scientist*, December 2010. Available at: <http://www.newscientist.com/article/dn19865-cryptographers-chosen-to-duke-it-out-in-final-fight.html>
- ▶ S. Barrett and T. Stace, "Fault Tolerant Quantum Computation with Very High Threshold for Loss Errors," *Physical Review Letters*, Vol. 105, 200502, 2010. Available at: <http://prl.aps.org/abstract/PRL/v105/i20/e200502>
- ▶ Z.L. Yuan, "Avoiding the Detector Blinding Attack on Quantum Cryptography," *Nature Photonics*, Vol. 4, 2010. pp. 800-801. Available at: <http://arxiv.org/ftp/arxiv/papers/1009/1009.6130.pdf>
- ▶ Richard Clarke and Rob Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Harper Collins Publishers, 2010. ISBN: 9780061962233.
- ▶ K.S. Choi, et al., "Entanglement of spin waves among four quantum memories," *Nature*, Vol. 468, No. 7322, November 18, 2010. pp.412-6.
- ▶ T.M. Babinec, et al., "A diamond nanowire single-photon source," *Nature Nanotechnology*, Vol. 5, 2010. pp. 195-199. Available at: <http://www.nature.com/nnano/journal/v5/n3/pdf/nnano.2010.6.pdf>
- ▶ R. Keating, "Alarming Tales of International Hacking from a Cyber-Terrorism Czar," *Discover Magazine*, July 2010. Available at: <http://discovermagazine.com/2010/jul-aug/21-the-cyber-warrior>
- ▶ L. Lydersen, et al., "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, Volume: 4, 2010. pp. 686-689.
- ▶ T.D. Ladd, et al., "Quantum Computers," *Nature*, Vol. 464, March 4, 2010. pp. 45-53. Available at: <http://www.nature.com/nature/journal/v464/n7285/full/nature08812.html>
- ▶ E. Knill, "Quantum Computing," *Nature*, Vol. 463, 2010. pp.441-443.
- ▶ M. Luce, "China's Secure Communications Quantum Leap," *China Brief*, Volume X, Issue 17, August 19, 2010.
- ▶ B. Testa, "Something Rich & Strange: Computing In The Quantum Realm," *Processor*, Vol. 32 Issue 21. October 8, 2010. Available at: <http://www.processor.com/editorial/article.asp?article=articles/P3221/33p21/33p21.asp&guid=>
- ▶ L. Wood, "The clock is ticking on encryption: Today's secure cipher-text may be tomorrow's open book," *Computerworld*, December 17, 2010. http://www.computerworld.com/s/article/9201281/The_clock_is_ticking_on_encryption?source=CTWNLE_nlt_security_2010-12-17
- ▶ The Wassenaar Arrangement, <http://www.wassenaar.org/introduction/index.html>; accessed, December 2010.
- ▶ Bruce Schneier, "Schneier on Security blog: Security in 2020," December 16, 2010. Available at: http://www.schneier.com/blog/archives/2010/12/security_in_202.html
- ▶ C. Savage, "U.S. Tries to Make It Easier to Wiretap the Internet," *New York Times*, September 27, 2010.

- ▶ A. Shields, "Quantum Cryptography breakthrough heralds un-crackable communication networks," Toshiba Research Europe Ltd., Cambridge Research Laboratory, Cambridge, UK, April 19, 2010. Available at: <http://www.toshiba-europe.com/research/crl/qig/Press2010-04-19-qcbreakthrough.html>
- ▶ R. Parker, "The spy threat from China Military behind many intrusions," *News Tribune*, July 11, 2010. Available at: http://www.thenewstribune.com/2010/07/11/v-printerfriendly/1259803_the-spy-threat-from-china-military.html
- ▶ A. Radnaev, et al., "A quantum memory with telecom-wavelength conversion," *Nature Physics*, Vol. 6, 2010. pp. 894-899.
- ▶ NIST, "Quantum Information Networks," retrieved December 2010. Available at: <http://math.nist.gov/quant>
- ▶ Quantiki Contributor, "Introduction: The Major Visions and Goals of QIPC," December 2010. Available at: [http://www.quantiki.org/wiki/Introduction: the major visions and goals of qipc](http://www.quantiki.org/wiki/Introduction:_the_major_visions_and_goals_of_qipc)
- ▶ R. Newell, et al., "Quantum Cryptography at Los Alamos National Laboratory: QES & QKarD," 2010. Available at: http://www.lanl.gov/orgs/tt/pdf/techs/quantum_crypt.pdf

