The background of the cover is a dark, atmospheric painting. In the foreground, a large wooden horse is mounted on a wheeled cart, moving across a dark street. Several small figures are visible in the distance, some appearing to be pulling or guiding the cart. In the background, a large, multi-story building with arched windows and a prominent tower with a flag is visible. The overall scene is dimly lit, with a focus on the central horse and the architectural details of the buildings.

Strategic Latency: Red, White, and Blue

Managing the National and International Security Consequences of Disruptive Technologies

Zachary S. Davis and Michael Nacht, editors

Center for Global Security Research
Lawrence Livermore National Laboratory

February 2018

Disclaimer:

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

Strategic Latency: Red, White, and Blue:
Managing the National and
International Security Consequences
of Disruptive Technologies

Zachary S. Davis and Michael Nacht, editors

Center for Global Security Research
Lawrence Livermore National Laboratory
February 2018

Table of Contents

Introduction Strategic Latency: Red, White, and Blue <i>Zachary Davis and Michael Nacht</i> _____	1
<hr/>	
Section 1	
The Red Side: S&T Threat Analysis for Strategic Warning	11
Chapter 1 Biotechnology, Commercial Veiling, and Implications for Strategic Latency: The Exemplar of Neuroscience and Neurotechnology Research and Development in China <i>Celeste Chen, Jacob Andriola, and James Giordano</i> _____	12
Chapter 2 “Sputnik-like” Events: Responding to Technological Surprise <i>Ron Lehman</i> _____	33
Chapter 3 Curious Incidents: Dogs That Haven’t Barked <i>C. Wes Spain</i> _____	52
Chapter 4 Emerging Trends in Big Data and Artificial Intelligence: Directions for the Intelligence Community <i>James Canton</i> _____	71
Chapter 5 3D Printing: Acknowledging the Dark Side and Why Speaking Openly About Technology Threat Vectors Is the Right Answer <i>Jennifer J. Snow</i> _____	88
<hr/>	
Section 2	
The White Side: Latent Technology Trends and Timelines	103
Chapter 6 New Technologies and International Order <i>Paul Bracken</i> _____	104
Chapter 7 New Is Not Always Better <i>David S.C. Chu, with the assistance of Allison Fielding Taylor</i> _____	115

Chapter 8	
What's Old Is New Again: Nuclear Capabilities Still Matter—and Will for a Long Time to Come	
<i>Joseph F. Pilat</i>	130
Chapter 9	
Backseat Driving: What Happens When Technology Outpaces Strategy?	
<i>Leo J. Blanken and Jason J. Lepore</i>	146
Chapter 10	
Terrorist Tech: How Will Emerging Technologies Be Used by Terrorists to Achieve Strategic Effects?	
<i>Zachary Davis and Michael Nacht</i>	160
Chapter 11	
The Latent Potential of Privacy Technologies: How Our Future Will Be Shaped by Today's Privacy Decisions	
<i>William Welser IV, Rebecca Balebako, Cameron Colquhoun, Osonde Osoba</i>	171
Chapter 12	
An Effects-Based Framework for Evaluating Latent Technology	
<i>Daniel Tapia-Jimenez</i>	187
<hr/>	
Section 3	
The Blue Side: Technology Innovation and National Security Applications	201
Chapter 13	
What Works? Public–private Partnerships for Development of National Security Technology	
<i>Frank D. Gac, Timothy P. Grayson, and Joseph M. Keogh</i>	202
Chapter 14	
Moving at the Speed of S&T: Calibrating the Role of National Laboratories to Support National Security	
<i>Lisa Owens Davis</i>	233
Chapter 15	
Picking Winners and Losers: How the Government Can Learn to Successfully Assess Technology Potential and Turn It into a Battlefield Advantage	
<i>Toby Redshaw</i>	250

Chapter 16

Strategic Latency, Technology Convergence, and the Importance of the Weapons Mix

Brian Holmes _____ 262

Chapter 17

Predicting and Guiding Change in the New Economy of Strategic Latency

Ben Forster _____ 269

Chapter 18

Closing Thoughts: Humanity, Machines and Power

Zachary Davis and Michael Nacht _____ 287

Author Biographies

Introduction

Strategic Latency: Red, White, and Blue

Zachary Davis and Michael Nacht

Technology is nothing. What's important is that you have a faith in people, that they're basically good and smart, and if you give them tools, they'll do wonderful things with them.

—Steve Jobs

Steve Jobs got it half right. People imagine, develop, and use technology to achieve “wonderful things,” but they also use technology to pursue harmful objectives. Insecurity, anger, jealousy, and greed are just as likely to motivate technological innovation as love, compassion, creativity, and altruism. Judgments about whether technological feats are wonderful or terrible are themselves highly subjective—one person’s big scientific breakthrough can just as easily turn out to be another person’s political, military, or economic disaster.

Nuclear technology, for example, makes possible life-saving medical treatments and clean energy that can help save the world from catastrophic climate change, yet also creates the means to wage nuclear war. Most technologies possess this Janus-faced potential, which we call *strategic latency*. The challenge for national-security policymakers is to harness the benefits of technology while preventing it from being used against us. This volume explores that dilemma.

We live in an era preoccupied with technology. Much has been written about Moore’s Law and the pedal-to-the-metal acceleration of technological progress in recent years. What will the onslaught of ubiquitous technology mean for individuals, society, nations and the world? Technology optimists speculate about how technology will solve the world’s hardest

problems and herald a new age of abundance.¹ Utopians, technocrats, some futurists, and Silicon Valley icons embrace technology as the lead agent of human progress. Pervasive technologies such as genetic engineering, robotics, artificial intelligence (AI), and the Internet of Things will (or already do) touch every facet of human existence, thereby making life easier by liberating people from the struggle for survival, freeing them to pursue more creative, productive, and enlightened lives.

With disease and poverty on the run, people around the globe will use universal access to information to satisfy the basic food, energy, and transportation needs of an enlightened populace. In a world of material abundance, there will be nothing left to fight over. Global commerce and consciousness will render nation-states obsolete and pave the road to permanent peace.² Technology will leapfrog over politics to provide the missing link in a progressive evolution worthy of philosophical optimists in the tradition of Immanuel Kant and Jean-Jacques Rousseau.

Other observers of technology futures warn of potential dangers, including existential threats associated with artificial intelligence, autonomous vehicles, and the unintended consequences of genetic engineering. Even high-tech luminaries such as Bill Gates, Elon Musk, Stephen Hawking, and Steve Wozniak openly express concern about the potential loss of human control over these otherwise beneficial developments.³ In open letters about unintended consequences, concerned scientists warned that massively powerful machines could misinterpret human intentions and turn on their masters, or give terrorists unprecedented destructive power. Military leaders promise to “keep humans in the loop” to preserve the role of ethical norms in warfare, but what happens when the machines determine that they know better than their flawed creators? From Frankenstein to HAL in *2001: A Space Odyssey* to the Terminator, the risk that our creations could betray us is inherent in the notion of technological progress.

Echoing Manhattan Project scientists’ admonitions about proliferation and the effects of atomic power on world politics,⁴ concerned scientists have called autonomous weapons “the Kalashnikovs of tomorrow,” poised to wreak havoc throughout the world, not necessarily as weapons of mass destruction, but as easily acquired commodities loaded with potential to upend global norms of war and politics.⁵ The specter of rogue drone swarms, genetic monsters, robot armies, death rays, and weird science may not

1 Peter Diamandis and Steven Kotler, *Abundance: The Future Is Better Than You Think* (New York: Free Press, 2014).

2 Ayesha and Parag Khana, *Hybrid Reality: Thriving in the Emerging Human-Technology Civilization* (TED Books, June 2012).

3 Open Letter on Research Priorities for Robust and Beneficial Artificial Intelligence, January 2015, accessed October 27, 2017, <https://futureoflife.org/ai-open-letter/>.

4 See for example the Franck Report, issued by nuclear scientists in 1945, accessed October 27, 2017, <http://www.atomicheritage.org/key-documents/franck-report>.

5 Autonomous Weapons: An Open Letter from AI and Robotics Researchers, July 28, 2015, <https://futureoflife.org/open-letter-autonomous-weapons/>.

be such a leap of imagination for Silicon Valley visionaries steeped in a culture known for bold thinking. In response, AI optimists fired back with a report of their own, calling the signatories of the AI and AV letters “alarmists,” and “neo-Luddites.”⁶

Undaunted, thoughtful tech sentinels applaud and support the benefits that technology brings to humanity, but nonetheless feel obligated to call attention to potential dangers. The strategic latency concept embraces technological progress while casting a critical eye on the history of warfare throughout human history. Lawrence Livermore National Laboratory, with its roots in the Manhattan Project and continued commitment to pursuing science in the national interest, is ideally suited to illuminate the challenges inherent in technology, and with its partners convened the Strategic Latency Project to study how emerging technologies benefit and threaten security in the modern world. We reached out to a broad spectrum of experts to bring rigor and clarity to this extremely complex and crosscutting topic.

Humankind’s dual capacity for compassion and cruelty, ingrained from the Stone Age to our present circumstances, suggests it would be unrealistic to assume that the “better angels of our nature” will invariably govern the quest for power. As the theologian Reinhold Niebuhr observed, “Society merely cumulates the egoism of individuals and transmutes their individual altruism into collective egoism so that the egoism of the group has a double force.” The result is the security–power dilemma that describes contemporary international politics.⁷

In the quest for power, humans develop tools to protect themselves and sometimes move beyond defense to pursue aggressive impulses. Technology can be channeled toward “soft” or “hard” power incarnations, depending on individual and collective motivations. There is abundant evidence on both sides of the ledger to illustrate human ingenuity in the peaceful and military applications of technology. While intentions—good and bad—clearly motivate innovation, curiosity and the spirit of exploration also drive people to experiment with new ideas. From da Vinci to the Wright brothers, some of the most inspired scientific advancements were inspired by motivations other than material gain. If necessity is the mother of invention, imagination is the father.

Our Strategic Latency Project has examined optimism and pessimism associated with the future applications of lasers, nanotechnology, additive manufacturing, nuclear technology, gene-editing techniques such as CRISPR, and other technologies. We appreciate the seeming contradictions that can lead life-saving technologies in unintended negative directions, or prompt military technologies toward peace and prosperity through spinoffs or war-avoiding defenses. In this volume, we are trying to advance our understanding of the

6 Information Technology and Innovation Foundation, “2015 ITIF Luddite Award Nominees: The Worst of the Year’s Worst Innovation Killers,” December 2015, accessed October 27, 2017, <https://itif.org/publications/2015/12/21/2015-itif-luddite-award-nominees-worst-year%E2%80%99s-worst-innovation-killers>.

7 Reinhold Niebuhr, quoted in Kenneth W. Thompson, *Masters of International Thought: Major Twentieth Century Theorists and the World Crisis* (Baton Rouge: Louisiana State University Press, 1980), 29.

human and technological factors that push and pull science in these directions. We look at complex motivations, including traditional state-based security requirements, economics, bureaucratic politics, and ideology as they commingle to shape the way humans use technology for security.

Sorting out which motivations drive innovation in particular technology areas takes complexity to new levels. We do not claim to have organized the hard and “soft” science relationships that exist among multiple causal factors and levels of analysis within a comprehensive theoretical framework, and we remain skeptical about the prospects for predictive modeling to forecast how groups and individuals will apply technology to their security. Instead, this volume represents a heuristic device to organize some of the most thoughtful research on the concept of strategic latency as it relates to national security.

The book is divided into three sections: Red, White, and Blue. Red refers to the acquisition of critical technologies by foreign adversaries and the challenge of strategic warning. Which countries and groups are developing the capacity to seriously harm the U.S. or others? The job of strategic warning rests with our intelligence community, which bears the responsibility for informing policymakers about emerging threats. How do we know if our adversaries will exploit technologies that clearly have potential for strategically significant military, economic, or political applications, but also have civilian applications that contribute to national and international well-being? White provides political, intellectual, and historic context for scientific and technical (S&T) innovation in national security. Blue examines U.S. efforts to direct the benefits of S&T innovation to U.S. national security requirements.

An Overview of the Chapters

The Red section begins with a study by James Giordano, Celeste Chen, and Jacob Andriola on China’s research and development in the field of neurobiology. China may not follow longstanding norms and practices established to govern the development and application of latent technologies, and is amassing impressive latent potential in the neurobiological sciences that could be transformed and weaponized in unprecedented ways. In their chapter, the authors posit a model for how China is laying a dual-use groundwork that can be transformed to produce military applications. This is the essence of strategic latency.

In his chapter, Ron Lehman revisits lessons learned from the Soviet launch of Sputnik, which triggered a massive S&T response from the United States to close perceived gaps in U.S. capabilities. He argues that the capacity to respond effectively, as the U.S. did in the 1960s, is more important than reacting to every technology advancement that could become a threat. As the U.S. confronts a myriad of technological challenges, this remains true today.

Wes Spain’s chapter explores why some perceived threats never materialize, yet still evoke hyperactive reactions, especially in intelligence circles. Individuals and institutions follow incentives to hype certain issues and ignore others. Spain focuses on biothreats and

man-portable anti-aircraft weapons to show how dramatic scenarios can overwhelm sober analysis and distort threat perceptions.

Next, futurist James Canton surveys the horizon of artificial intelligence that is transforming society and suggests how these trends could revolutionize intelligence and strategic warning worldwide. To conclude the Red section, Jennifer Snow uses the examples of additive manufacturing and 3D printing to show that governments stand little chance of keeping pace with global S&T developments—unless they engage directly with nontraditional communities such as hackers, makers, and DIY enthusiasts who are on the cutting edge of innovation. Outreach to these “self-regulating communities” can provide the government with unique insights and willing partners against technology threats.

The White section offers perspective on latent technologies past and present. Perhaps our preoccupation with the latest shiny objects is clouding our appreciation for the latent potential of old technologies, which in many cases are better positioned to deliver strategic effects than unproven new ideas. Indeed, our previous study of private-sector perspectives of technology competition emphasized the importance of business models as being equally or more disruptive than particular technologies.⁸ The essays in this section question whether we have the right analytic constructs to attack the problem of strategic latency, or perhaps should think about it differently.

Paul Bracken warns that the current global order was not designed to govern today’s technology revolution, and that the leveling effects of technology diffusion have become a centrifugal force that is pulling apart the post-World War Two international system. He advocates a new strategy to cope with the leveling effects that multiple converging technologies are having on world order.

Economist David Chu reviews the modern history of military strategy and technology to show how political, economic, cultural, and underappreciated contextual factors shape decision-making about defense expenditures, often leading to bad choices and disastrous strategy. Chu argues that greater appreciation for proven technologies and adversary objectives should weigh heavily on decisions about military technology, especially purchases of major systems.

Next, Joe Pilat reminds us of the preeminent place of nuclear energy in the pantheon of latent technologies and its unmatched effects on world politics. Pilat argues that few if any current technologies can match the nuclear revolution. By this standard of military potential, recent technological wonders such as cyberattacks and AI would not qualify as true strategic weapons. His chapter raises important questions about our standards for strategic significance.

⁸ Expert Advisory Panel Workshop, *Strategic Latency and Warning: Private Sector Perspectives on Current Intelligence Challenges in Science and Technology*, (Livermore: Lawrence Livermore National Laboratory, January 8, 2016).

Professors Leo Blanken and Jason Lepore offer alternative models to integrate technology innovation assessments as a major element of military strategy in a competitive international system. They use game theory modeling to capture the tension between competitive markets and security-seeking states and offer sobering conclusions for defense spending on new technologies. All that glitters, they warn, is not gold.

Addressing the issue of non-state actors, the editors, Zachary Davis and Michael Nacht, examine developments in terrorist innovations to determine if new technologies will greatly enhance their lethal firepower to the point of giving them strategic leverage. We argue that graduated advancements in terrorist capabilities due to the incorporation of new technologies and disruptive tactics are certain to occur, but unlikely to produce truly strategic effects. We conclude that nuclear weapons stand alone as potential game changers.

The chapter by the RAND team of Welser, Balebako, Colquhoun, and Osoba examines the strategic potential that is latent in massive collections of data about individuals and the potential levers that will control privacy and regulate access to centralized data centers. The authors project three alternative futures to illustrate how the latent potential of data collections and the control of them will shape the geopolitical balance of power by redefining citizenship and national identity.

To conclude the White section, Daniel Tapia Jimenez offers a constructivist perspective on strategic latency that views current and emerging technologies as strategically important if they incorporate at least two of five possible characteristics: they change technical capabilities, they change the means or methods of interaction, they change belief systems, or they change the way we think about issues. He uses the advent of submarine-launched ballistic missiles as an historic case study to show how they changed the concept of deterrence, and then applies his framework to additive manufacturing to determine if it meets the criteria to be classified as a strategically latent technology.

The Blue section explores how the U.S. government tries to develop latent technologies for use by the national security establishment. The Third Offset⁹ initiative launched by then Secretary of Defense Ashton Carter was inspired by frustration that the government has become stymied by a cumbersome and self-defeating procurement system that is so bogged down by bureaucracy that it cannot provide cutting-edge weapons to the warfighters.¹⁰ What can be done?

Championed by Deputy Defense Secretary Robert Work, the Third Offset explores ways to expedite the process to ensure that American warfighters of the future will be armed with the most advanced weapons. One of the lessons of strategic latency is that even the most

9 The so-called first offset was the initial nuclear revolution; the second offset was the Carter–Reagan fueled Revolution in Military Affairs.

10 Remarks by Deputy Secretary Bob Work on Third Offset Strategy, Brussels, Belgium, April 28, 2016, accessed October 27, 2017, <https://www.defense.gov/News/Speeches/Speech-View/Article/753482/remarks-by-d%20eputy-secretary-work-on-third-offset-strategy>.

advanced weapons can be defeated unless they are embedded in a strategy that takes into account the human factors examined in the Red and White sections. The technologies we select for the warfighter of tomorrow risk being ineffectual unless they anticipate the adversary's objectives, strategy, culture, and capabilities, not just counter their technology.

In their chapter, Frank Gac, Tim Grayson and Joe Keogh survey the new mechanisms developed to accelerate government access to cutting-edge technologies and assess their track record. Taking a close look at public-private partnerships spawned by government-sponsored entities such as the Defense Advanced Research Projects Agency (DARPA), In-Q-Tel, and the Defense Innovation Unit Experimental (DIUx), they review successes and failures and derive lessons for future partnerships.

Building on the theme of public-private partnerships, Lisa Owens Davis looks at the role of national laboratories as innovation incubators and evaluates ways that the government and the labs can maximize the labs' contributions to national security. She flags the national laboratories' unique capabilities in simulation, modeling, and rapid prototyping as a "sweet spot" for the labs to use their "big science" capabilities to fill a gap between the pure scientific research of academia and the production capabilities of private industry.