2009

- ▶ N. Lutkenhaus and A.J. Shields, "Focus on Quantum cryptography: Theory and Practice," *New Journal of Physics*, retrieved on July 3, 2009. Available at: <http://www.iop.org/EJ/abstract/1367-2630/11/4/045005>
- ▶ Z.J. Lemnios, "Creating Capability Surprise," Chief Technology Officer, MIT Lincoln Laboratory; Department of the Air Force, FA8721-05-C-0002, 2009.
- ▶ R. Kelson, and B. Gittins, "Proprietary Technologies to create 50-to-100 year including Post Quantum: Secure Communications Infrastructure and Secure Collaboration Applications such as e-mail, Instant Messaging, and VoIP," Synaptic Laboratories; 2009. Available at: <http://synaptic-labs.com/>
- ▶ D. Bernstein, "Introduction to Post-Quantum Cryptography," in Daniel J. Bernstein, et al., *Post-Quantum Cryptography*, Berlin: Springer, 2009.
- ▶ Swiss Quantum, "Cryptography," 2009. Available at: <http://www.swissquantum.com/?Cryptography>
- ▶ SQIS, "A Federal Vision for Quantum Information Science," Subcommittee on Quantum Information Science (SQIS), Executive Office of the President, National Science and Technology Council, Washington, D.C., 2009.
- ▶ David Robson, "Most Powerful Ever Quantum Chip Undergoing Tests," *NewScientistTech*, February 24, 2009. Available at: <http://www.newscientist.com/article/mg20126965.600-most-powerful-ever-quantum-chip-undergoing-tests.html>
- ▶ "S&T for National Security," JASON Defense Advisory Panel Report, JSR-OB-146, May 2009. Available at: <http://www.fas.org/irp/agency/dod/jason/sandt-full.pdf>
- ▶ Mikio Fujiwara, et al. "Updating Quantum Cryptography," UQC Report Ver. 1, May 2009. Available at: http://www.uqcc2010.org/archives/images/UQCreport_ver1.pdf
- ▶ J.P. Home, et al., "Complete methods set for scalable ion trap quantum information processing," *Science Express*, August 6, 2009. Available at: <http://nanotechwire.com/news.asp?nid=8352&ntid=&pg=149>

- ▶ Bruce Tarter and Robert Nesbit, "Report on Advanced Computing," Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., March 2009. Available at: <http://handle.dtic.mil/100.2/ADA495920>
- ▶ C.H. Bennett, G. Brassard, and A. Ekert, "Quantum Cryptography," 2009.

2008

- ▶ S. Lloyd, "Riding D-Wave," *MIT Technology Review*, May/June 2008. Available at: http://www.technologyreview.com/read_article.aspx?id=20590&pg=4&ch=infortech&a=f
- ▶ V. Makarov, et al., "Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve," 2008. Available at: [arXiv:0809.3408v2](http://arxiv.org/abs/0809.3408v2)
- ▶ D. James, "Quantum Computing Technology," LANL/Quantum Institute, 2008. Available at: http://www.lanl.gov/physics/quantum/james_qct.shtml
- ▶ EU-Project SECOQC, "Quantum Cryptography Secures Communication in a Commercial Network," Vienna, 2008. Available at: <http://www.secoqc.net/html/technology/enablingtechnology.html>
- ▶ D. Barrett, Jr., "Quantum Cryptography: Operational Impact on 2030 Operations," Air Command and Staff College thesis, Air University, 2008.