Toby Redshaw provides a business perspective on high-tech innovation. He argues against trying to enlist the creative chaos of the private sector to pursue technologies for national defense. He warns that Silicon Valley's tolerance for risk and failure are not transferable to government priorities funded by tax dollars. Moreover, the operational speed characteristic of high-tech business means that government is ill suited to harness those practices, especially for purchases of major weapon systems. Redshaw advises us to develop clear technology priorities and objectives and embrace innovation wherever possible, especially in terms of organizational culture and workforce incentives.

Brian Holmes defends experiments like DIUx and the Intelligence Advanced Research Program as agents of incremental change that should not be judged on short-term outcomes but on their contributions to long-term systemic change in U.S. technology procurement practices. Holmes praises these technology procurement innovations for bringing a multidisciplinary, strategic policy-minded approach to the U.S. response to strategic latency. These are, in his view, essential pieces of an overall "weapons mix" that can be calibrated to changing defense requirements.

The Blue section concludes with an essay by Ben Forster, who looks at the economic drivers of technology innovation in the defense sector. Macroeconomic theories explain national investments in technologies with commercial and military potential, such as computers and aircraft. However, microeconomics best describes the fierce commercial competition that fuels so much of the underlying technologies for modern defense systems. He argues that global markets for talent and capital will outstrip the technical needs of national defense policies. Innovative purchasing models such as those being developed by DIUx and DARPA can help to ameliorate some of these market hazards.

The Red, White, and Blue framework of the book covers a lot of territory. The goal was to encompass the massively multidisciplinary nature of the topic, which includes equal parts pure research, applied sciences, economics and business, international relations theory, and security studies. Strategy demands that all of these complex fields of study be focused on specific countries, groups, and regions to build appreciation for adversary intentions and capabilities. We add to this aggregate analysis contributions from anthropology, ethics, bureaucratic politics, organizational theory, psychology, sociology, and, of course, science fiction.

While recognizing the existence of linkages among these factors, causation remains elusive. Is technology driving behavior, or vice versa? Necessity may be one of the mothers of invention, but it shares patronage with curiosity and creativity as motivations for scientific achievement. As a group, the chapter authors acknowledge the sprawling complexity that defies simplification into more tractable problem sets. Each chapter incorporates the variables most relevant to the analytic objective; none of us claim to have discovered a unified field theory for strategic latency. We gave the authors wide range to address their topics and did not enforce uniformity. By dividing the book into the three categories we hope to establish three discernable lines of inquiry: Red for foreign threat assessment and strategic warning, White for conceptual frameworks and grand strategy, and Blue for operational plans and procurement. We hope that this analytic framework provides structure on which to advance our understanding of strategic latency.

Acknowledgments

The people who follow strategic latency do so out of a sense of duty, often without strong institutional support. We have been fortunate to have strong and consistent support from several institutions. Lawrence Livermore National Laboratory has stepped up to the plate by devoting resources and people to the Strategic Latency Project. This has enabled the Center for Global Security Research (CGSR) to take the lead in organizing workshops and funding the research in this volume.

Lab Director Bill Goldstein, CGSR Director Brad Roberts, Deputy Director Mona Dreicer, former LLNL weapons program director Bruce Goodwin, and CGSR administrators Sandra Maldonado and Katie Thomas made the Latency Project possible through their support and guidance. Z Program Manager Nils Carlson cheered our progress and enabled the participation of key experts. We owe a special debt to Paris Althouse, who navigated the contract maze that led us from concept to completion. Tom Bentley of *The Write Word* performed editorial services beyond the call of duty. Harry Flashman provided inspiration. Former CGSR Director Ron Lehman is the intellectual godfather of strategic latency and continues to be a thought leader.

Similarly, National Intelligence Manager Larry Gershwin provided intellectual and material support from the outset. His former deputy at the National Intelligence Council and Los

Alamos National Laboratory (LANL), scientist Frank Gac, has been instrumental in guiding the project and coordinating with current and former scientific and technical intelligence (S&TI) officials. LANL Director Charlie MacMillan provided input and advice at key junctures.

Brian Shaw, Dean at National Intelligence University, School of Science and Technology, has been a co-conspirator from the outset. His insights and guidance, especially regarding strategic warning and threat analysis, are built into the foundations of the book. Jim Stokes at the Office of the Secretary of Defense supported innovative research at the Naval Postgraduate School and collaboration with academic and government institutions. Finally, we are indebted to the scientists and engineers who have devoted their careers to national service. Without them, the risks to our country would be greater and the responses weaker.

1

The Red Side:

S&T Threat Analysis for Strategic Warning



Chapter 1

Biotechnology, Commercial Veiling, and Implications for Strategic Latency: The Exemplar of Neuroscience and Neurotechnology Research and Development in China

Celeste Chen, Jacob Andriola, and James Giordano

Introduction

Within the past ten years, Chinese leaders have come to recognize science research and development (R&D), technological innovation, and intellectual property policies as critical means through which to strengthen China's global economic power. Both former President Hu Jintao and current President Xi Jinping have emphasized that China's future development in these areas stands as an overarching theme across its policy and planning blueprints, and figures heavily in achieving (1) sustainable economic growth, (2) increased social welfare, and (3) movement up what Chinese national planning documents term the "global value chain."

Because Chinese leaders continue to recognize innovation as key to securing and sustaining China's future, science and related biotechnology R&D will play increasingly larger roles in national priorities and strategies. Over the past ten years, Chinese leaders have shifted research efforts aimed at maintaining population health and reaching hard production targets for strategic initiatives that target emerging industries, scientific development, and infrastructure geared towards achieving "long-term, steady, and relatively

rapid economic development.”¹ Moreover, the newest iteration of China’s national strategy lists innovation, coordination, green development, and sharing as guiding principles.^{2,3,4}

Accordingly, research output in the sciences, particularly within the neurosciences and neurotechnology (i.e., neuroS&T) has increased exponentially within the past decade.⁵ New programs designed to attract both Chinese scientists who have historically left the mainland for better opportunities in the West and researchers from Western universities have reinvigorated a previously small, insular domestic research community. Recent plans to expand laboratory networks, particularly the Institute of Neuroscience (ION) of the Chinese Academy of Sciences (CAS) at Shanghai will also foster a diverse portfolio of research at least through the remainder of the current decade, and very likely beyond. As universities like the East China Normal University and Tsinghua University build and expand upon their neuroscience departments, China will assuredly become and remain a major contributor within the international neuroscience and biotechnology milieu.

China: Strategic Latency via NeuroS&T and Biotechnology

Strategic latency is defined as “the inherent potential for technologies to bring about significant shifts in the military or economic balance of power.”⁶ Given this definition, China’s present and ongoing efforts in (1) harnessing academic potential, (2) encouraging policy that favors greater government agency, and (3) providing loopholes for opportunities wherein intellectual property can be co-opted for national use can be recognized as a prototypic enterprise for effecting strategic latency. The engagement of such enterprise in the neurosciences and biotechnology positions China to establish R&D efforts and outcomes capable of tilting economic, political and military power and influence in brain science and its varied uses away from the United States, and more broadly, the West.

The short-term outcomes and implications are evident: establishment of a diverse, well-funded population of neuroS&T and general biotech talent; a range of research products

1 Dan Harris, “China’s 12th Five-Year Plan. Go With It, Not Against It,” China Law Blog, accessed October 27, 2017, <http://www.chinalawblog.com/2013/03/chinas-12th-five-year-plan-go-with-it-not-against-it.html>.

2 In developing the 13th Five-Year Plan (FYP), the State Council Information Office of the People’s Republic of China has proposed that the new FYP contain, “five development concepts of innovation, coordination, green development, opening up, and sharing, among which innovation is considered the core. Those concepts are the key to resolving the problems that impede China’s economic growth and roadmap towards socio-economic development.”

3 State Council Information Office of the People’s Republic of China, “Innovation-driven development benefits China and the world,” accessed October 27, 2017, <http://www.scio.gov.cn/32618/Document/1472758/1472758.htm>.

4 Owen Haacke, “Understanding China’s 13th Five-Year Plan,” *China Business Review*, accessed October 27, 2017, <http://www.chinabusinessreview.com/understanding-chinas-13th-five-year-plan/>.

5 A. Bala and B.M. Gupta, “Mapping of neuroscience research: a quantitative analysis of publications output of China, 1999–2008,” *Annals of Neurosciences* 17, no. 2 (2010): 63–73, doi:10.5214/ans.0972-7531.1017204.

6 Zachary Davis, Ronald Lehman, and Michael Nacht, *Strategic Latency and World Power: How Technology Is Changing Our Concepts of Security* (Livermore: Lawrence Livermore National Laboratory, 2014), accessed October 27, 2017, https://cgsrc.llnl.gov/content/assets/docs/Strategic_Latency.pdf.

to bring to market and/or develop toward national security agendas; elevated status as a nation that values scientific research, and thus perhaps the ability to drive global research directions; and a fortified S&T capability within the military. The long-term implications for global markets and security will be considerable, with manifest effects upon intellectual property (IP) rights, ethical bases and considerations relative to the conduct and use of scientific research and its outcomes and products, and ever-expanding economic and military capabilities.

From an academic standpoint, China’s efforts in attracting foreign researcher scholars by establishing visiting professorships within the Chinese Academy of Sciences enables Western scientific techniques and technologies to be imported, cultivated, and examined within Chinese research institutions, and creates a nexus for such research techniques, tools, and products to be incorporated and allocated according to national priorities. Indeed, Chinese efforts at streamlining viable research toward the creation of potentially high value commercial products, in concert with its IP policies, have allowed China to “catch up” to the United States’ R&D enterprises in several domains, as depicted in Figures 1–3 and Table 1.

US vs. China: Patent Applications, Residents (1960–2013)

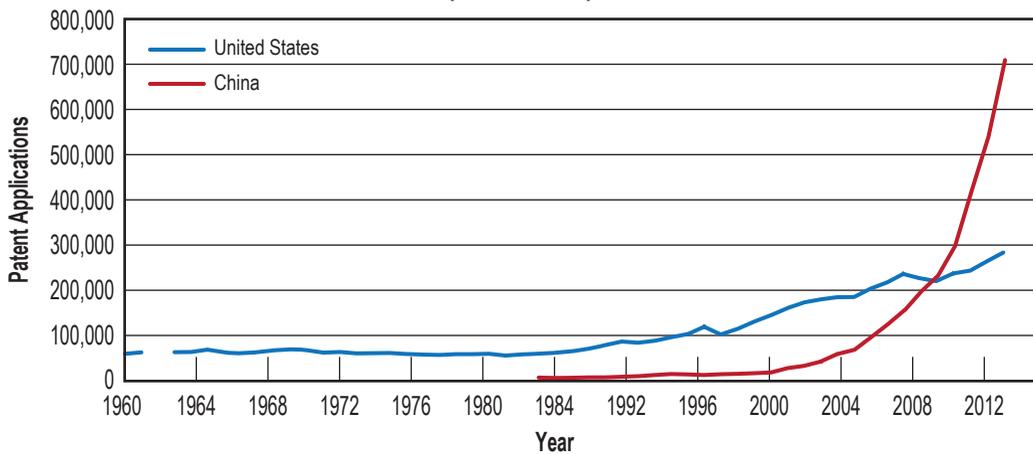


Figure 1: A comparison of the number of patent applicants filed by residents in China and the U.S. Data based on World Bank Open Data “Country Profiles” dataset. The number of patent applications filed by residents has skyrocketed in China, particularly within the past twenty years. In 2009, the number of patent applications filed by residents was 229,096, compared to the 704,936 patents filed in 2013. In 2014, this number was 801,135, far outpacing the rate of filing in the U.S. Residents in the U.S. filed 285,096 patents in 2014.

US vs. China: High-Technology Exports as % of Manufactured Exports (1989–2013)

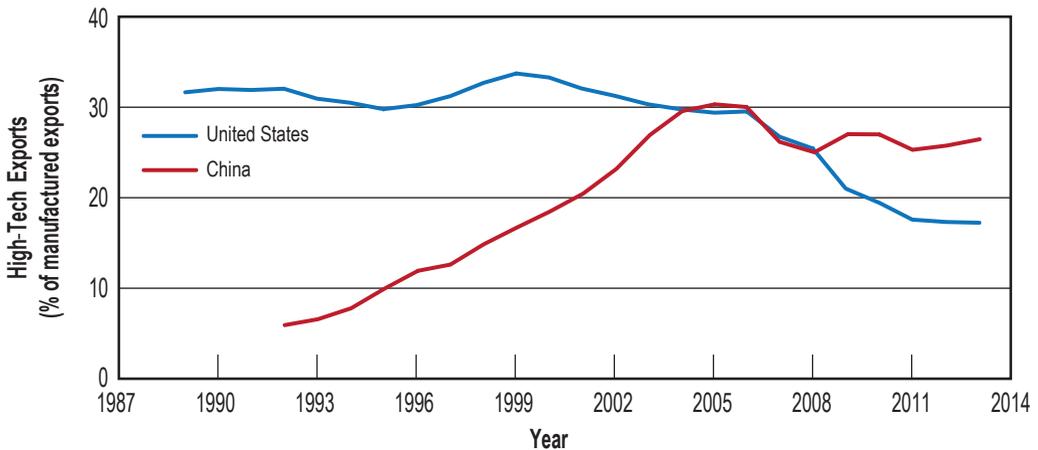


Figure 2: A comparison of high-technology exports as a percentage of total manufactured exports in the U.S. and China between 1989–2013. Data based on World Bank Open Data “Country Profiles” dataset. The number of high-technology exports as a percentage of total manufactured exports has increased dramatically in fewer than 30 years. In 2000, this number was 19.0% in China, and by 2006, it had increased to 30.5%, just eclipsing the U.S. percentage of 30.1%. Though percentages dropped for both countries after 2005, China has maintained its lead in high-tech exports as a percentage of manufactured exports: current high-tech exports comprise 25.4% of China’s manufactured exports, compared to 18.2% of U.S. GDP, a clear indicator of China’s efforts at sustaining an innovation and R&D-based economy.

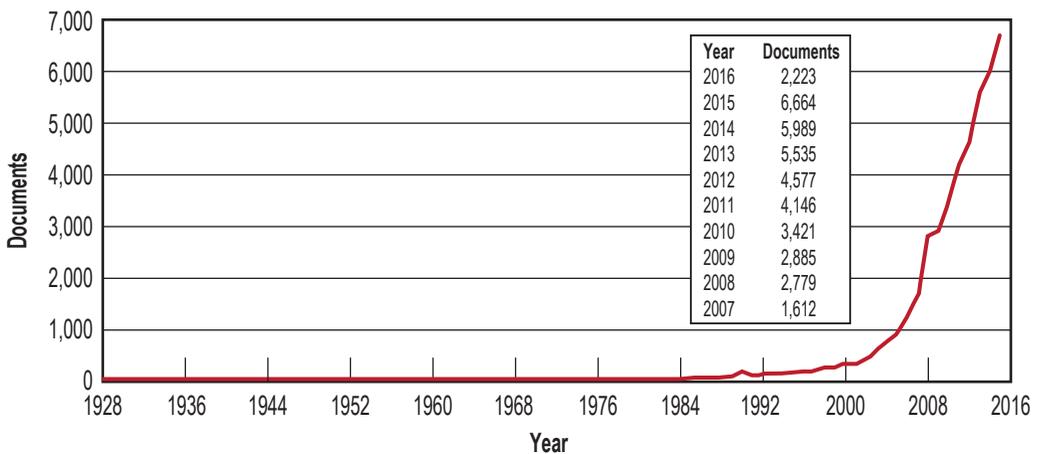


Figure 3: Number of Chinese publications in the neurosciences from the Scopus citation database between 2007–2016. Parameters are based on Bala, A. and Gupta, B.M. (2010) Mapping of neuroscience research: a quantitative analysis of publications output of China, 1999–2008. An exponential increase in neuroscience-related publications is clearly observable.

	US	China
Trademark applications, direct resident (2013) [indicative of invent 1st vs. patent 1st]	270,761	1,733,364
Patent applications, residents (2013)	287,831	704,936
High-Tech Exports, as % of manufactured exports (2013)	17.755765081363%	26.965489517382%
High-Tech Exports, in USD (2013)	148,000,000,000 (148b USD)	560,000,000,000 (560b USD)
R&D Expenditure, as % of GDP (2012, 2013)	2.80604% in 2012	2.01466% in 2013
Scientific and technical articles published (2009, 2011)	208,600.8 in 2009	89,894.4 in 2011
Researchers in R&D	4018.635/1,000,000 people in 2012	1089.192/1,000,000 people in 2013
Charges for use of IP, receipts (2014, 2013)	130,000,000,000 USD in 2014 (130b USD)	887,000,000 in 2013 (887m USD)
Charges for use of IP, payments (2014, 2013)	42,124,000,000 (~42b USD)	21,033,078,371 (~21b USD)

Table 1: U.S and China R&D Efforts.

Of particular note in this regard is China’s Project 863—also referred to as the 863 Program—which is known by the U.S. Office of the National Counterintelligence Executive to provide “funding and guidance for efforts to clandestinely acquire U.S. technology and sensitive economic information.”⁷ Originally established by Deng Xiaoping in March 1986, Project 863 targeted seven industrial sectors, including biotechnology.^{8,9,10} Because government-funded research in the neurosciences (and other sciences) can be directly co-opted for national use, and because many visiting professorships are either within the governing body of the CAS or within state-run universities themselves, the potential for any such research to be combined with Project 863’s portfolio, and other clandestine research efforts, poses definite implications for strategic latency.

Such deepening interests and funding in the neurosciences and biotechnology increases concerns regarding Chinese military applications of these academic and commercial R&D efforts. As a charter member of the United Nations (and thus obligated to adhere to UN

7 Christian Aghroum, “Foreign spies stealing U.S. economic secrets in cyberspace. Report to Congress on foreign economic collection and industrial espionage. 2009-2011,” *Sécurité et stratégie* 8, no. 1 (2012): 78–79.

8 Two recent examples involve those of Huang Kexue, Yu Xue, and Lucy Xi. Huang Kexue leaked trade secrets relating to the manufacture of food products to Project 863 and the National Natural Science Foundation of China between 2008–2009; Yu Xue and Lucy Xi shared trade secrets related to biopharmaceutical drugs and allegedly received funding from the Chinese government to replicate their work by establishing a new Chinese pharmaceutical company.

9 BBC News, “Chinese scientist Huang Kexue jailed for trade theft,” December 22 2011, <http://www.bbc.com/news/business-16297237>.