2007

- ▶ SecurIST Advisory Board, "Recommendations for a Security Issue 2.0 and Dependability Research Framework," European Commission, January 15, 2007. Available at: ftp://ftp.cordis.europa.eu/pub/ist/docs/trust-security/securist-ab-recommendations-issue-v3-0_en.pdf
- ▶ NISTEP, "Science Map 2004," Study on Hot Research Areas (1999-2004), NISTEP REPORT No. 95, Science and Technology Foresight Center, National Institute of Science and Technology Policy (NISTEP), Ministry of Education, Culture, Sports, Science and Technology (MEXT), Japan, 2007.
- ▶ A. Vance, "D-Wave qubits in the era of Quantum Computing," *The Register*, February 13, 2007. Available at: http://www.theregister.co.uk/2007/02/13/dwave_quantum
- ▶ Zeta Dooly, et al. "ICT Trust, Security and Dependability Research Strategy beyond 2010," Presented at IST Africa, 2007.
- ▶ D. Rosenberg, "Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber," LA-UR-06-5220; *Physical Review Letters*, 98 010503, 2007.
- ▶ Ned Potter, "Quantum Leap: Computer to 'Make Computer History,'" *ABC News*, February 12, 2007. Available at: <http://abcnews.go.com/Technology/story?id=2864363&page=1>
- ▶ L. Greenemeier, "Election Fix? Switzerland Tests Quantum Cryptography," *Scientific American*, October 19, 2007. Available at: <http://www.scientificamerican.com/article.cfm?id=swiss-test-quantum-cryptography>
- ▶ S. Aaronson, "Shtetl-Optimized," April 10, 2007. Available at: <http://scottaaronson.com/blog>

2006

- ▶ F.G. Deng, et al., "Robustness of two-way quantum communication protocols against Trojan horse attack," *Quantum Physics*, June 25, 2006. Available at: <http://arxiv.org/abs/quant-ph/0508168>
- ▶ T. Simonite, "Flat 'ion trap' holds quantum computing promise," *NewScientistTech*, July 2006. Available at: <http://www.newscientisttech.com/article/dn9502-flat-ion-trap-holds-quantum-computing-promise.html>
- ▶ J. Ruttimann, "2020 computing: Milestones in scientific computing," *Nature*, Vol. 440, March 2006. Available at: <http://www.nature.com/nature/journal/v440/n7083/full/440399a.html>
- ▶ Benjamin Wallace-Wells, "Private Jihad: How Rita Katz got into the spying business," *New Yorker*, May 29, 2006. Available at: http://www.newyorker.com/archive/2006/05/29/060529fa_fact?printable=true#ixzz16zFp6Xxu
- ▶ Richard Silbergliitt, et al., "The Global Technology Revolution 2020, In-Depth Analyses Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications," RAND Corporation, 2006. Available at: http://www.rand.org/pubs/technical_reports/2006/RAND_TR303.pdf
- ▶ S. Snow, "Public Key Cryptography 30th Anniversary Conference," Former Technical Director of the U.S. National Security Agency, December 2006.
- ▶ S. Dasgupta, C.H. Papadimitriou, and U.V. Vazirani, "Algorithms," 2006. Available at: <http://www.cs.berkeley.edu/~vazirani/algorithms/all.pdf>

2005

- ▶ E. Jonietz, "Quantum Calculation," *Technology Review*, July 2005. Available at: <http://www.technologyreview.com/Infotech/14591>
- ▶ X.B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," *Physical Review Letters*, Vol. 94, 230503, 2005.
- ▶ H.K. Lo, H.F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and Proof of its Security," *Journal of Cryptography*, Vol. 18, No. 133, 2005.
- ▶ J. Ouellette, "Quantum Key Distribution," *The Industrial Physicist*, American Institute of Physics, December 2004/January 2005.
- ▶ R. Dettmer, "Light holds the key," *IEE Review*, Vol. 51, Iss. 7, July 2005.