10 U.S. v. Xue, 16-cr-00022, U.S. District Court, Eastern District of Pennsylvania (Philadelphia) <https://www.justice.gov/usao-edpa/file/814381/download>.

Security Council Resolution 1540),¹¹ and signatory party to the Geneva Conventions, the Biological Toxins and Weapons Convention,¹² and the Chemical Weapons Convention, China is prohibited from production, acquisition, and manufacture of biological and chemical weapons and their precursors.¹³

However, these policies do not prevent China, along with a number of other nations, from exploring both dual-use scientific R&D and direct military innovation. Biotechnology firms operate within an environment that permits copyright infringement and ambiguous protection of IP rights. Such laxity is due to (1) evolving domestic patent law and procedures, (2) purposefully overlapping laws, and (3) highly utilitarian patent application processes. These factors ultimately produce confusion as to which agency makes license determinations and which standards are employed, thus conferring to the Chinese government the ability to incorporate a broad palette of neuroS&T and biotech R&D for dual-use and direct military purposes.

The loopholes in current laws and lack of policy enforcement pivot towards IP misuse, and Chinese governmental involvement in such activities has already strained U.S. and international business relations with China, and several multinational corporations operating in China have cited the apparent lack of IP protection as a primary challenge to continued commercial viability. The U.S. International Trade Commission has identified China as responsible for 80% of all IP thefts from U.S.-headquartered organizations in 2013, leading to a loss of business revenue of approximately \$300 billion.^{14,15} Consequently, the Office of the United States Trade Representative has expressed concern over China's rules, regulations, and policies surrounding innovation and R&D: Chinese policies often require IP rights to be developed in China, and/or IP to be owned by or licensed to a Chinese party (often with exclusivity).¹⁶

However, such governmentally-imposed conditions and incentives may act as a double-edged sword: license distortion and private business arrangements may enable domestic

11 "Resolution 1540 (2004) imposes binding obligations on all States to adopt legislation to prevent the proliferation of nuclear, chemical and biological weapons, and their means of delivery, and establish appropriate domestic controls over related materials to prevent their illicit trafficking. It also encourages enhanced international cooperation on such efforts. The resolution affirms support for the multilateral treaties whose aim is to eliminate or prevent the proliferation of WMDs and the importance for all States to implement them fully; it reiterates that none of the obligations in resolution 1540 (2004) shall conflict with or alter the rights and obligations of States Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, the Chemical Weapons Convention, or the Biological Toxins and Weapons Convention or alter the responsibilities of the IAEA and OPCW."

12 China ratified GC I-IV in 1956 and ratified Protocols I-II in 1983.

13 United Nations 1540 Committee, "United Nations Security Council Resolution 1540 (2004)," accessed June 9, 2016, <http://www.un.org/en/sc/1540/>.

14 Schotter, Andreas, and Mary Teagarden, "Protecting Intellectual Property in China," *MIT Sloan Management Review* 55, no. 4 (2014): 41.

15 Representative, U.S. Trade, "Special 301 Report," April 30, 2010, <http://www.ustr.gov/about-us/press-office/reports-and-publications/2010-3>.

16 United States International Trade Commission, "China: effects of intellectual property infringement and indigenous innovation policies on the U.S. economy," investigation (U.S. International Trade Commission, 2011).

Chinese biotechnology industries and the Chinese government greater access, purview, and control of neuroS&T and overall biotechnology markets and their products, but innovation and market participation may also decline as a result of these conditions. Thus, understanding the ways in which Chinese biotechnology industries can leverage national and international IP and proprietary information protection statuses and laws will become critical to (1) assessing how China can veil and protect dual-use and/or direct military acquisition of neuroS&T and biotechnology research and (2) predicting potential divergences, risks and/or threat(s) that current and near-term future Chinese R&D (and end-use) initiatives may pose.

Understanding and Evaluating Chinese S&T Research and IP Policy

In order to examine the strategic latency potential fostered by Chinese efforts in neuroS&T and bioscience and biotechnology more broadly, it is important to first evaluate extant driving forces in the R&D policy environment. Since 1953, China has communicated top policy priorities through a series of Five-Year Plans (FYPs), which are meant to (1) highlight industry areas deserving of focused government funding and (2) guide all levels of government regulators and officials in policy decisions and actions. The reach of these Five-Year Plans extends beyond that of government bodies: FYPs are written with state-owned and private-sector enterprises in mind, with funding and policy goals steering industry priorities and market growth.

In its past two national Five-Year Plans (FYP), China has highlighted R&D and innovation as key themes defining its economy's transition from one based on a manufacturing model to one based on a growth model of production services. In heralding this transition, the 12th FYP introduced a new set of three key indicators with which to measure nationwide progress. These were: total gross domestic product (GDP) growth; percentage of GDP spent on strategic, emerging industries (explicitly including biotechnology, high-end equipment manufacturing, new materials, and next-generation information technology); number of patents (per person); and total R&D spending.

Most notably, China sought to address and overcome its relative non-competitive standing in international scientific and technological fields and markets by encouraging innovation and the production of emerging technologies. Defined goals toward such ends were: increasing R&D spending from 1.75%–2.2% of total GDP by 2015, and raising the rate of patents per person from 1.7–3.3 patents/10,000 people.^{17,18}

17 The State Council, "12th Five-Year Plan," The People's Republic of China, accessed June 9, 2016, http://kraneshares.com/resources/2013_10_kfyp_fan_gang_white_paper.pdf; <http://www.cbichina.com.cn/cbichina/upload/fckeditor/Full%20Translation%20of%20the%2012th%20Five-Year%20Plan.pdf>; https://www.uscc.gov/sites/default/files/Research/12th-FiveYearPlan_062811.pdf

18 "China's 2015 ratio of R&D expenditure to GDP expected to be 2.1%, missing 2.2% target for 12th Five-Year plan," *People's Daily*, January 12, 2016, accessed June 9, 2016. <http://en.people.cn/n3/2016/0112/c98649-9002610.html>.

US vs. China: R&D Expenditure (1996–2013)

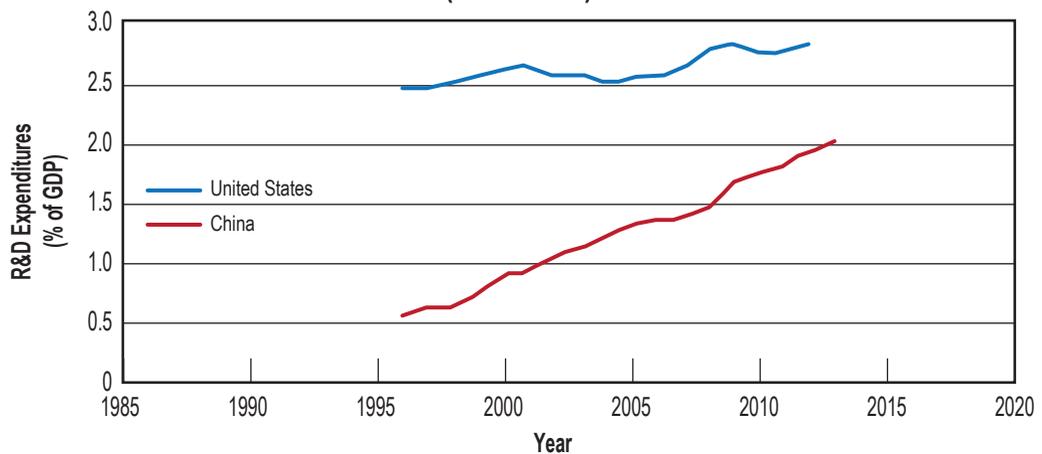


Figure 4: Comparison of U.S. vs. Chinese R&D expenditure between 1996–2013. Data based on World Bank Open Data “Country Profiles” dataset. Chinese R&D expenditure has increased from ~0.5% of GDP to 2% GDP in fewer than 20 years, though is still less than U.S. R&D expenditure, which rested at 2.8% in 2012.¹⁹

Prescriptions for S&T growth defined in and by China’s other policies were similarly expansive. The 12th FYP essentially aimed to align Chinese economic goals with progress within R&D by means of increasing investment and the establishment of an innovation-based economy. The 12th FYP emphasized changes within investment and financial policies that included dedicating funds for the development of strategic industries, focusing development of micro-enterprises to promote scientific innovation, and guiding tax support for such directed investments and use of economic capital within the bioscientific and biotechnology sectors. Policy called for “the establishment of industrial standards” for emerging industries, together with new patent and IP rights that were aimed at encouraging both innovative products and increased market viability and value.²⁰ (See Table 2.)

The 12th FYP aimed to enhance industrial competitiveness through a shift to systems engineering, management of R&D, and the application of a “scientific lens to streamline R&D across sectors, from energy to biotechnology.”²¹ No longer were cheap labor and means of production viewed as viable, long-term economic goals; rather, the 12th FYP envisioned Chinese enterprise that (1) prioritized “becoming a competitive industry in terms of quality and innovation rather than brute mass,” and (2) contributed to

19 Dan Harris, “China’s 12th Five-Year Plan. Go With It, Not Against It,” China Law Blog, accessed October 27, 2017, <http://www.chinalawblog.com/2013/03/chinas-12th-five-year-plan-go-with-it-not-against-it.html>.

20 “The State Council, “12th Five-Year Plan,” The People’s Republic of China, accessed June 9, 2016, https://www.uscc.gov/sites/default/files/Research/12th-FiveYearPlan_062811.pdf; <http://www.cbichina.com.cn/cbichina/upload/fckeditor/Full%20Translation%20of%20the%2012th%20Five-Year%20Plan.pdf>.

21 Ibid.

	U.S.	China
Patent-Granting Institution	United States Patent and Trademark Office (USPTO)	State Intellectual Property Office (SIPO) (adjudicates patent disputes)
Patent Types	Utility patents (20 years): aimed at machines; human made products; compositions of matter; and processing methods. Ornamental design patents (14 years) There are no utility model patents or equivalents protected in U.S. compared to those in China.	Invention patents (20-year term protection) Utility model patents (10-year term protection) Design patents
Subject Matter	Larger scope	Cannot patent: 1). Scientific discoveries; 2). Rules and methods of mental activities; 3). Methods for diagnosis or treatment of diseases; 4). Animal and plant varieties, not including the processes used in producing the products; and 5). Substances obtained by means of nuclear transformation.
Public/Academic Knowledge	U.S.—more well-versed	Chinese inventors and academic researchers—much less versed

Table 2: Breakdown of Patent System Comparison.

the “global trend of scientific and technological progress” as instrumental to gaining “comparative advantage.”²²

Of the seven strategic emerging industries that the 12th FYP highlighted as focal to innovation and development-centered policies, four were directly related to neuroS&T and biotechnology writ-large. These were: biology, next-generation IT, high-end equipment manufacturing, and new materials.^{23,24} Additionally, the 12th FYP noted that approximately 14 trillion RMB (U.S. \$2.16 trillion) would be spent across a 60 calendar-month initiative to grow these industries to advance China’s standing and influence the value chain of international S&T production and output.

²² Ibid.

²³ The seven strategic emerging industry areas were identified as biotechnology, clean energy, next-gen IT, high-end equipment manufacturing, alternative energy, new materials, and clean energy vehicles.

²⁴ “The State Council, “12th Five-Year Plan,” The People’s Republic of China, English translation, <http://www.britishchamber.cn/content/chinas-twelfth-five-year-plan-2011-2015-full-english-version>

The most recent Five-Year Plan, the 13th FYP, further hones China's focus on R&D, entrepreneurship, and innovation as key themes through which to attain its economic goals. President Xi Jinping's proposal explicates the decision to move from the management of R&D to the creation and strengthening of Chinese "innovation services," which include biomedicine and smart manufacturing, and emphasize research to produce "subversive technological breakthroughs"—the first time that this phrase has been used in formal, governmental discourse.²⁵ Recognizing prior over-reliance on exports and fiscal investment for GDP growth, the 13th FYP aims to re-orient China's future development on innovation through a series of policy goals, including: (1) restructuring systems supporting R&D; (2) allowing universities and research institutions greater freedom in the distribution and utilization of funds; (3) setting up innovation enterprises, innovation cities, and regional innovation centers; and (4) establishing an "Industrial Technology Innovation Alliance" to facilitate innovation across sectors and regions, among other goals.²⁶

The aims of the FYPs are supported by other national policies. The Chinese State Council's "Made in China 2025" roadmap recognizes the need for a continued push in independent innovations in specific mega-project areas, including drug innovation and development, genetically modified organisms, and high-end chip design and software—each of which is a major component within neuroS&T (and other biotechnology fields).^{27,28} China's Mid- to Long-Term Plans (MLP) also reiterate the goals of the FYP, and yoke them to overcoming current challenges in IP claims and rights.²⁹

The funding mechanisms and governing bodies that support China's economic goals also tie academic and research institutions to government policies. Consequently, researchers within China's academic sector often participate in a bi-directional relationship with policy makers. The Ministry of Science and Technology (MOST), CAS, and the National Science Foundation of China (NSFC) each have specific roles, but all act to distribute funds from the National High-Tech Research and Development Program and the Key Basic Research Program to individual scientists and institutions throughout China, thus shaping the tenor and foci of academic research in accordance with the extant FYP and current S&T (and political, economic, and military) policies. Individually, the MOST and the CAS have played

25 APCO Worldwide, "The 13th Five-Year Plan: Xi Jinping Reiterates his Vision for China," 2015, accessed October 27, 2017, <http://www.apcoworldwide.com/docs/default-source/default-document-library/Thought-Leadership/13-five-year-plan-think-piece.pdf?sfvrsn=2>.

26 Frank Lyn and David Wu, "Prosperity for the masses by 2020," *PwC*, accessed July 9, 2016, <https://www.pwccn.com/en/about-us/prosperity-for-the-masses-by-2020.html>.

27 Xin En Lee, "Made in China 2025: A New Era for China Manufacturing," CKGSB Knowledge, 2015, accessed October 17, 2017, <http://knowledge.ckgsb.edu.cn/2015/09/02/technology/made-in-china-2025-a-new-era-for-chinese-manufacturing/>.

28 Guo Fa, "State Council issued the 'Made in China 2025' notice," State Council, 2015, accessed October 27, 2017, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

29 Richard P. Suttmeier and Xiangkui Yao, "China's IP Transition: Rethinking Intellectual Property Rights in a Rising China," NBR Special Report 7 (2011), last accessed October 27, 2017, http://china-us.uoregon.edu/pdf/IP_report.pdf.

overarching, supervisory roles in directing and funding scientific and technical activity—as well as military research—for the Chinese government.³⁰

Working in concert with MOST, the CAS acts to (1) promote S&T research to the potential benefit of those sectors identified to maximize national economic and political standing; (2) amalgamate academic and research institutions in a functional network to maximize collaboration; and (3) provide scientific advice to the government. The National Science Foundation of China (NSFC) serves as a multi-disciplinary research council to co-steer these efforts.³¹

The relationship between high-level government officials and academicians extends beyond funding initiatives. Endeavors such as the Hundred Person Program, Thousand Talents Program, Spring Light Program, Youth Thousand Talents Program, Recruitment Program of Foreign Experts, and the Friendship Award have been established to enable incubation of domestic talent, re-attract Chinese scientists who may have left the country in search of international opportunities, and attract foreign researchers to work in China, respectively.^{32,33,34,35} Notably, the Organization Department of the Communist Party of China Central Committee (once headed by current Vice President Li Yuanchao) organizes the South China Global Talent Institute, a think tank in Guangzhou, China which launched the “Thousand Talents Program” in 2008—one of the main venues through which China is able to attract Western researchers.³⁶ The CAS has organized affiliated professorships with researchers from a number of international universities, including the Massachusetts Institute of Technology (MIT), Stanford University, and Harvard University in the U.S., and the University of Würzburg in Germany. Reflective of the close tie between the governmental and academic arms of R&D in China, President Xi Jinping’s visit to the CAS in July of 2013 was influential to initiating the CAS’s Pioneer Initiative, which features the Hundred Talents Program as one of its several efforts in (explicitly) recruiting international S&T talent.

As an effort to nurture an environment that attracts rather than loses talent, these programs—along with the spectrum of CAS’s recruitment initiatives—are intended to

30 Robert Ash, Robin Porter, and Tim Summers, *China, the EU and China’s Twelfth Five-Year Programme* (London: Europe China Research and Advice Network, 2012), accessed October 27, 2017, <https://www.chathamhouse.org/publications/papers/view/182630>.

31 Ibid.

32 The Recruitment Program for Innovative Talents, accessed October 27, 2017, <http://www.1000plan.org/en/>.

33 Case, Steve. “As Congress Dawdles, the World Steals Our Talent.” *The Wall Street Journal*. Last modified Sept. 9, 2013. <http://www.wsj.com/articles/SB10001424127887324577304579054824075952330> [Last accessed October 27, 2017](#).

34 “100 Talents Program of Chinese Academy of Sciences.” Chinese Academy of Sciences. Last modified 2014. http://sourcedb.cas.cn/sourcedb_rcees_cas/yw/tp/. [Last accessed October 27, 2017](#).

35 Huiyao Wang, “Chinese Returnees: Impact on China’s Modernization & Globalization,” presentation to Brookings Institute, Washington DC, April 6 (2010), https://www.brookings.edu/wp-content/uploads/2012/04/20100406_china_returnees_huiyao.pdf

36 Sean Sanders, “Science in the Chinese Academy of Sciences,” ed. Chinese Academy of Sciences (The American Association for the Advancement of Science, 2012), accessed October 27, 2017, https://www.sciencemag.org/site/products/CAS_FINAL_Online_version_30aug12.pdf.

enhance China's competitiveness in innovation, academic contributions in the sciences, and status as an S&T manufacturing power that successfully transitions its economy into one rooted in innovation services. The Hundred Person Program, for example, was CAS's first effort in recruiting promising and leading scientists, engineers, and technicians from around the world.³⁷ Similarly, the Spring Light Program was designed to entice the return of Chinese scientists who had left to work overseas.³⁸ The Thousand Talents Program is perhaps China's broadest and most ambitious recruitment effort; its sub-program, the Recruitment Program for Innovative Talents, offers short- and long-term opportunities for candidates who may be entrepreneurs, young professionals, foreign experts, and "topnotch [sic] talents and teams."³⁹

Such programs and ongoing support through strategic funding directives have increased the development of domestic S&T research talent and enabled acquisition of international expertise. Exemplary of this trend, the Institute of Neuroscience (ION) was founded in 1999, a time when its parent organization, the CAS, began to play a growing role in funding and directing Chinese S&T research. The first Chinese papers on neuroscience to be published in major international journals (e.g., *Cell*; *Science*; *Neuron*; *Nature Neuroscience*, and *Nature Cell Biology*) were authored by Chinese scientists at ION.