2004

- ▶ V. Scarani, et al., "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters*, 92, 057901, 2004.
- ▶ Tom Spring, "Al Qaeda's Tech Traps, Investigations, arrests highlight how technology aids and weakens terror network," *PC World*, September 1, 2004. Available at: http://www.pcworld.com/article/117658/al_qaedas_tech_traps.html
- ▶ "A Quantum Information Science and Technology Roadmap," ARDA, LANL LA-UR-04-1778, April 2, 2004. Available at: <http://qist.lanl.gov>

2003

- ▶ W.Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters*, Vol. 91, 057901, 2003.
- ▶ Anton Zeilinger, "Quantum Teleportation," *Scientific American*, Scientific American Collection "The Edge of Physics," 2003.
- ▶ K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Physical Review A*, Vol. 68, Issue 2, 2003.

2002

- ▶ Aris A. Pappas and James M. Simon, Jr., "Daunting Challenges, Hard Decisions—The Intelligence Community: 2001-2015," *Studies in Intelligence*, Vol. 46, No. 1, 2002. Available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no1/article05.html>
- ▶ Marco A. Barreno, "The Future of Cryptography Under Quantum Computers," Dartmouth College Computer Science Technical Report TR2002-425, July 21, 2002. Available at: <http://www.cs.dartmouth.edu/~sws/theses/marco.pdf>
- ▶ K. Inoue, E. Waks, and Y. Yamamoto, "Differential Phase Shift Quantum Key Distribution," *Physical Review Letters*, Vol. 89, 037902, 2002.
- ▶ S. Vittorio, "Quantum Cryptography: Privacy through Uncertainty," October, 2002. Available at: <http://www.csa.com/discoveryguides/crypt/overview.php>
- ▶ N. Gisin, et al. N., "Quantum cryptography," *Reviews of Modern Physics*, Vol. 74, January 2002.

2001

- ▶ Justin Mullins, "The Topsy Turvy World of Quantum Computing," *IEEE Spectrum*, February 2001. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=00898799>
- ▶ Bruce Schneier, "Bruce Schneier on crypto, the FBI, privacy and more," October 3, 2001. Available at: <http://www.theregister.co.uk/content/archive/21993.html>
- ▶ J.S. Katz and S. Stewart, "Science Foresight, Project Final Report," DSTL/TR01697, Ministry of Defence, UK, 2001.

2000

- ▶ Cryptography and Liberty 2000, "An International Survey of Encryption Policy," (Electronic Privacy Information Center), 2000, pp. 15-20.
- ▶ Jacob West, "The Quantum Computer," Computer Science at CalTech, April 28, 2000. Available at: <http://www.cs.caltech.edu/~westside/quantum-intro.html>
- ▶ D. DiVincenzo, "The Physical Implementation of Quantum Computation," IBM, April 13, 2000. Available at: <http://arxiv.org/abs/quant-ph/0002077>
- ▶ G. Brassard, et al., "Security Aspects of Practical Quantum Cryptography," *Lecture Notes in Computer Science*, Volume 1807/2000, 2000.
- ▶ Alan Boyle, "A Quantum Leap in Computing," MSNBC, May 18, 2000. Available at: <http://www.msnbc.msn.com/id/3077363>

- ▶ Arjen K. Lenstra, "Integer Factoring," *Designs, Codes and Cryptography*, Vol. 19, Iss. 2-3, 2000.
- ▶ J. Birnbaum, and R.S. Williams, "Physics and the Information Revolution," *Physics Today*, Vol. 53, No. 1, January 2000, pp. 38-42.