According to ION Director Mu-Ming Poo, ION has produced "more than half of all top-level neuroscience publications from Chinese institutions and [its] membership has quadrupled from 1500 to 6000 scientists within the past decade."^{40,41} In 2009, the CAS approved a ten-year expansion plan to grow ION into a network of 50 laboratories, allocating funding to support 50% of ION's budget—an increase from the previous 30% funding, and naming Mu-Ming Poo's "neural basis of intelligence" project as the recipient of one of China's largest and most competitive basic science grants.⁴²

Chinese universities have also been the beneficiaries of increased governmental investment in neuroS&T over the past decade. In 2008, Shanghai's East China Normal University established an Institute of Cognitive Neuroscience with Chinese scientists who had returned

37 "Global Recruitment of Pioneer 'Hundred Talents Program' of CAS," Chinese Academy of Sciences, accessed October 27, 2017, http://english.cas.cn/join_us/jobs/201512/t20151204_157107.html.

38 Ministry of Science and Technology of China, "Hundred Talents Program of Chinese Academy of Science—Young Talents," accessed October 17, 2017, <http://employment.ustc.edu.cn/cn/enindexnews.aspx?infold=665597895156250032>.

39 "The Recruitment Program for Innovative Talents (Long Term)." Recruitment Program of Global Experts, 1000 Plan, accessed October 17, 2017, <http://www.1000plan.org/en/>.

40 David Cyranoski, "Neuroscience in China: Growth Factor," *Nature* 476 (2011): 22–24, <http://www.nature.com/news/2011/110803/full/476022a.html>.

41 David Cyranoski, "What China's latest five-year plan means for science," *Nature* 531 (2016): 524–525, accessed October 17, 2017, <http://www.nature.com/news/what-china-s-latest-five-year-plan-means-for-science-1.19590>.

42 David Cyranoski, "Neuroscience in China: Growth Factor," *Nature* 476 (2011): 22–24, accessed October 17, 2017, <http://www.nature.com/news/2011/110803/full/476022a.html>.

from working in the United States. Three years later, Patrick McGovern—one of the major donors to MIT’s McGovern Institute for Brain Research—agreed to donate \$10 million to establish a sister institute at Beijing’s Tsinghua University.⁴³ In 2013, Hangzhou’s Zhejiang University received a \$25 million grant to build an Interdisciplinary Institute of Neuroscience and Technology, one of the largest investments that any university in China set aside towards a single project.⁴⁴

Universities producing top research receive additional governmental funding through Project 211—an initiative of the Ministry of Education that distributed \$2.2 billion to more than 100 schools between 1996 and 2000—and Project 985, which sponsors 39 of China’s top research universities.⁴⁵ The current 13th FYP will increase S&T spending to 9.1%, the equivalent of U.S. \$41 billion.⁴⁶ (See Table 3.)

Despite such growth, the Chinese research environment is not immune to setbacks and tensions. Opportunities for career advancement are not always available, and graduate students often do not have the chance to conduct their own research. Success is measured in the quantity of articles published, rather than quality, with principal-investigator positions bestowed upon those scientists with the greatest number of publications. Emphasis on quantity of publications can stifle innovation by encouraging the forfeiture of actual scientific progress for the sake of more publications. Institutes also compete for researchers: 50% of the researchers currently at ION have been in residence for fewer than five years, and ION has reportedly lost senior staff to the National Institute of Biological Sciences.⁴⁷

Nevertheless, China has undeniably made significant strides in neuroS&T R&D. China’s Weighted Fractional Count (WFC)—a measure of its contribution to the *Nature* journals—increased by 37% between 2012 and 2014, and by 2014, China possessed the second highest WFC, with 8,641 articles, exceeded only by the U.S., with an article count of 26,638.^{48,49} To date, ION scientists have made major discoveries in pain regulatory systems,

43 Ibid.

44 Sarah O’Meara, Sarah, “At the very heart of progress,” *Nature* 528 (2015): S179–S181, http://www.nature.com/nature/journal/v528/n7582_supp_ni/full/528S179a.html.

45 “Are You Partnering With Chinese 211 and 985 Universities?” International Education Advantage, <http://services.intead.com/blog/are-you-partnering-with-chinese-211-and-985-universities>

46 David Cyranoski, “What China’s latest five-year plan means for science,” *Nature* 531 (2016): 524–525, accessed October 17, 2017, <http://www.nature.com/news/what-china-s-latest-five-year-plan-means-for-science-1.19590>.

47 David Cyranoski, “Neuroscience in China: Growth Factor,” *Nature* 476 (2011): 22–24, accessed October 17, 2017, <http://www.nature.com/news/2011/110803/full/476022a.html>.

48 Sarah O’Meara, Sarah, “At the very heart of progress,” *Nature* 528 (2015): S179–S181, http://www.nature.com/nature/journal/v528/n7582_supp_ni/full/528S179a.html.

49 Ibid.

Research Institute	Research Portfolio
Beijing Normal University	<ul style="list-style-type: none"> • Molecular chaperones regulatory mechanism on protein for Alzheimer’s dementia; the characteristics of ARPP-90 which is phosphorylated by specificity; molecular mechanism of sAPPalpha’s neurons protection. • Metabolic regulation and homeostasis of nuclear receptor mediating; nuclear receptor’s drug screening and drug mechanism; foreign substance’s influence on animal development and its molecular modulation mechanism. • Stem cells and tumor cell biology, virology, and gene therapy. • The chemical and neurobiological mechanisms of mammals’ olfactory communications. • Neural degenerative diseases. • Modulation of neuronal function by the natural triterpenoid toosendanin. • Source: http://lifescience.english.bnu.edu.cn/facultyresearch/fulltimefaculty/index.htm
Peking University	<ul style="list-style-type: none"> • The first IVF baby born following MALBAC-based whole genome screening. • Source: http://english.pku.edu.cn/news_events/news/research/2031.htm • Mechanisms and management of small vessel dysfunction in neurological diseases. • Source: http://english.bjmu.edu.cn/research/key_laboratories/44260.htm • Relationships between sleep disorder and depression/anxiety, including the relationships of the neuroendocrine stress response and cytokine induction of sleep in animal models. • Source: http://english.bjmu.edu.cn/research/phd_supervisors/basicmedalscience/46234.htm • Behavioral sensitization, depression, anxiety, and aggressive behavior in addictive animals and drug abusers. • Source: http://english.bjmu.edu.cn/research/phd_supervisors/basicmedalscience/46235.htm
Institute of Neuroscience	<ul style="list-style-type: none"> • Neurotransmitters (such as glutamate and GABA (-aminobutyric acid)), how neuronal properties are specified during development, etc. • Source: http://www.ion.ac.cn/laboratories/int.asp?id=69 • Embryonic origin of adult retinal stem cells, timing control, of neurogenesis, and functional analysis of neural circuit development. • Source: http://www.ion.ac.cn/laboratories/int.asp?id=91 • Cortex development and evolution, axon growth and guidance, and synapse differentiation and pruning. • Source: http://www.ion.ac.cn/laboratories/int.asp?id=41 • Mu-Ming Poo, PhD—ongoing projects: plasticity of neural circuits, synaptic structural mechanism for storing long-term memory, and neural circuit basis of higher cognitive functions in primates. • Source: http://www.ion.ac.cn/laboratories/int.asp?id=42
National Institute of Biological Sciences	<ul style="list-style-type: none"> • Serotonin in pre-implantation mouse embryos is localized to the mitochondria and can modulate mitochondrial potential. • Source: http://www.ncbi.nlm.nih.gov/pubmed/18304982 • Activation, internalization, and recycling of the serotonin 2A receptor by dopamine. • Source: http://www.ncbi.nlm.nih.gov/pubmed/17005723 • Encoding of fear generalization at the level of single neurons of the amygdala, delayed impact of a single episode of stress: implication for PTSD, cellular, and behavioral correlates of antidepressant action in the amygdala. • Source: https://www.ncbs.res.in/faculty/shona-research

Table 3: Brief overview of portfolios of major research institutions with neuroscience departments.

brain plasticity, and the mechanisms of a number of neurodegenerative diseases.^{50,51} To be sure, as publication data previously depicted in Figures 1 and 2 reveal, China has established a strong and growing presence in S&T, inclusive of neuroS&T (see Figure 3).

Engaging Opportunities for Dual and Direct Military Use

China's emphasis on neuroS&T and biotechnology R&D affords considerable potential for products to be utilized in dual- and/or direct-use applications for military initiatives. Government funding can “nudge” or more explicitly mandate R&D directions toward fulfilling needs and opportunities relevant to military and intelligence agendas. As well, Chinese military medical centers have laboratories specifically devoted to neuroS&T. For example, Southern Medical University (the former First Military Medical University) in Guangzhou has an Institute of Neuromedicine, housed within Zhujiang Hospital, and the Third Military Medical University in Chongqing features programs in Biotechnology, Pharmacy, and Biomedical Engineering—all of which are integral components of neuroscientific programs of R&D.^{52,53,54}

Of all Chinese military medical university centers, the Fourth Military Medical University in Xi'an appears to possess the most expansive research portfolio in neuroS&T: its Department of Neurobiology, founded in 1985, focuses research in central nervous system repair, brain mechanisms, and function in military stress; neural coding of pain; neuro-immunological modulation; and development of novel approaches to therapeutics for neurodegenerative diseases.⁵⁵ As well, the unit has established publication vehicles for both national and international dissemination of its R&D—the *Chinese Journal of Neuroanatomy* and the *Chinese Journal of Neurosurgical Disease Research*, which enable constituent researchers to accrue requisite publications, while also developing a presence within international indices of scientific standing.^{56,57}

50 See appendix for additional examples of S&T breakthroughs and new R&D milestones.

51 Michael Gross, “Boom time for neuroscience in China,” *Current Biology* 21, no. 12 (2011): R441–R444, accessed October 17, 2017, [http://www.cell.com/current-biology/fulltext/S0960-9822\(11\)00646-4](http://www.cell.com/current-biology/fulltext/S0960-9822(11)00646-4).

52 Southern Medical University, Centers and Institutes, http://portal.smu.edu.cn/en/Research/Centers_And_Institutes.htm

53 “The 10th Biennial Conference of the Chinese Neuroscience Society,” Chinese Neuroscience Society, last accessed October 17, 2017, <http://www.csn.org.cn/2013/en/organizers.asp>.

54 Haisheng Li et al, “The progress of Chinese burn medicine from the Third Military Medical University—in memory of its pioneer, Professor Li Ao,” *Burns Trauma* 5, no. 16 (2017), doi: 10.1186/s41038-017-0082-z.

55 “Institute of Neurosciences,” The Fourth Military Medical University, last accessed October 17, 2017, <http://en.fmmu.edu.cn/info/2488/23832.htm>.

56 *Chinese Journal of Neuroanatomy*, The Fourth Military Medical University, last accessed October 17, 2017, <http://en.fmmu.edu.cn/info/2494/23783.htm>.

57 *Chinese Journal of Neurosurgical Disease Research*, The Fourth Military Medical University, last accessed October 17, 2017, <http://en.fmmu.edu.cn/info/2494/23791.htm>.

Perhaps the most overt move to engage academic researchers in national security and dual-use initiatives has been the 2016 launch of a new Chinese S&T research agency, *junweikejiwei*, intended to undertake and achieve the high-risk, high-reward R&D model upon which DARPA credits its success. This agency directly links the CAS with China's Ministry of Defense. The agency will be headed by and take directives from Liu Guozhi,⁵⁸ an applied physicist and academician from the CAS, with a history of past projects with Mu-Ming Poo of ION and current Chinese vice president Li Yuanchao.^{59,60}

Leveraging Policy and Law to Veil and Protect Dual and/or Direct Use R&D

From a legal standpoint, three main components drive China's ability to sidestep, utilize, and leverage policy toward incorporating neuroS&T and other biotechnology R&D in dual-and/or direct-use applications: (1) the patent system and application process, (2) loopholes and terminology in Chinese patent law and intellectual property rights, and (3) enforcement of patent law and intellectual property rights (IPR).

Biases in the legal and patent systems facilitate a lack of uniformity and clarity, which allows greater ease in veiling and protecting dual/direct use of neuroS&T and other biotechnological R&D. Of particular importance is China's utility model system, which creates a "patent thicket."⁶¹ In this system, patents are no longer solely intended and explicitly employed to ensure the protection of innovative technologies and encourage further innovation. Instead, the "patent thicket" ecosystem brought about by the utility model system emphasizes patenting as an end unto itself rather than as a protective measure for innovative activity. Thus, the relative financial and legal ease with which utility model patents can be filed has produced a flood of patents that are often based on partially or wholly copied concepts (e.g., "fast following") and/or older patents.

One pattern that has emerged is that of domestic patent filers applying for approval on leaked and/or stolen foreign patent applications and information. According to a Beijing-based attorney at the international law firm Orrick, Herrington & Sutcliffe, one can "literally copy patents from any country and have them filed and granted in China as a utility model patent."⁶² This can result in spillover effects, wherein domestic U.S. industries can

58 Lio Guozhi is also a former Commander of Malan nuclear test base and served as Deputy Director of the presently-dissolved People's Liberation Army General Armaments Department.

59 Hao Xin, "China to create its own DARPA," *Science Mag*, March 11, 2016, <http://www.sciencemag.org/news/2016/03/china-create-its-own-darpa>.

60 Ibid.

61 National Bureau of Asian Research, "The Report of the Commission on the Theft of American Intellectual Property," *The IP Commission Report*, May 2013, last accessed October 17, 2017, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

62 Pritchard, Julian Evans and Mark, Annie, "Innovate, Litigate, or Tax Rebate?" *Caixin Online*, September 11, 2012. <https://www.caixinglobal.com/2012-09-11/101015225.html>

litigate against foreign patent holders if the latter attempt to enter the Chinese market.⁶³ Consequently, Chinese companies—particularly those with governmental ties—are able to leverage the patent thicket, incorporate R&D from a variety of foreign sources, and pursue neuroS&T and biotechnological R&D for a multitude of capabilities under the guise of commercial enterprise.

Of note is that Article 26.3 of the Chinese Patent Law allows parties to invalidate chemical patents filed before 2006. The retroactive invalidation enables new investors and parties to copy, manipulate, and reproduce IP, inventions, and utility models from previous (i.e., pre-2006) patents. This contributes to the growing patent thicket, and provides a new source from which Chinese companies, particularly those with governmental support, can develop and expand dual and/or direct-use neuroS&T and biotechnological R&D within a protected commercial space.

Additionally, the Chinese Patent Law contains provisions that enable the government to intervene and co-opt inventions and products within a set of circumstances vis-à-vis compulsory licensing. Namely, Article 48 states:⁶⁴

Under any of the following circumstances, the patent administration department under the State Council may, upon application made by any unit or individual that possesses the conditions for exploitation, grant a compulsory license for exploitation of an invention patent or utility model patent:

(1) When it has been three years since the date the patent right is granted and four years since the date the patent application is submitted, the patentee, without legitimate reasons, fails to have the patent exploited or fully exploited; or

(2) The patentee's exercise of the patent right is in accordance with law, confirmed as monopoly and its negative impact on competition needs to be eliminated or reduced.

Chinese patent law also allows for compulsory licensing under somewhat vaguely defined conditions, including “for the benefit of public health,” in “public interests,” and in scenarios wherein the IP in question presents “a major technological advancement,” or is of “remarkable economic significance.”⁶⁵ This lack of clarity creates opportunities for such

63 U.S. Chamber of Commerce—Asia, “China’s Utility Model Patent System: Innovation Driver or Deterrent,” by Moga, T. T., (Washington, D.C.: U.S. Chamber of Commerce, November 2012).

64 “Patent Law of the People’s Republic of China,” *State Intellectual Property Office of the P.R.C.* (2008), last accessed October 17, 2017, http://english.sipo.gov.cn/laws/lawsregulations/201101/t20110119_566244.html.

65 *Ibid.*

property, including technology that possesses dual/direct-use, to be easily obtained by the government for production and application(s) to meet any needs as defined. Because Chinese patent law does not mention the governing agency that would be responsible for evaluating the aforementioned conditions, abuse of compulsory licensing can serve as a means by which the government can manipulate commercial enterprise and direct and expand the dual/direct-use portfolio of neuroS&T (and biosciences and technologies, more broadly).

Moreover, conflicting terminology within Chinese patent law makes it difficult for patent applicants to reasonably apply for and maintain ownership of IP in China. Article 20 of Chinese patent law requires (1) applicants seeking to file foreign patents to first file for a patent within China, and (2) a confidentiality examination if applicants seek to file a foreign patent for an invention or utility model “accomplished in China.” As a result, the work of multinational companies must comply with Chinese patent parameters before patents can be applied for and/or filed in foreign countries. This brings into question the definition of “made in China,” and also forces foreign/multinational applicants to file for patents in China, thereby providing fodder from which Chinese domestic commercial enterprises—and potentially those with government ties—are free and open to copy and incorporate.

It should also be noted that academicians and researchers producing work with government funding and within universities possess limited rights over their research. Ideally, and as consistent with standards of responsible conduct of research, the university owns IP rights, regardless of whether the work was funded by the government (unless otherwise specified by government contract). According to China’s National Commission of Science and Technology 1994 regulation *Measures for Intellectual Property Rights Made Under the Governmental Funding of the National High Technology Program*, universities retain the option to keep results as trade secrets and may use, assign, and exclusively license such IP. In 2002, the Chinese Ministry of Science and Technology and the Ministry of Finance amended this regulation and transferred greater agency to the government.

Their jointly issued *Measures for Intellectual Property Made Under Government Funding* specified that the funding government agency may “decide, for compelling reasons (such as the security of the state, other vital interests of the state, or vital interest of the public), that title to the IP should be vested in the government.”⁶⁶ Additionally, “the government retains a non-exclusive, royalty-free license to practice inventions made under government funding.”⁶⁷ These amended policies doubly benefit Chinese R&D initiatives: because many funding and research opportunities rely on government funds, China is now able to attract diverse international talent in neuroS&T (and other sciences) and also incorporate much of what

66 Guo H., “IP Management at Chinese Universities.” *Intellectual Property Management in Health and Agricultural Innovation: A Handbook of Best Practices*, eds. A. Krattiger et al. (MIHR: Oxford, U.K., and PIPRA: Davis, U.S.A. 2007), last accessed October 17, 2017, available online at www.ipHandbook.org.

67 Ibid.

is produced in the academic sector toward national security, defense, and other politically and/or economically priority use(s).

Poor enforcement contributes to situations in which patent applicants and holders are often deterred from filing expensive lawsuits, and are forced to operate within a system that is relatively permissive of abuse and theft—providing such actions benefit defined governmental aims and initiatives. China’s patent law, the *Law on Promoting the Transformation of Scientific and Technological Achievements*, and contract laws are all applicable to reward and remuneration in patent cases, and yet each uses conflicting terms and overlaps the others in jurisdiction, thereby creating loopholes, confusion, and a general lack of uniformity in establishing and enforcing legal statute(s).

In the case of remuneration, Article 78 of China’s patent law directly conflicts with Article 29 of *The Law on Promoting the Transformation of Scientific and Technological Achievements*.^{68,69,70} When seeking injunction, Chinese patent law Article 66 states that if parties can “prove that another person is committing or is about to commit a patent infringement, which, unless being checked in time, may cause irreparable harm to his lawful rights and interests, he may, before taking legal action, file an application to request that the people’s court order to have such act ceased.” Courts are restricted to using government or court-sanctioned experts, who often lack background or familiarity with the technology or property disputed, thus further preventing sound decisions on the issue of the vaguely defined condition “irreparable harm.”

Conclusion

As innovation becomes increasingly vital to Chinese economic growth, attention must be paid to the ways that such innovation, particularly innovation within the neuroS&T and

68 Article 78 of patent law states: Where an entity to which a patent right is granted fails to conclude with the inventor or creator an agreement on, and fails to provide in its bylaws formulated in accordance with law, the manner and amount of the rewards referred to in Article 16 of the Patent Law, it shall, after the patent for invention-creation is exploited within the duration of the patent right, draw each year from the profits from exploitation of the patent for the invention or utility model a percentage of not less than 2%, or from the profits from exploitation of the patent for the design a percentage of not less than 0.2%, and award it to the inventor or creator as remuneration. The entity may, as an alternative, by making reference to the said percentage, award a lump sum of money to the inventor or creator as remuneration once and for all. Where an entity to which a patent right is granted authorizes any other entity or individual to exploit its patent, it shall draw from the exploitation fee it receives a percentage of not less than 10% and award it to the inventor or creator as remuneration.

Article 29 of the *Law on Promoting the Transformation of Scientific and Technological Achievements* states: When transferring a scientific or technological achievement made by employees while holding positions in a unit, the unit shall take not less than 20 percent of the net income, obtained from transfer of the achievement, to award persons who made important contributions to the scientific or technological achievement or to its transformation.

69 “Law of the People’s Republic of China on Promoting the Transformation of Scientific and Technological Achievements,” The National People’s Congress of the People’s Republic of China, last accessed June 9, 2016, http://www.npc.gov.cn/englishnpc/Law/2007-12/11/content_1383582.htm.

70 “Patent Law of the People’s Republic of China.” State Intellectual Property Office of the P.R.C. (2008), last accessed October 17, 2017, http://english.sipo.gov.cn/laws/lawsregulations/201101/t20110119_566244.html.

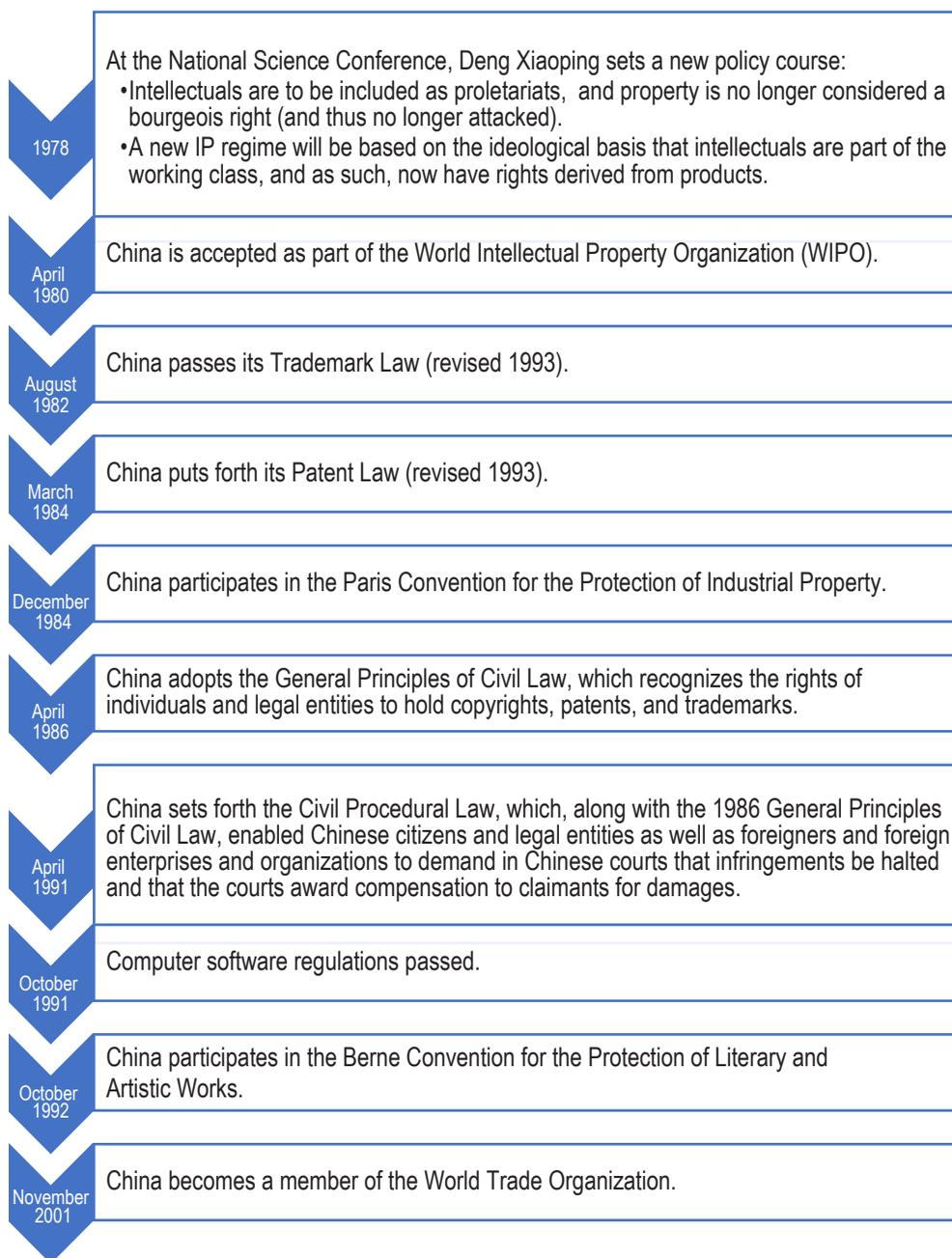
biotechnological industries, can be seeded and leveraged for dual- and/or direct-use, and to effect (multi-focal) strategic latency on the global stage. The current Chinese patent system, patent law and policies, and enforcement mechanisms foster an environment that is plagued with IP exploitation, which further enables Chinese commercial enterprise—in conjunction with governmental initiatives—to explore, exploit, and protect domestic IP and products in ways that are consistent with and supportive of national priorities, goals and agendas.

The policies that China’s institutions are putting forward are substantially improving its scientific and military capabilities. Thus, it is becoming increasingly plausible—and likely—that the conditions necessary for developing unique weapons or other militarized, regulated substances will be met.

Ultimately, the current Chinese posture, as a fast-follower through concerted efforts in S&T within the academic and commercial with government support, evokes security concerns about both exploitation of dual- and direct-use R&D and leveraging of neuroS&T (and other biosciences and technologies) to exercise economic leverage and power in global markets. By attracting foreign researchers, co-opting foreign IP, engaging a sprawling “patent thicket,” and capitalizing upon its domestic market, China has become well positioned to exert considerable latent potential for future exploitation.

As China continues to advance present and latent investment in a variety of R&D sectors under the veiling of IP rights and commercial proprietary interests, it will be ever more important to remain aware of the focus and scope of Chinese S&T interests, as well as the growing tacit knowledge and capabilities fostered by current and future gaps and voids in policy, which can fortify strategically latent influence in international healthcare, economic, and military domains.

Appendix: Timeline: Progression of Chinese Intellectual Property and Patent Policy^{71,72}



71 Michel Oksenberg, Pitman B. Potter, and William B. Abnett, *Advancing Intellectual Property Rights: Information Technologies and the Course of Economic Development in China*, National Bureau of Asian Research, 1996, last accessed October 17, 2017, <http://www.nbr.org/publications/issue.aspx?id=89>.

72 P. Yu, "The sweet and sour story of Chinese intellectual property rights," 2004, retrieved July 18 2011, last accessed October 17, 2017, <http://www.peteryu.com/sweetsour.pdf>.

Chapter 2

“Sputnik-like” Events: Responding to Technological Surprise

Ron Lehman

Sputnik in a Nutshell

National security costs imposed by technological surprise can be immense. Take the case of “Sputnik I,” the first man-made satellite. Launched by the Soviet Union on October 4, 1957, Sputnik—primarily a technology demonstration—humiliated a superpower, catalyzed mankind’s greatest national-security technology competition, encouraged risky geostrategic behavior, and transformed the world in ways that still shape our future.

Few technological surprises match the impact of Sputnik, and like Sputnik, few are totally unexpected. Their consequences, however, are often not those anticipated. Exploiting lessons learned from the “Sputnik Crisis” to plan and prepare for future technological surprise can reduce danger, mitigate damage, and even promote technological progress and strategic gains.¹ Relearning these lessons is urgent, given current international dynamics involving Russia, China, Iran, North Korea and others.

Sputnik is an existence proof that revolutionary strategic consequences can result from catalytic events. Sputnik shocked the world because an uneven response made the U.S. appear ineffectual when confronted with a rising Soviet Union. Awkward attempts to mitigate the damaging effects of Sputnik—denigrating the Soviet accomplishment after welcoming it and then failing to match it—only reinforced the view that the U.S. was outclassed. As public fear of the military implications of Sputnik grew, invoking the specter of “Massive Retaliation” to suggest that no technological advance by any adversary

¹ The most detailed of several recent histories of the “Sputnik Crisis” is Yanek Mieczkowski, *Eisenhower’s Sputnik Moment: The Race for Space and World Prestige* (Ithaca: Cornell University Press, 2013). See below the *Appendix: Readings on the History of Sputnik* for other interesting accounts and perspectives.

could ever be significant enough to alter the military balance only made the U.S. look uncompetitive and perhaps even desperately at risk.

Subsequent U.S. successes, including some coinciding with Soviet failures, were unable to quickly undo the image of Soviet superiority built up at the beginning of the “space race.” Moscow sustained its public affairs momentum by continuing to exploit Sputnik-style spectacles, often preempting planned U.S. events or “bookending” U.S. milestones with immediate, newsworthy launches of its own.

As the superiority of the longer-term U.S. space program became apparent to the technologically savvy, the U.S. still found itself behind the public-opinion power curve. However, twelve years later, the momentum shifted decisively when the U.S. manned lunar landings on the moon contrasted so vividly with the numerous failures in the troubled Soviet unmanned lunar robot program.

The steps necessary to undo the damage caused by the original Sputnik Crisis were costly. They were also insufficient to discourage dangerous adventures by the U.S.S.R. in Berlin, Cuba, and elsewhere. Still, the American technological hyper-response to Sputnik ultimately transformed the Western democracies and their economies such that their successes highlighted Soviet failings, eventually accelerating the internal collapse of the Soviet Union.

Public perceptions about American technological superiority may again be changing direction. After decades of U.S.–Russian space cooperation, debate with respect to comparative U.S.–Russian prowess in space has returned. With the retirement of its space shuttles in 2011, the U.S. temporarily de-emphasized manned spacecraft. Russian Soyuz rockets currently transport all astronauts—including American—to the International Space Station. While the U.S. explores privatization of space launch,² Russia continues to be the major manned space-launch player. Some believe that U.S. dependence on Russian rocket motors even for important unmanned launches today, in the context of the Russo-Ukrainian crisis, exposes a mini-Sputnik-like embarrassment about a U.S. lack of capacity.

Dramatic demonstrations by Russia and China of anti-satellite (ASAT) and military cyber-capabilities have underscored concerns about national security threats to U.S. operations both in space and on earth. Russia and China are exploring cooperation in space bilaterally³ and as an incentive for cooperation within the BRICS group.⁴ In the years ahead, China may surpass Russia in producing technological surprises in space and in other domains that have significant geostrategic impact. Continuous testing of ever more capable missiles by

2 “Commercial Resupply Services Overview,” NASA, accessed November 1, 2016, https://www.nasa.gov/mission_pages/station/structure/launch/overview.html.

3 “China offers electronics for Russian rocket engines,” *Space Daily*, April 20, 2016, http://www.spacedaily.com/reports/China_offers_electronics_for_Russian_rocket_engines_999.html

4 A first meeting of the Space Agencies of Brazil, Russia, India, China, and South Africa (BRICS) was held this year; see “China wants to buy Russian rocket engines as BRICS boosts space cooperation,” *RT*, November 1, 2016, <https://www.rt.com/news/364921-rocket-space-china-russia/>.

North Korea, which has nuclear weapons, and by Iran, which has a latent nuclear program, expands the pool of potential purveyors of surprise.

Sputnik demonstrated that rapid technological change, compounded by political turmoil, could produce major national security surprises. Sputnik-like events remain likely because potential adversaries see leverage in exploiting the global advance and spread of technology. In many regions and scenarios, numerous technologies short of the cutting edge also provide asymmetrical responses to Western capabilities. Future technological surprises will differ from Sputnik and may never match its impact. Indeed, the near-term aftermath of Sputnik would not have been so disadvantageous to the West if the developing crisis had been handled well.

Predicting and preventing Sputnik-like events is difficult, but careful preparation can mitigate their impact, reverse momentum, and prove productive over time. To exploit opportunities and avoid dangers, the U.S. should plan and program recognizing that:

- Some surprise is inevitable.
- The national security impact of technological surprise can be great.
- Valuable “lessons learned” exist.
- Sound strategy and ongoing preparation can help the U.S. anticipate, mitigate, and respond to surprise.
- Timely exploitation of peer-level technical competence is essential.
- Taking on the risk inherent in cutting-edge S&T programs can give the U.S. the insight and options necessary to reduce the national security consequences of surprise.
- Preventing an embarrassing or dangerous “fait accompli” requires that agile planning, talent, tools, infrastructure, and organizations be in place.
- To minimize damage in the face of strategic surprise, a healthy habit of competitive innovation and exploration of diverse options must be established.

In short, maintaining a timely ability to anticipate, innovate, and act in fields of science and technology that others may exploit is essential to managing technological surprises such as Sputnik-like events. The sixtieth anniversary of Sputnik I in 2017 can energize efforts to revisit the impact of technological surprise and lessons learned. Given the rise of technological near-peers such as Russia and China and antagonistic states such as Iran and North Korea that have technological means and psychological motivations to demonstrate their prowess vis-à-vis “The West,” the failure to prepare for technological surprise could be dangerous and costly.

The Sputnik Crisis—Existence Proof and Case Study

The premier existence proof of the potential for dramatic effects from a singular event was the 1957 launch by the Soviet Union of Sputnik I, the first space satellite of human origin. Experts anticipated the launch. It demonstrated no immediate military utility. Nevertheless, Sputnik I had a profound and immediate strategic impact. The reasons for the heightened global surprise and uneven American response are clear.

First, the U.S. was expected to be first and best, but was not. The U.S. had already announced a planned launch of its own satellite during the upcoming International Geophysical Year. Indeed, the U.S. was so certain that the U.S. Navy Vanguard rocket would work that Washington had already ordered an Army competitor to stop work. The U.S. began a self-confident public drumroll, building expectation of peerless U.S. leadership. Despite Moscow's announcement that the Soviet Union would attempt to launch its own satellite, the U.S. did not prepare the public or opinion leaders for the prospect that the United States might not be first. Nor did the U.S. government anticipate that the American public would see being second as a sign of grave danger.

Second, the initial U.S. response was inarticulate and ineffective in the face of America's highly visible superiorities in rocket throw-weight and payload size. Although Soviet General Secretary Nikita Khrushchev's comment that "The United States now sleeps under a Soviet moon" was hyperbole, the American attempt to dismiss the successful Soviet launch of an "artificial moon" as merely well-understood celestial mechanics and the simplest of rocket science was widely perceived as "sour grapes." Quickly the story was viewed in geostrategic and political terms, with U.S. Senate Majority Leader Lyndon Johnson calling for a congressional investigation of the implications of Sputnik.

A second successful Soviet launch a month later with the live dog "Laika" on board (November 3, 1957), even before the first U.S. launch attempt, built a news storyline that contrasted accelerating Soviet success with U.S. inertia. On December 6, 1957, when the first American attempt to launch a satellite with the Navy's Vanguard I blew up on the launch pad, press coverage switched from a theme of the United States moving to regain the lead to a theme of America falling further behind.

On January 31, 1958, four months after Sputnik I and almost two months after the first failed Vanguard attempt, the first U.S. satellite, Explorer I, was finally launched through a reactivated Army/Jet Propulsion Laboratory program. Earlier, that program had been put aside, in part because it was a military program and included former German rocket scientists. The rapid Explorer I response was made possible only because the Army had independently decided to keep its own space launch options open.⁵

⁵ For a detailed history of the Army efforts and the controversial role of German scientists, see Paul Dickson, *Sputnik: The Shock of the Century* (New York: Walker Publishing Company, 2001), especially Chapter Three, "Vengeance Rocket."

The quick success of the reconstituted Explorer I program had only a limited impact on the public. In contrast with the 1,121-pound Sputnik II, launched in November 1957, the thirty-one-pound Explorer I seemed small. Soviet General Secretary Khrushchev pounced on the even smaller Vanguard I, calling the three-pound payload a “grapefruit satellite.” This comparison shaped the public image of the emerging Sputnik Crisis.

Both the United States and the Soviet Union followed with successes and failures, but the early failure rates were different. A Soviet satellite launch failure on February 3, 1958, four days after the U.S. launched its first Explorer I, was followed two days later by the second Vanguard failure, again undermining American talking points asserting that the U.S. was regaining the lead. Between December 6, 1957, and September 18, 1959, eight of eleven U.S. Navy/Navy Research Laboratory attempts to launch satellites on Vanguard failed, continuously and vividly undercutting U.S. prestige. The contrast between self-confident Soviet achievements and nervous American failures was amplified by the new social media of the time, television, which instantly and vividly portrayed Soviet space boosters on launch platforms ascending juxtaposed with U.S. boosters exploding.