1999

- ▶ News World Communications, "Enemies of the State," September 13, 1999. Available at: <http://www.mail-archive.com/ctrl@listserv.aol.com/msg21747.html>
- ▶ Q. Liang and W. Xiangsui, "Unrestricted Warfare," Beijing: PLA Literature and Arts Publishing House, 1999.
- ▶ Kevin Maney, "Beyond the PC: Atomic QC," *USA Today*, July 14, 1999. Available at: http://www.amd1.com/quantum_computers.html
- ▶ Lov K. Grover, "Quantum Computing," *The Sciences*, July/August 1999. Available at: <http://cryptome.org/qc-grover.htm>

1998

- ▶ J. Preskill, "Reliable Quantum Computers," *Proceedings of the Royal Society of London*, A454, 1998, pp. 385-410.
- ▶ Lydia L. Sohn, "A Quantum Leap for Electronics," *Nature*, Vol. 394, No. 6689, July 1998.
- ▶ D.G. Cory, et al., "Experimental Quantum Error Correction," American Physical Society, Physical Review Online Archive, September 1998. Available at: http://prola.aps.org/abstract/PRL/v81/i10/p2152_1

1997

- ▶ Louis Freeh, Testimony before the Senate Judiciary Subcommittee on Terrorism, Technology & Government Information, September 3, 1997.
- ▶ N. Gershenfeld and I.L. Chuang, "Bulk Spin Resonance Quantum Computation," *Science*, Vol. 275, 1997.
- ▶ G. Brassard, "Quantum Information Processing: The Good, the Bad, and the Ugly," 1997.
- ▶ S. Lloyd, "Quantum-Mechanical Computers," *Scientific American*, 1997. pp. 98-104.
- ▶ P.W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer (AT&T Research)," *SIAM J. Sci. Statist. Comput.*, Vol. 26, 1997.
- ▶ Simone Bone and Matias Castro, "A Brief History of Quantum Computing," Imperial College, London, Department of Computing, 1997. Available at: http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/
- ▶ C.H. Bennett, et al. "The Strengths and Weaknesses of Quantum Computation," *SIAM Journal on Computing*, Vol. 26, No. 5, 1997.

1996

- ▶ Tad Hogg, "An Overview of Quantum Computing." "Quantum Computing and Phase Transitions in Combinatorial Search," *Journal of Artificial Intelligence Research*, Vol. 4, 1996. pp. 91-128. Available at: <http://www.cs.cmu.edu/afs/cs/project/jair/pub/volume4/hogg96a.html/node6.html>

- ▶ Bruce Schneier, *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996, ISBN 0-471-11709-9.
- ▶ Lov K. Grover, "A fast quantum mechanical algorithm for database search," Proceedings, 28th Annual ACM Symposium on the Theory of Computing, May 1996.
- ▶ A. Ekert and R. Jozsa, "Quantum Computation and Shor's Factoring Algorithm," *Reviews of Modern Physics*, 68, 1996. pp. 733-754.

1995

- ▶ S. Lloyd, "Quantum Computation," *Scientific American*, Vol. 273, No. 4, 1995. pp. 44-50.
- ▶ J. Glanz, "A Quantum Leap for Computers?" *Science*, Vol. 269, pp. 28-29, 1995.
- ▶ D. DiVincenzo, "Quantum computation," *Science*, Vol. 270, 1995, p. 255.
- ▶ C.H. Bennett, "Quantum information and computing," *Physics Today*, Vol. 48, No. 10, October 1995, pp. 24-30.

1994

- ▶ P.W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," Proceedings of the 35th Annual Symposium Foundations of Computer Science, Vol. 124, 1994.

1985

- ▶ D. Deutsch, "Quantum Theory, the Church-Turing Principle, and the Universal Quantum Computer," *Proceedings of the Royal Society of London, Series A, Mathematical and Physical Sciences*, Vol. 400, No. 1818, July 1985. pp. 97-117.

1984

- ▶ C. Bennett and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 1984. p. 175.

1982

- ▶ R.P. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics*, Vol. 21, 1982. pp. 467-488.

1971

- ▶ Walker Publishing Group, "The Correspondence between Albert Einstein and Max and Hedwig Born," 1971.

1964

- ▶ J.S. Bell, "On the Einstein, Podolsky, Rosen Paradox," *Physics*, Vol. 1, 1964. pp. 195-200.