Successes for the United States, such as Explorer I’s discovery of the Van Allen radiation belts, were drowned out by the overwhelming perception that the U.S.S.R. was ascendant. Vice President Richard Nixon, in his 1959 Moscow “Kitchen Debate” with First Secretary Khrushchev, emphasized the high standard of living that everyday Americans obtained from the peaceful application of technology, but at home, as the U.S. elections approached, the debate focused on Soviet technological prowess, the “missile gap,” and American decline. The economic recession and the Asian flu pandemic of 1957/’58 that had killed some 69,800 Americans⁶ provided a domestic backdrop that reinforced pessimism.

Dismissing possible new Soviet nuclear threats as insignificant given the existing nuclear capabilities of the United States was seen as “spin control” and political damage limitation at best. Worse, invoking our nuclear deterrent and asserting that it was already sufficient to negate any new developments only invited questions about U.S. leadership and competence. Such reassurances only amplified the perceived danger, raised questions about the credibility of U.S. commitments to provide allies with an American nuclear umbrella, and encouraged debates over “How many nuclear weapons are enough?”, the increasing risk of surprise nuclear attack, and “Does the U.S. government know what it’s doing?”

Third, Sputnik was seen as a harbinger of a military revolution. Both domestic and international press rushed to extrapolate the Sputnik Crisis into a “missile gap” more frightening than the earlier “bomber gap.” Intercontinental missiles were seen as making the U.S.S.R. the true, modern global power. The prospect of shorter-range Soviet missiles as well as intercontinental ballistic missiles (ICBMs) undermined allies’ confidence in the U.S.

⁶ “Asian flu of 1957,” *Encyclopedia Britannica*, accessed October 14, 2016, <https://www.britannica.com/event/Asian-flu-of-1957>.

and built pressure for American regional deployments to avoid the “decoupling” effects of emerging local Soviet nuclear advantages.

The specter of the “weaponization of space” moved quickly to the United Nations, ultimately leading to the Outer Space Treaty. Concern about crisis stability led to the 1958 international “Surprise Attack Conference.” The potential for satellite communications and spy satellites was seen as further enabling global military reach. Defenses against missiles joined air and civil defense as hot topics. Lack of confidence in both U.S. intelligence and counter-intelligence became widespread, with renewed concerns about “atomic spies” and the “Red Scare.” In government, interest in controlling technology through export controls expanded.

Although President Eisenhower hoped that Sputnik would lead to Moscow’s acceptance of the legality of future reconnaissance-satellite overflight of sovereign Soviet territory, in the near term, U-2 flights over the central U.S.S.R to monitor missile fields became more urgent. This led to the 1960 Soviet shoot-down of Francis Gary Powers and the collapse of a U.S.–U.S.S.R. Summit to deal with Berlin. Fear of advancing Soviet intercontinental nuclear capability increased pressure for the 1958 Nuclear Test Moratorium.

Fourth, the global shadow of the Sputnik Crisis led to geopolitical interpretations adverse to the United States. Western media declared the Soviet Union to be leading in a “space race,” prompting a flurry of competing stories underscoring indications of the decline of the American-led West. Moscow exploited the contrast between Soviet technological successes and American failures to pronounce the superiority of the Soviet economic system. A number of countries, such as Ghana,⁷ strengthened their ties to Moscow, although none went so far as Cuba. Others distanced themselves from the West in general and from capitalism in particular. In 1961, the Non-Aligned Movement (NAM) was created. Led by Yugoslavia, India, Indonesia, Ghana, and Egypt, this diverse group of nations quickly included most newly independent countries, but also included Cuba and the People’s Republic of China.

Many political parties in the West, as in the developing world, cited Sputnik as a demonstration that command economies, central planning, and state-ownership were the wave of the future politically, economically, and technologically. This complicated closer ties among market economies and created sharper divisions within Western democracies. Policies of NATO members toward the Soviet Union diverged as each government dealt with domestic political polarization between Left and Right, leading to mass peace movements, but also mobilizing nationalists. France moved decisively in its own direction, making the decision to acquire nuclear weapons and ultimately withdrawing from NATO’s integrated military command.

7 See for example Alessandro Iandolo, “The Rise and Fall of the ‘Soviet Model of Development’ in West Africa, 1957–64,” *Cold War History* 12, no. 4 (2012): 683–704, accessed 28 Feb 2017, <http://www.tandfonline.com/doi/citedby/10.1080/14682745.2011.649255>.

Fear of a missile gap became a central issue in the 1960 presidential election, shaping public perceptions of U.S. vulnerability and driving public policy analysis and priorities. Belief in a missile gap may have helped determine the outcome of the election. The debate had an impact overseas as well. NATO insecurities led to flirtation with the concept of a Multilateral Force (MLF) and ultimately the elaboration of the declared nuclear doctrine of “flexible response” in an effort to reassure allies and discourage more states from seeking nuclear weapons. U.S. flight test failures involving an air-launched ballistic missile (ALBM) being developed with the United Kingdom led to the 1961–62 “Skybolt Crisis.” Efforts to repair the U.S.–U.K. “special relationship” after the Skybolt debacle resulted in the Nassau Agreement to share Polaris Submarine Launched Ballistic Missiles (SLBMs) with the UK.

A more self-confident Soviet Union increased its adventurism. Moscow’s perception that geostrategic trends were going its way perhaps made more likely the Berlin Crisis of 1961 that led to the Berlin Wall, the 1961 Soviet breakout from the Nuclear Test Moratorium, and the 1962 Cuban missile crisis. Insurgencies and regimes such as Fidel Castro’s Cuba looked increasingly to Moscow for support. Demonstrations of Soviet technical prowess in one area made more credible reports of Soviet advances in other areas: for example, corroborating reports of a massive, high-tech Soviet biological weapons program that caused the United States to worry about a “bug gap.” Ironically, in the Soviet Union, the success of Sputnik contrasted with weaknesses in microbiology resulting from Stalin’s purges and the remnants of Lysenkoism. As a result, a major qualitative modernization of the large Soviet biological weapons program actually followed several years after Sputnik.⁸

Building on Sputnik-derived technology, Yuri Gagarin’s orbiting of the earth on April 12, 1961 dramatically boosted the idea of Soviet technical superiority once again. Subsequent U.S. suborbital flights contrasted poorly. The one-two punch of Sputnik I and II and momentum resulting from Moscow’s “bookending” of the first U.S. manned space launches with the orbital flights of Yuri Gagarin and Gherman Titov shaped the new Kennedy Administration’s views on Berlin, Vietnam, and Cuba, leading both to the largest nuclear buildup in history and to the decision to put a man on the moon. Fear of missiles, amplified by the very public Sputnik experience and the missile gap debate, shaped how the Cuban missile crisis was perceived and handled.

Fifth, and finally, the U.S. response that ultimately proved necessary to counter the adverse impact of the Sputnik surprise was larger, more urgent, and more far reaching than anyone had anticipated at the beginning of the Sputnik crisis. Just 18 days after the second Sputnik launch, President Eisenhower upgraded the Scientific Advisory Committee in the Office of Defense Mobilization to be the Presidential Science Advisory Committee and moved it to the White House. DOD created the Advanced Research Project Agency (now DARPA) a few months after Sputnik, accelerating innovation for military and ultimately civilian applications. The National Defense Education Act (NDEA) was enacted, funding the greatest

⁸ See for example, Milton Leitenberg and Raymond A. Zilinskas with Jens H. Kuhn, *The Soviet Biological Weapons Program: A History* (Harvard University Press: Cambridge, Massachusetts, 2012).

increase in STEM expertise in American history and providing much of the national-security related talent in the U.S. over the next four decades.

The North American Air Defense Command, activated one month before Sputnik to deal with the bomber threat, was re-oriented to deal also with the anticipated missile threat. Ballistic Missile Early Warning System (BMEWS) radars were deployed over the next few years. The National Aeronautics and Space Administration (NASA) was created to replace the National Committee on Aeronautics (NACA) ten months after Sputnik. The National Science Foundation budget was increased by 271% in one year on the way to an increase of 964% in eight years.⁹

Three months after Sputnik I, one month after the U.S. Navy Vanguard I “Kaputnik” failure, and one month before the U.S. Explorer I success, the Pentagon decided to accelerate the Polaris SSBN submarine program. The decision exploited a fundamentally new warhead technology developed at Lawrence Livermore National Laboratory that would permit smaller solid-rocket-motor SLBMs. The new solid-rocket-motor SLBMs, in turn, permitted adding a quickly designed, 16-tube missile section to an SSN attack sub already under construction by cutting the existing submarine in two.¹⁰

Thus, U.S. ballistic missile submarines went on patrol in two years rather than in the seven or more years that would be required with a new submarine design even with existing Cold War urgency (i.e., in 1960 rather than in 1965). To put this in perspective, consider that comparable programs today may be twenty years or more. In just the ten years following Sputnik, the U.S. nuclear weapons stockpile grew from 5,543 in 1957 to 31,255 in 1967 (compared to today’s pre-Sputnik level of 4,018).¹¹ Immediately after the launch of Sputnik, DOD turned to the Program Analysis and Review Technique (PERT) to manage and accelerate complex research and development programs such as Polaris, where uncertain requirements and timelines exist.¹² Notably, a missile-defense development program including both sensors and interceptors was expanded and accelerated. Most memorable, however, was President Kennedy’s widely publicized commitment to send a man to the moon and back, renewing an emphasis on big science that had declined after the Manhattan Project.

9 See National Science Foundation, *NSF Requests and Appropriations By Account: FY1951–FY2017*, accessed February 28, 2017, <https://dellweb.bfa.nsf.gov/NSFRqstAppropHist/NSFRequestsandAppropriationsHistory.pdf>,

10 See for example, Graham Spinardi, *From Polaris to Trident: The Development of U.S. Fleet Ballistic Missile Technology* (New York: Cambridge University Press, 2008) and George J. Refuto, *Evolution of the U.S. Sea-Based Nuclear Missile Deterrent: Warfighting Capabilities* (Xlibris Press, 2011).

11 U.S. Department of Defense, “Stockpile Numbers: End of Fiscal Years 962–2015,” 2015, accessed October 14, 2016, http://open.defense.gov/Portals/23/Documents/frddwg/2015_Tables_UNCLASS.pdf, and see Office of the Vice President, “Remarks by the Vice President on Nuclear Security,” Washington, D.C., January 11, 2017, accessed February 28, 2017, <https://obamawhitehouse.archives.gov/the-press-office/2017/01/12/remarks-vice-president-nuclear-security>.

12 See the classic Harvey M. Sapolski, *The Polaris System Development: Bureaucratic and Programmatic Success in Government* (Cambridge, MA: Harvard University Press, 1972), accessed February 28, 2017, <http://www.hup.harvard.edu/catalog.php?isbn=9780674432703>.

Surprise and Security: “The Frog in the Pot” Versus Sputnik

In the rapid political, economic, social, and technological change of the 21st Century, the United States needs strategies and capabilities to respond effectively to technology challenges through which other actors may:

- catch up with us on paths we are taking,
- pass us even on our own preferred paths,
- advance on paths we do not favor,
- accelerate along new paths we did not foresee, or
- exploit older, even abandoned paths as asymmetric responses.

The widespread availability of latent, dual-use technology portfolios, the proliferation of scientific talent, and the growth of centers of excellence around the world provide many alternative paths and reduce lead times for exploitation of technology. This global S&T dynamism increases the chances of surprise. Even if most technological challenges are associated with recognized trends and closely watched developments, some challenges do result from unexpected circumstances or events that suddenly surprise us. Such risks, however, are reduced when we have adequate and timely responses.

Most S&T challenges are obvious, although some may be hidden in plain sight. Few are completely concealed. Not all result in surprise, and most surprises are matched, countered, co-opted, or exploited before they become a national security danger. More often a rising tide lifts all boats, as technological competition makes advanced capabilities available more broadly.

Even equal access to technology, however, can have asymmetric effects, sometimes favoring smaller, more agile actors. Such highly focused innovators may be less transparent, less risk averse, and more persistent. Moreover, they may have the opportunity to pick the time, location, and scenario in which to mount precise challenges against technology leaders whose larger size; broader vision; risk aversion; and complex budget, management, and decision processes may slow responses.

In some cases, surprise may emerge slowly and openly. Consider the proverbial “frog in the pot” psychology wherein we find ourselves unprepared because we do not perceive any individual event to be action-forcing until it’s too late to do anything about it. Our sensitivity threshold is too high to trigger a response before the situation becomes dire. With each small step taken against our interests we do not perceive the ultimate consequences of the many steps to come.

In other cases, a specific galvanizing act or event does occur. If the impact is very large and persistent, we might say it was a “Sputnik-like event.” Such singular technological developments that have sudden, significant geopolitical and/or military consequences

are rare, but they can be especially challenging to national security. This paper focuses on the potential for Sputnik-like events rather than on threats that accumulate and reveal themselves gradually. The lessons learned, however, apply more widely to technological challenges, surprise or no surprise.

To avoid the fate of the frog in the pot, Sputnik-like events require the accumulation of STEM¹³ talent, ample resources, and sustained programs over time. The central features of Sputnik-like events are sudden awareness of immediate or inevitable risks of large magnitude combined with unavailable, inadequate, or inappropriate response options. In seismic terms, the frog in the pot produces many tremors and occasional large quakes, but Sputnik produced “The Big One.” In either case, the ultimate consequences can be great.

Potential Sputnik-like events could involve peer, non-peer, and even non-state actors. Today, transformation takes place in weapons themselves and in delivery platforms, basing, connectivity or control, situational awareness, support technology, research empowering technology, technical demonstrations, industrial technology, or the life and behavioral sciences. Technologies exploited might have applications to weapons of mass destruction (WMD),¹⁴ kinetic weapons, cyber operations, space warfare, multi-mission and poly-capable military or civilian delivery platforms, space launch vehicles, conventional or exotic explosives, unconventional/covert operations, counter-space capabilities, Electromagnetic Pulse (EMP), other weapons effects, warhead packaging, CBRNE (Chemical, Biological, Radiological, Nuclear, and High Yield Explosive) materials production, communications, sensors, battlefield awareness, force integration, stealth or counter-stealth, advanced submarines, anti-submarine warfare (ASW), air and missile defenses, and directed energy weapons.

The technologies themselves might include lasers, optics, information technology, artificial intelligence, robotics, unmanned vehicles, precision navigation, advanced manufacturing, HPC-aided design, simulations and surrogate operational testing, miniaturization, new and engineered materials, advanced armor, synthetic chemistry, nanotechnology, genetic engineering and other biotechnology, human performance enhancement, planetary or moon exploits, geo-engineering, tunneling and other target hardening, camouflage and deception, encryption, non-lethal weapons, new scientific principles, counterfeiting and other technology-enabled economic or societal warfare, etc.

Thus, the symbol of a Sputnik-like event may be a prototype, a technical demonstration, an enabling technology, or even a basic science experiment. It could be some combination of these. Sputnik itself was flown on the prototype of an ICBM, the R-7 “Semyorka,” which had a spotty early test record, prompting the substitution of the hastily assembled, lightweight payload that became Sputnik I for a much heavier satellite that became Sputnik III.

13 Science, Technology, Engineering, Mathematics.

14 Weapons of Mass Destruction, sometimes expanded to WMDD or Weapons of Mass Destruction and Disruption.

Ironically, the R-7 quickly proved to be a poor ICBM, but, as the technology matured over the decades, the R-7 became the basis for one of the most successful and frequently used families of large space-launch vehicles. Likewise, the Sputnik I satellite itself did little more than demonstrate celestial mechanics, although scientists were able to add some science value by tracking and listening to its simple broadcast.

The significance of the R-7 and Sputnik I was less what they did, or how well they did it, than what they portended. The driver for a Sputnik-like event is the geostrategic context as much as the technology. Sputnik-like events can differ in type and magnitude due to factors such as:

- the implications for our interests and values,
- the centrality of the technology involved,
- the weight of circumstances or the context,
- the achievements of others,
- the exploitation by the successful actor,
- the clarity of public discussion despite complex, proprietary, and even classified information,
- the capacity for meaningful, timely, and sustained response,
- the perceived magnitude of our failure,
- the impact on third parties internationally, and
- the domestic audience that becomes aware, i.e., experts, officials, publics.

No consensus exists establishing a threshold for declaring an event “Sputnik-like,” and analysts disagree as to what events are legitimate examples. A spectrum of candidates to be Sputnik-like shocks includes the 9/11 attacks; the “Shock and Awe” of stealth and precision in Desert Storm; the Manning/Snowden/NSA downloads; “Stuxnet” and other cyber activities such as the hacking of the Democratic National Committee; the Three Mile Island, Chernobyl, and/or Fukushima nuclear reactor accidents; radioactive fallout contamination such as the “Castle Bravo” contamination from an atmospheric nuclear test; nuclear missile or bomber accidents; the sinking of nuclear submarines; new nuclear weapons tests (atmospheric or underground); the technological escalation of improvised explosive devices (IED); WMD terrorism such as that of Aum Shinrikyo; or even the disappearance of Malaysian Airliner MH370.

All have had international security impact. Nuclear weapons use would be a major tipping point, but thus far chemical weapons use, the accidental sinking of nuclear powered submarines, and the post-9/11 anthrax attacks have had less of a Sputnik-like effect than many had anticipated. Perhaps decryption by a future quantum computer of highly

encrypted nuclear weapons data, acquired but unreadable in the past, would be Sputnik-like. Again, the context is as important as the event.

Contrasting success with failure was a major feature of the original Sputnik dynamics and contributed to its instant and escalating consequences. Had Soviet success been followed by a corresponding U.S. record of success, President Eisenhower's letters to Soviet Premier Bulganin and First Secretary Khrushchev of 1957–58 proposing cooperation on the peaceful uses of space might have enabled the joint U.S.–U.S.S.R. space program to begin many years earlier. Instead, his proposals were rejected in a climate of Soviet triumphalism, including Moscow's demand that U.S. forward-based nuclear systems be removed from Turkey as a precondition.

The Soviet Union proved initially unenthusiastic even in the multilateral negotiations in the United Nations that led to the Outer Space Treaty of 1967. Discussions began after John Glenn's orbital flight, but a concrete cooperative space program did not begin until the Soviet-manned lunar program experienced major setbacks while the U.S. Apollo program successfully put men on the moon.

Some technological surprises with major strategic consequences are driven by a sudden failure rather than success. Three Mile Island for the United States, Chernobyl for the Soviet Union, and Fukushima for Japan all involved domestic failures that had important international impact. Chernobyl was a major catalyst for the collapse of the Soviet Union. Some would not consider such predominantly self-induced negative technological catastrophes as Sputnik-like no matter what the strategic effect. Still, Moscow's silence, then obfuscation concerning the massive radioactive releases from the nuclear reactor accident at Chernobyl—located in Ukraine near Belarus and contaminating parts of Western Europe, especially in Scandinavia—raised doubts about the legitimacy and viability of the Soviet Union compared to the Western model.

What can cause a Sputnik-like event changes with circumstances over time. The threshold to produce a psychological impact has risen markedly. Consider the example of space-launch capability. In 2010, Japan completed a seven-year round-trip to a distant asteroid, gathering samples and successfully returning them to earth. Ten countries, the European Union, and even private companies have now launched their own satellites on their own boosters. This includes India, Israel, Iran, and North Korea. India has launched an orbiter to Mars; China has placed the "Jade Rabbit" rover on the moon; and SpaceX Corporation has put a 7000-pound commercial satellite into geosynchronous orbit. None of these activities has yet produced a dramatic public effect like that in the original Sputnik crisis, but all signal important trends with both positive and negative strategic implications.

Terra Bella,¹⁵ the commercial miniature satellite constellation project formerly known as "Skybox," aims toward providing global, real-time one-meter photographic resolution

15 "Terra Bella," *Planet*, accessed December 4, 2017, <https://www.planet.com/terrabella/>.

to customers around the world. Terra Bella, recently sold by Google to Planet,¹⁶ builds on the “CubeSat” format that has permitted smaller countries, industry, and nonprofit organizations to have their own satellites in space. Private launch services are supplementing traditional space-launch vehicles for this purpose. Today, private individuals can already obtain essentially free access to satellite imagery that once only superpowers could obtain and then only after those powers invested billions of dollars. What was once inconceivable is now routine. Numerous state and non-state actors may soon have the means to exploit space activities in surprising ways.

Sputnik-like events require more than a spectacular technological accomplishment. They must take place in an international security context involving competitors willing to exploit the event for strategic gain, both political and military. Immediately after the launch of Sputnik I, Moscow was slow to comment on what it had achieved. The excitement of Western audiences, however, sparked the multi-decade implementation by the Soviet Union of a strategy aimed at contrasting Soviet technical prowess with images of American “Me too!” efforts to catch up. Moscow sustained its public affairs momentum by continuing to exploit Sputnik-style spectacles, notably politically symbolic “firsts” such as the first animal, man, and woman in space, the first spacewalk, the first probe to reach the moon, the first moon rover, etc.

The original U.S. space technology program had some qualitative advantages over Soviet technology. Much of this was too subtle, however, to manifest itself in the battle for public opinion. Subsequent U.S. successes, even in the face of Soviet failures, were unable to quickly undo the image of Soviet superiority built up at the beginning of the space race. The momentum shifted decisively, however, after 1969, when U.S.-manned lunar landings on the moon contrasted so vividly with the numerous failures in the troubled Soviet unmanned lunar robot program. Indeed, Luna 15 crashed on the moon while Apollo 11 was still on the moon’s surface. Apollo was meant to be a “counter-Sputnik,” and it was. It was meant to rebalance, and it did. Much of the positive symbolism of Apollo, however, was drowned out by the consequences of the war in Vietnam.

The space race did not end with Apollo, but its context changed. In the period since the breakup of the Soviet Union, widespread dependence on the Russian Federation to put men and objects in space has been a major source of Russian pride. During the recent Russo-Ukrainian crisis, however, reacting to Western sanctions in April 2014, the Deputy Prime Minister of the Russian Federation, Dmitry Rogozin, tweeted the message, “After analyzing the sanctions against our space industry, I suggest to the U.S.A. to bring their astronauts to the International Space Station using a trampoline.”¹⁷ Immediately, a sub-committee

16 Alex Knapp, “Google Is Selling Its Satellite Business Terra Bella to Satellite Startup Planet,” *Forbes*, accessed February 28, 2017, <https://www.forbes.com/sites/alexknapp/2017/02/07/google-is-selling-its-satellite-business-terra-bella-to-satellite-startup-planet/#35612b946231>.

17 “Trampoline to Space? Russian Official Tells NASA to Take a Flying Leap,” *NBC News*, accessed November 4, 2016, <http://www.nbcnews.com/storyline/ukraine-crisis/trampoline-space-russian-official-tells-nasa-take-flying-leap-n92616>.

of the U.S. House Armed Services Committee added money to the defense budget for development of an American-sourced rocket motor to replace Russian motors now used by United Launch Alliance (ULA) for its Atlas V rocket. Orbital Sciences Corporation also uses Russian-designed motors for its Antares rocket.

In response, Elon Musk, founder of SpaceX, which provides American-built rockets for NASA, tweeted “Sounds like this might be a good time to unveil the new Dragon Mk 2 spaceship that @SpaceX has been working on w @NASA. No trampoline needed.”¹⁸ Musk had earlier announced a suit against the Defense Department for sole-sourcing military launches to the ULA team of Boeing and Lockheed Martin. The geopolitics of space competition remain active today.

Future Sputnik-like events need not involve space. Nevertheless, the growing dependence of the United States and its allies and friends on extremely valuable but fragile space-based assets still makes that domain a prime candidate for surprise. The surprise, however, may or may not involve traditional access and use of space. Candidates for national security surprise in space include cyber operations, direct-ascent or directed-energy anti-satellite weapons (ASATS), anti-space nuclear and other weapons effects, and even manned operations. Sputnik-like events in space may be enabled by technologies not normally associated with that domain.

Scenario-Based Assessments of Possible Sputnik-like Consequences

The 1957 Sputnik surprise impacted nearly all aspects of national security. A future Sputnik-like event, however, will likely differ from the historic Sputnik crisis in terms of the technology involved, the path it takes, how quickly it plays out, and its significance. Analysis of alternative scenarios, taking into account both new technological developments and a range of actors and dynamics, greatly assists simulation, evaluation, planning, and training related to policy, strategy, RDT&E, procurements, and operations.

The time factor is also important. The Sputnik crisis is remembered primarily for U.S. mistakes. Nevertheless, early U.S. responses to Sputnik included successes as well as failures, and the cumulative response over time was an overwhelming success. Reduction of harm early on could have been achieved given Soviet problems and the existence of countervailing U.S. achievements. Some would argue, however, that the early embarrassments to Washington actually resulted in a larger and more successful response over time, strategic as well as technological.

To improve the ability to anticipate, mitigate, and respond quickly to possible Sputnik-like events, challenging scenarios should be developed and analyzed. For example, useful scenarios could assess whether a plausible surprise might:

¹⁸ Ken Kremer, “SpaceX CEO Elon Musk to unveil manned Dragon ‘space taxi’ on May 29,” *Phys*, May 28, 2014, accessed November 4, 2016, <http://phys.org/news/2014-05-spacex-ceo-elon-musk-unveil.html>.

- 1) Alter peer relationships adversely by creating the reality or perception of U.S. weakness, for example demonstrating military capabilities beyond those of the United States.
- 2) Provide incentives for Russia, China, or others to form adversarial alliances aimed at the U.S. and its allies.
- 3) Undermine confidence in U.S. extended deterrence, perhaps by presenting scenarios in which the U.S. might not have credible responses or is seen as “decoupled from the region.”
- 4) Permit an adversary to implement a “fait accompli” attack on the U.S., an ally, its own soil, or perhaps disputed territory.
- 5) Provide competitors or adversaries with a more credible ability to act decisively at lower levels of the escalatory ladder or along an “escalatory lattice” of multi-domain¹⁹ technologies (e.g., cyber, electromagnetic, etc.) with precise attacks, low collateral damage, tailored effects, or even non-kinetic kill to negate the U.S. nuclear umbrella or conventional force projection.
- 6) Project an aura of geographical isolation of U.S. strategic forces from the allies overseas they are meant to reassure.
- 7) Encourage potential adversaries to offer special security guarantees to countries of concern, such as North Korea, Iran, etc.
- 8) Incentivize closer relationships between an adversary and nations for whose loyalty we compete, even if only to encourage U.S. allies and friends to play both sides against each other.
- 9) Create unintended acquiescence in support of an adversary’s achievement while inspiring campaigns to freeze, block, or ban any comparable U.S. response.
- 10) Encourage alternative, independent military power centers that may be destabilizing globally or in regions.
- 11) Focus blame on the U.S. rather than the actual initiators for having inspired new military capabilities.
- 12) Undermine U.S. exploitation of dual-use technology, especially if the impression is created that the new technologies are in tension with major international instruments and objectives such as the biological weapons convention (BWC), chemical weapons convention (CWC), Landmine convention, Treaty on the Nonproliferation of Nuclear Weapons (NPT), Comprehensive Nuclear-Test-Ban Treaty (CTBT), Fissile Material Cut-Off Treaty (FMCT), etc.
- 13) Inspire civilian exploitation by others who seek latent military capabilities.

What Is to Be Done? Learning from Sputnik and the Space Race

Successfully addressing the consequences of Sputnik-like events and other, less dramatic technological surprises requires effective strategies, capabilities, and actions in the face of

¹⁹ “Multi-domain” has largely replaced “cross-domain” in Defense Department references to the interaction of these different military technologies.

uncertainty. This means success depends on America's ability to anticipate, innovate, and deliver diverse responses. Clear recognition of circumstances, prediction of events, and prevention of adverse developments, however, are problematic. Thus, realistic scenarios that introduce uncertainty should be elaborated to guide formulation of strategies for prevention and response. Furthermore, poor timing and performance, often made more likely by dynamic and morphing scenarios, can negate otherwise prescient strategies and amplify surprise. Such uncertainties are too often not reflected in planning assumptions.

Even with perfect prediction, developments clearly anticipated in planning can get lost in the noise or momentum of implementation of the plan. Surprise should be seen as a process in which adverse consequences are multiplied when uncertainty and inattention undermine capabilities for timely response. In the case of technological surprise, the products of research and development may be clear long before the significance for national security is clear. Even when national security concerns emerge, overburdened decision-makers often see unrealized techno-military possibilities as "improbable," "over the horizon," or even "inconceivable," until after a concrete, dramatic demonstration. Even then, a response might not be supported until the broader political community recognizes the consequences.

Compartmentalization, "stovepiping," and failure to see multi-disciplinary synergism and multi-mission applications increase the risk of surprise. Preexisting STEM competence and sustained capabilities are vital, but interdisciplinary knowledge of interacting technological, economic, or strategic factors is also essential. Likewise, diverse, cross-cultural experts provide different insights into potential developments.

Such cross-discipline brainstorming tends to reduce surprise. More general understanding of the sources of surprise provides a framework for anticipation including difficulties in:

- detecting change,
- identifying possibilities,
- calculating probabilities,
- evaluating trends,
- clarifying consequences,
- anticipating reactions,
- predicting counter-reactions,
- computing complex dynamics, and
- compensating for emergent behavior.

Prior planning and preparation are the keys to timely and effective mitigation even in the face of surprise, not because the plans will be perfect, but because the skills necessary for managing surprise will be honed. Lessons learned from past events such as Sputnik can

help. For example, mitigation of the consequences of Sputnik-like events generally requires early demonstration of similar or superior knowledge and capability.

With advanced warning and mature capability, one could preempt with a demonstration of one's own equivalent or better capability. This may help defuse negative reaction to the action of the other. Unfortunately, acting first may also place any perceived responsibility for undesired implications of the action on the U.S. rather than on the party being preempted. "Who is to blame" is a classic element when political or policy debates are about an arms race.

The ability to announce in advance someone else's activity tends to reduce the shock effect when the event occurs. Leaks and false denials, however, can create a drumroll effect that magnifies the adversary's event when it ultimately occurs. Immediate identification of an event and clear explanation based on technical competence tends to be reassuring to allies and publics. Interventions to prevent surprise may be more likely to succeed if private communications are opened before the event and if public statements are made with the confidence of sound information and technical competence.

Acknowledging the self-evident significance of a surprise and then placing it in proper context increases credibility. On the other hand, erroneous statements and assumptions create initial damage that is difficult to reverse. Presentation of a combination of other new or similar capabilities by the U.S. may also reassure. Making available to allies quickly the benefits of any positive, peaceful applications helps reassure, but decisions to deny friends access to technology demonstrated by others may have the opposite effect. Developing tools to balance advantages and disadvantages helps greatly. For example, having some concept about how to exploit, manage, or control the spread of a breakthrough technology may turn the focus toward a work plan rather than an inquisition.

Counter-responses can be similar or asymmetric, immediate or longer term, and qualitative or quantitative. Also, different approaches to countering technological surprise may have different benefits and costs over time. The timeliness and appropriateness of the response may provide more psychological leverage than does the ultimate magnitude of the response. Would the launch of Sputnik have had the effect it had if Washington had emphasized in public in advance that both the United States and the Soviet Union were about to launch satellites and if that statement had been soon followed by a successful American launch?

Readiness for surprise requires the development of options, which in turn requires a relevant technical infrastructure and knowledge base with the agility to respond. This requires practice. "Pay me now" versus "pay me later" trade-offs are inherent in the key questions: What should we prepare for? What are the risks? How ready should we be? What are the costs? How much is enough? Ongoing programs may provide more timely responses than restarts or new starts, but only if they provide a foundation for the needed technical competence and capability.

Conclusions

The 60th anniversary of Sputnik I on October 4, 2017 can be a catalyst to review lessons from the Sputnik crisis. In the context of a Sputnik-like event, success in minimizing the magnitude of surprise, mitigating the downsides of surprise, maximizing possible benefits of change, and managing the process of creative technological advance and obsolescence successfully is more likely when we:

- recognize that surprise is inevitable, and that punctuated, bold “Firsts” carry great weight;
- consider that incremental improvements may have less immediate international or public impact even if their long-term strategic contributions can be large;
- demonstrate the capability and competence to respond credibly to surprise and change;
- understand that appearance of a sudden threat may generate opportunities, resources, and the will to act that might have been lacking without the event;
- explore cutting-edge, albeit risky, S&T in addition to maintaining diverse, multi-disciplinary R&D to gauge possibilities that you or others may wish to explore and provide a foundation for alternative options to match or leapfrog in-kind or asymmetrically;
- prepare to articulate and demonstrate mastery of the subject, initially and over time;
- speak with the confidence that comes from being candid and truthful; and
- understand cultural and political diversity in order to see how different audiences at home and abroad, especially friends and allies, may react and address their individual concerns in a way that is consistent with the message to others.

In short, technological surprise can have severe international security impact. To respond effectively, an energetic base of talent and technology is needed to anticipate, innovate, and deliver options in a timely manner. Creating a healthy habit of promoting and assessing innovation that includes high-risk/high-potential S&T enhances the capability to be competitive in the face of surprise.

Readings on the History of Sputnik

Brzezinski, Matthew B., *Red Moon Rising* (New York: Henry Holt and Company, 2007).

Dennis, D.J., *The Great Space Race* (Australia: coffebook.com.au, 2013). Includes website and video.

Dickson, Paul, *Sputnik: The Shock of the Century* (Walker Publishing Company, 2001).

Divine, Robert A., *The Sputnik Challenge* (New York and Oxford: Oxford University Press, 1993).

Dudney, Robert S., "When Sputnik Shocked the World," *Air Force Magazine*, October 2007, <http://www.airforcemag.com/MagazineArchive/Magazine%20Documents/2007/October%202007/1007sputnik.pdf>. (September 24, 2014.)

Isachenkov, Vladimir, "Sputnik at 50: An improvised triumph," *U.S.A Today*, September 30, 2007, http://usatoday30.usatoday.com/money/topstories/2007-09-303949485139_x.htm. (September 24, 2014.)

Logsdon, John M., *John F. Kennedy and the Race to the Moon*, Palgrave Studies in the History of Science and Technology (New York: Palgrave MacMillan, 2010).

Mieczkowski, Yanek, *Eisenhower's Sputnik Moment: The Race for Space and World Prestige* (Ithaca: Cornell University Press; 2013).

Neal, Homer Alfred, Tobin Smith, and Jennifer McCormick, *Beyond Sputnik: U.S. Science Policy in the 21st Century* (Ann Arbor: University of Michigan, 2008).

Sagdeev, Roald, and Susan Eisenhower, "United States-Soviet Cooperation during the Cold War," *50th Magazine*, May 28, 2008, https://www.nasa.gov/50th/50th_magazine/coldWarCoOp.html.

Siddiqi, Asif A., *Sputnik and the Soviet Space Challenge* (Gainesville, FL: The University of Florida Press, 2000).

Chapter 3

Curious Incidents: Dogs That Haven't Barked

C. Wes Spain

“Is there any point to which you would wish to draw my attention?”

“To the curious incident of the dog in the night-time.”

“The dog did nothing in the night-time.”

“That was the curious incident,” remarked Sherlock Holmes.

—Arthur Conan Doyle, in “Silver Blaze”

We've Been Warned!

Almost daily, we are reminded by journalists, academics, media analysts, business leaders, and domestic and international government officials of the omnipresent dangers of a rapidly globalizing world of high technology that may be beyond our control. The very science and technology that has delivered unprecedented gains in global health and human longevity is also feared to possibly introduce an era of unprecedented vulnerability and harm to the species.

Information and communication technologies that increasingly tie the world together in a global commons are forecast to provide the means to set the world back to the dark ages through destruction of fundamental infrastructure. The means of weaponizing technologies are no longer the sole province of the state, but are increasingly available to groups and individuals enabling unprecedented capabilities to do harm on grand scales. Even military technologies that have been securely maintained by governments are moving to non-state groups as international instability brings about the collapse of states and the loss of control of military technologies.

Warnings of the dangers from new technologies are not new, particularly in the Western world, with more liberal and open societies that almost guarantee their inherent vulnerability to those wishing to do harm. A more recent development is the prominence of the threat of non-state actors, largely driven by assessments that new technologies now can provide the destructive power of the nation-state to these groups or individuals. We are told biological weapons are accessible to terrorists and, on a free and open society, have the mass destructive effect of nuclear weapons, which still remain the ultimate weapon of the state—for now. Individual actors, however, can exploit the computer networks of critical energy, financial, and health systems to wreak havoc on entire nations with very little concern for attribution or penalty.

Despite the near-constant reminder of how dangerous the modern world is, events that match forecasted high-impact threats from modern science and technology are extremely rare. Much more common are attacks using technologies that trace their origins to the ninth century. Why? Are forecasts of threats from S&T simply wrong? Are the warnings prescient, providing governments ample time to respond to, mitigate, or prevent the danger? Are the warnings just too early, and the threats are real and will manifest—in time? Or is something else at work, skewing our threat assessments?

Consider two threats that, despite experts forecasting for decades as nearly inevitable to cause mass carnage, have not produced the warned impacts even when used successfully against unprotected civilian populations: man-portable air defense systems (MANPADS) and biological weapons (or biological agents used to do harm, shortened here to BW). MANPADS and BW are very different weapon technologies, but both have concerned security officials for decades for their potential use against civilian populations. Despite their technological differences, the warnings have been similar: both are readily available, easy to use, could easily claim hundreds—or in the case of BW, thousands—of lives, and, if successful, could dramatically impact the world's economy.