1935

- ▶ Albert Einstein, et al. "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?" *Phys. Rev.*, Vol. 47, No. 777, 1935. Available at: http://www.phys.uu.nl/~stiefelh/epr_latex.pdf

APPENDIX I: LITERATURE—E-BOMBS

2007

- ▶ Bayram Mert Deveci, "Directed-Energy Weapons: Invisible and Invincible?" Naval Postgraduate School thesis, September 2007. Available at: http://edocs.nps.edu/npspubs/scholarly/theses/2007/Sep/07Sep_Deveci.pdf

2006

- ▶ James A. Horkovich, "Directed Energy Weapons: Promise and Reality," Paper presented at 37th AIAA Plasmadynamics and Lasers Conference, June 5-8, 2006.

2005

- ▶ Doug Beason, *The E-bomb: How America's New Directed Energy Weapons will Change the Way Future Wars will be Fought*, Cambridge, MA: Da Capo Press, 2005.
- ▶ David A. Fulghum, "Microwave Weapons Emerge," *Aviation Week & Space Technology*, Vol. 162, June 13, 2005.
- ▶ Michael Sirak, "Directed-energy Protection Systems Unveiled by Raytheon," *Jane's Defence Weekly*, September 30, 2005.

2004

- ▶ EdI Schamiloglu, "High Power Microwave Sources and Applications," IEEE Microwave Theory and Techniques Society, Fort Worth, TX, 2004. Available at: <http://www.ece.unm.edu/ifis/papers/MTT.pdf>

2003

- ▶ M. Abrams, "Dawn of the E-bomb," *IEEE Spectrum* Vol. 40, 2003. pp. 24-30.

2001

- ▶ Robert J. Barker and Edl Schamiloglu, *High-power Microwave Sources and Technologies*, New York: IEEE Press, 2001.
- ▶ Sandra I. Erwin, "Directed-energy Weapons Promise 'Low Cost Per Kill,'" *National Defense*, Vol. 86, September 19, 2001.
- ▶ Larry D. Welch and Donald C. Latham, "Defense Science Board Task Force on High Energy Laser Weapon Systems Applications," Defense Science Board, Washington D.C., 2001.
- ▶ Jim Wilson, "E-Bomb," *Popular Mechanics*, Vol. 178, No. 9, September 2001. pp. 50-53. Available at: <http://prepbug.com/files/EMP/E-Bombs%20And%20Terrorists.pdf>

2000

- ▶ Mark Hewish, "Beam Weapons Revolution: Directed-energy Weapons Point the Way for Battlefield Technology," *International Defense Review*, August 17, 2000.
- ▶ Eileen M. Walling, "High Power Microwaves: Strategic and Operational Implications for Warfare," Occasional Paper No. 11, Center for Strategy and Technology, Air War College, Air University, Maxwell Air Force Base, Alabama, February 2000. Available at: <http://www.globalsecurity.org/military/library/report/2000/occppr11.htm>

1998

- ▶ Victor Sheymov, "The Low Energy Radio Frequency Weapons Threat to Critical Infrastructure," Joint Economic Committee, United States Congress, 1998.

1997

- ▶ Christopher C. Bolkcom and Joseph A. Tatman, "Directed Energy Technologies," *Jane's Defence Weekly*, January 7, 1997.

1995

- ▶ Cecil John, "Directed Energy Warfare," *Journal of Electronic Defense*, June 1995.

1991

- ▶ Don White, "HEW and Electromagnetic Terrorism," *EMC Technology*, Volume 10/Number 3, January/February 1991.
- ▶ E. Van Keuren, J. Wilkenfeld, and J. Knighten, Utilization of High-Power Microwave Sources in Electronic Sabotage and Terrorism, *IEEE*, 1991. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=202184&userType=inst>

1985

- ▶ Cosmo DiMaggio, "Directed Energy Weapons Research: Status and Outlook," Congressional Research Service, Library of Congress, 1985.

1984

- ▶ Jeff Hecht, *Beam Weapons: The Next Arms Race*, New York: Plenum Press, 1984.