The experience of the past 40 years is very different, however. MANPADS are a very mature and proven weapon system under state control in most countries, but with many available on the black market or in regions of crisis, particularly in recent years. Terrorists or non-state groups have successfully used this weapon system against civilian aviation with varying degrees of effectiveness. According to the U.S. Department of State, since 1975 there have been 40 civilian aircraft hit by MANPADS, causing about 28 crashes, with more than 800 deaths around the world.¹

In contrast, biology is a rapidly evolving scientific field with an expanding array of technical applications and developed technologies, under very little state control globally. Terrorists or non-state groups are reportedly interested in bioweapons, but their use is extremely rare.

1 U.S. Department of State, "MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems," Bureau of Political-Military Affairs, July 27, 2011, last accessed October 17, 2017, https://fas.org/programs/ssp/asmp/issueareas/manpads/Combating_the_Threat_July_2011.pdf.

According to published reports, there have only been two known successful non-state uses of biological agents² since the end of World War II to purposely inflict harm on civilians, resulting in relatively modest impact. In 2001, a reported lone perpetrator conducted an anthrax bacteria attack against government and civilian individuals, as well as employees and customers of the U.S. postal service, resulting in five deaths and 17 injuries over a period of several days. In 1984, a cult used salmonella bacteria to poison food at restaurants in Oregon, resulting in 751 injuries, but no deaths.³

Despite the rare use and relatively modest impact, the warnings continue. Recently in the conflict zones of Syria and Libya, rebels have used MANPADS acquired from fallen government stocks effectively against government aircraft, raising fresh warnings about potential acquisition by terrorist groups for use against civilian aircraft.⁴ In a statement for the U.S. Senate Armed Services Committee in February 2016, Director of National Intelligence James Clapper included the relatively new field of genome editing as a biological technology with WMD potential.⁵

While one can reasonably argue that the attention governments have focused on these threats (particularly MANPADS)⁶ has significantly complicated or disrupted nefarious actors' acquisition and use, that cannot fully explain why impacts of actual use have been much less than warned. Clearly other factors impact the accuracy and reliability of these threat assessments. Instead of government actions, have the limited effects of actual attacks diminished the desirability of these means of attack?

Timely, Accurate Warnings Are Challenging

Why do our government officials, national security, and technical experts continue to warn the public about these dangers when past warnings have proven apparently misleading? The experience of MANPADS and BW suggests the answer is that those responsible for warning of potential threats will sound the alarm because it is better to be "safe than sorry"; better to warn than not. Warned threats that fail to materialize can be attributed to any number of theories to explain absence; failing to warn of successful threats will only be explained as

2 Reference here is made to pathogens.

3 National Consortium for the Study of Terrorism and Responses to Terrorism (START), Global Terrorism Database [data file], 2017, <https://www.start.umd.edu/gtd/>; and Wm. Robert Johnston, "Summary of historical attacks using chemical or biological weapons," *Johnstons Archive*, accessed October 27, 2017, <http://www.johnstonsarchive.net/terrorism/chembioattacks.html>.

4 See Adam Entous, "U.S. Readies 'Plan B' to Arm Syria Rebels," *The Wall Street Journal*, April 12, 2016, accessed October 10, 2016, <http://www.wsj.com/articles/u-s-readies-plan-b-to-arm-syria-rebels-1460509400>; Ben Farmer, "RAF aims to stop menace of terrorist missile strikes on airliners," *The Telegraph*, July 19, 2015, accessed August 24, 2016, www.telegraph.co.uk.

5 Senate Armed Services Committee, "Worldwide Threat Assessment of the U.S. Intelligence Community," by James R. Clapper, February 9, 2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

6 For U.S. government efforts to mitigate the threat from MANPADS, see U.S. Department of State, "MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems," Bureau of Political-Military Affairs, July 27, 2011, last accessed October 17, 2017, https://fas.org/programs/ssp/asmp/issueareas/manpads/Combating_the_Threat_July_2011.pdf.

warning failure.⁷ Moreover, the major consequences of a successful attack of a sort that can conceivably cause a massive number of deaths and colossal economic or environmental disruption is simply too significant to be completely ignored, regardless of how practically remote its chances.

Some of the so-called “failures” of warning are, in fact, emblematic of the inherently difficult proposition of forecasting in general and threat assessment more specifically. The *raison d’être* of the American intelligence community (and a focus of many academic and private-sector analysts) is to provide actionable warning to support timely, prudent, and effective national security decision-making. By forecasting threats and threatening futures through assessment, analysts provide decision-makers with information needed to understand an evolving security environment, more clearly see specific threats to national interests, and inform policy development and prioritization of resource allocation. Since the end of World War II, and significantly shaped by Japan’s surprise attack on Pearl Harbor leading to the U.S. entering that war, American intelligence has been challenged to consistently deliver that service to national security decision-makers.

Central to any meaningful threat assessment is an understanding of an adversary’s intentions and capabilities to realize those intentions. However, intention and capability alone do not represent a complete threat assessment, as neither intention nor capability exists in a vacuum but are absolutely context-dependent. For example, to understand the threat from an adversary’s capability, understanding your own vulnerability to that capability is essential. An adversary wielding a weapon system that can have no negative impact on you (an archer against a modern battle tank, for example) is not a threat.

In contrast, an adversary with a weapon system with no known means of defense—a weapon against which you are completely *vulnerable*—is highly threatening possibly even to the point of calling into question your survival. Consequently, assessments of threats for which defense is impossible or extremely challenging command greater attention from national security decision-makers. Highly capable actors with clear intention to exploit vulnerabilities to do harm to your interests rise to the top of the list of concern.

Accurately and consistently assessing and forecasting threats based on a genuine understanding of an adversary’s intentions and capability is very challenging. Calculating actual risk as a function of this threat calculus greatly complicates the task. Collecting, processing, analyzing, and integrating a threat and risk assessment regarding a particular adversary is prone to error, susceptible to deceit and manipulation, and inherently subjective. Each element—intention, capability, vulnerability, and consequence—demands often distinct or unique information collection and assessment methods that are often disconnected and highly asynchronous.

⁷ Robert Jervis describes a natural trade-off: “When intelligence serves a warning function, there is likely to be a trade-off... between being too sensitive and giving false alarms on the one hand and being less sensitive and running a greater risk of failing to detect a threat on the other.” In *Why Intelligence Fails* (Ithaca, NY: Cornell University Press, 2010), 180.

In contrast, assessing and warning of *potential* threats is, in fact, a simpler and (arguably) safer undertaking. Potential threats are those that can be reasonably assessed as being likely to produce harm if executed, but are not *proven* threats, demonstrated through multiple “successful” attacks. Typically, assessment of potential threats assumes intention of the adversary to do harm and focuses on specific capabilities to harm. Those capabilities that appear most threatening to exploit known or assumed vulnerabilities naturally get much attention. An examination of what damage a particular threat with known or assessed characteristics *could* inflict will contain many assumptions and caveats, making such an assessment easier to complete.

In the absence of specific results of successful attacks, a prudent assessment of a potential threat will almost certainly optimize key variables (even while noting that many variables are not well characterized and may affect a threat, resulting in sub-optimal performance) in order to—at a minimum—simplify analysis and highlight potential impact. Consequently, potential threats almost always are highly impactful and worthy of further investigation.

Other critical drivers of threat assessment are timing and specificity. For an assessment to be “actionable,” it must be timely and specific enough to allow decision-makers a response. Assessments coming too late or being too general provide no time or direction for mitigation or response actions. Conversely, specific threats assessed with enough lead time to allow for action are most prized and—again—are a simpler and safer undertaking. At a minimum, better to warn early than to warn late (even accounting for the high costs of false alarm).

Warning early to allow for mitigation or countermeasure is a core responsibility for those conducting threat assessment of science and technology. If followed closely, developments in the scientific community can indeed provide adequate warning time. Advances and breakthroughs in fields of science typically precede technological application and implementation by years, if not decades, and are not immediately operationalized with widespread national security impacts.⁸ For example, radar has its scientific and technical origins in the late 19th century, with Heinrich Hertz’s experiments in 1887 showing metallic objects reflected radio waves. Fifty years later, with the onset of World War II motivating acceleration of its development, nations operationalized and deployed the technology with strategic military impact.

Contrasted with sudden and salient political developments—such as the so-called Arab Spring of 2011—S&T threat assessment enjoys the benefit of time. Assessments, therefore, can investigate potential impacts of evolving S&T years ahead of any demonstrated threat. For information or intelligence-gathering activities, this lead time may allow for more rigorous and comprehensive collection and analysis.⁹

⁸ See, for example, Max Boot, *War Made New* (New York, NY: Gotham Books, 2006), 8. “Inevitably, there was a lag, ranging from a few decades to a few centuries, between the initial development of a technology and the moment when it transformed the battlefield.”

⁹ S&T advancements relevant to BW may prove to be an exception, with much shorter development times.

Despite the positive attributes, early warning of potential S&T threats has significant drawbacks. Warning too early of S&T developments that *may* have negative national security impact in the future runs the very real risk of no one in a decision-making position paying attention. Decision-makers have to respond to the more urgent—and typically those are issues where more immediate action can have nearer-term effects. There are no shortages of threats; those that are proven and can be addressed in a reasonable time frame (a budget cycle, a political administration’s tenure, etc.) are much more likely to be acted upon. Over time, assessments of more distant threats are more challenging to keep current or to maintain consistent information collection and analytic focus. Once warned (early), there may be very little left to do until the warnings are proven by some technological breakout that would leave very little time to make extremely difficult decisions to mitigate. Practitioners in the field of technology assessment have appreciated this dilemma for decades. As David Collingridge wrote in 1980¹⁰:

The dilemma of control may now be summarized: attempting to control a technology is difficult, and not rarely impossible, because during its early stages, when it can be controlled, not enough can be known about its harmful social consequences to warrant controlling its development; but by the time these consequences are apparent, control has become costly and slow.

Collingridge’s dilemma may be uniquely problematic for S&T assessment in the intelligence community; it challenges the very premise of the intelligence warning function. The problem is compounded by innovative use of existing or dated technology. Providing timely and actionable warning of threats from emerging S&T in this context may be nearly impossible on any reliable basis.

People Are More Challenging

In addition to the general difficulty inherent in the early warning of S&T threats, technical assessments are further challenged because they typically do not adequately consider the critical impact of the people involved, instead focusing primarily (if not exclusively) on technical topics and variables. S&T is only dangerous when a person or group applies it to threatening ends. The people involved in fashioning or employing a technology as a means to do harm against other people or their interests must be central to any robust threat assessment. And to really understand the impact of the people, analysts must consider specific individuals or groups, not generalizations such as “terrorists with university-level education.”

Understanding peoples’ motivations, intentions, and capabilities, as well as the sociocultural and political context matters as much as—if not more than—specific technical characteristics

10 David Collingridge, *The Social Control of Technology* (New York, NY: St. Martin’s Press, 1980), 19.

of particular S&T. With more sophisticated S&T, such as biotechnology and nuclear weaponry, characteristics of the entire development team will directly impact likelihood of success. Factors such as scientific and technical knowledge, tacit knowledge, knowledge transfer and absorption capacity, experience, local culture and work ethic, management culture and practice, work environment, and political environment will determine technical success or failure.¹¹ Analysis must consider these “softer” factors as much as it considers the specific technical issues.

Analysis that neglects or separates the “human” and technical elements is demonstrably flawed. A contemporary example suffices: in a government-directed postmortem that evaluated and critiqued the intelligence and analysis associated with the war in Iraq, a group of former senior intelligence officers led by the former Deputy Director of Central Intelligence, Richard J. Kerr, concluded:¹²

...[T]he analytic judgments rested almost solely on technical analysis, which has a natural tendency to put bits and pieces together as evidence of coherent programs and to equate program to capabilities. As a result the analysis, although understandable and explainable, arrived at conclusions that were seriously flawed, misleading, and even wrong...The national intelligence produced on the technical and cultural/political areas [in Iraq], however, remained largely distinct and separate. Little or no attempt was made to examine or explain the impact of each area on the other.

Thus, perspective and a comprehensive sense of understanding of the Iraqi target per se were lacking. This independent preparation of intelligence products in these distinct but interrelated areas raises significant questions about how intelligence supports policy...The bifurcation of analysis between the technical and the cultural/political in the analytic product and the resulting implications for policy indicates systemic problems in collection and analysis. Equally important, it raises questions about how best to construct intelligence products to effectively and accurately inform policy deliberations.

11 See Kathleen M. Vogel, *Phantom Menace or Looming Danger?* (Baltimore, MD: The Johns Hopkins University Press, 2013); Sonia Ben Quagham-Gormley, *Barriers to Bioweapons* (Ithaca, NY: Cornell University Press, 2014); and Jacques E. C. Hymans, *Achieving Nuclear Ambitions* (New York, NY: Cambridge University Press, 2012).

12 Richard Kerr et al., “Collection and Analysis on Iraq: Issues for the U.S. Intelligence Community,” *Studies in Intelligence* 49, no. 3 (2005): 48.

Another human element that impacts assessment of threats from S&T is the limitations of the people making the assessment in the first place—the “experts.” Limits of experts’ ability to accurately forecast or predict future events, particularly in time frames of more than a few years out, is well researched.¹³ Some recent work has investigated expert judgment and forecasting specifically in the context of intelligence analysis, with findings clearly relevant to the challenges of warning of S&T threats. In his groundbreaking investigation, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*, Rob Johnston explores the paradox of expertise and accurate forecasting. He argues “... the specificity of expertise ... makes expert forecasts unreliable...[and] seldom as accurate as Bayesian probabilities.”¹⁴ Johnston cites numerous researchers who conclude human biases explain unreliable expert forecasts, with general agreement on two types of bias:

- Pattern bias: looking for evidence that confirms rather than rejects a hypothesis and/or filling in—perhaps inadvertently—missing data with data from previous experiences; and
- Heuristic bias: using inappropriate guidelines or rules to make predictions.¹⁵

Most directly, Johnston concludes that the very process of becoming an expert hamstrings reliable forecasting.¹⁶

In other words, becoming an expert requires a significant number of years of viewing the world through the lens of one specific domain. This concentration gives the expert the power to recognize patterns, perform tasks, and solve problems, but it also focuses the expert’s attention on one domain to the exclusion of others.

It should come as little surprise, then, that an expert would have difficulty identifying and weighing variables in an interdisciplinary task, such as forecasting an adversary’s intentions. Put differently, an expert may know his specific domain, such as economics or leadership analysis, quite thoroughly, but that may still not permit him to divine an adversary’s intention, which the adversary may not himself know.

13 For example, Philip E. Tetlock, *Expert Political Judgment* (Princeton, NJ: Princeton University Press, 2005).

14 Rob Johnston, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, 2005), 61.

15 Ibid, 66.

16 Ibid.

This paradox of expertise may be further amplified for S&T threat assessment. Many of the highly technical topics of analytic interest today—rapidly evolving S&T like bio-, nano-, and information technologies—require much specialization for genuine expertise, further focusing the expert on one domain, or even a sub-domain, to the exclusion of others.

Assessment and Warning Processes Are Flawed

In addition to the difficulties inherent in S&T threat warning, the bifurcation of technical and human assessment, and the paradox of expertise, the assessment process itself is biased by incentives and rewards that tend to overstate developments—or warnings—at the expense of more sober and likely conclusions, directly impacting policy and decision-making. Whether in the private or public sector, analysts and forecasters typically are rewarded and incentivized to produce headlines (not footnotes)—and the more the better. Motivations vary but the results are similar: impacts are hyped; perspective is lost. For example, despite its common usage, Michael Hopkins and colleagues writing in 2007 have shown that empirical evidence does not support the existence of a biotech “revolution,” at least in the area of drug innovation.

Nor does the data support the widely held expectations that biotechnology is having a revolutionary impact on healthcare or economic development. The revolutionary model is therefore a misleading basis for policymaking as it over-estimates the speed and extent of any changes in productivity or the quality of therapeutics. Instead, the evidence suggests biotechnology is following a well-established incremental pattern of technological change and “creative accumulation” that builds upon, rather than disrupts, previous drug development heuristics.

Hopkins concludes his study by noting that the “hype” of a biotech revolution “...is an important part of the process of technological change itself. Shared expectations are needed to ensure the coordination of the large amounts of resources needed for major innovations.”¹⁷

17 M.M. Hopkins et al., “The myth of the biotech revolution: As assessment of technological, clinical and organizational change,” *Research Policy* 36, no. 4 (2007): 566–589. See also, Jon Guice, “Designing the future: the culture of new trends in science and technology,” *Research Policy* 28, no. 1 (1999): 81–98.

The key message...is that biotechnology is not being hyped because it is a revolutionary technology. If it were revolutionary there would be no need for hype, as people would be too busy making new medicines. Instead, it is being hyped precisely because it is not revolutionary, and shared expectations are needed to co-ordinate the long-term, incremental process of technological accumulation. As such the biotechnology revolution myth might be viewed as a rhetorical device employed to generate the necessary political, social, and financial capital to allow perceived promise to emerge.

Hype is not only an effective rhetorical device in the business of drug development, but has also proven effective in shaping government policy development and funding priorities. Susan Wright has shown how during U.S. President Clinton's administration, key players in the executive and legislative branches of the federal government and prominent individuals from scientific, biotechnology, policy, and media circles helped form a single view—the view that terrorists will use biological weapons—and how it "...came to dominate Washington politics and to justify opening the federal coffers to major new civilian biodefense programs."¹⁸ Wright asserts that "by the end of the Clinton administration, the claim that terrorists armed with biological weapons represented a huge threat to the security of the United States had achieved the status of received knowledge."^{19,20}

Both Hopkins and Wright warn of the negative impacts hype has on policymaking. Hopkins argues that using a "revolutionary" model to promote biotechnology is a "...misleading basis for policymaking as it over-estimates the speed and extent of any changes in productivity or the quality of therapeutics...The translation of advances in bioscience into new technology is far more difficult, costly and time-consuming than many policymakers believe."²¹ Wright explains the views of at least one senior intelligence official that ran contrary to the "received knowledge" of bioterrorism (as part of a general concern about terrorists with chemical, biological, radiological, or nuclear weapons—WMD) and questioned the wisdom of a focus on such an extreme case at the expense of "...other,

18 Susan Wright, "Terrorists and biological weapons: Forging the linkage in the Clinton Administration." *Politics and the Life Sciences* 25, no. 1–2 (2006): 59.

19 Ibid., 57.

20 Over time, hype can inform development of narratives and myth, generally unquestioned and accepted as given fact with powerful impacts. Myth used in a classical sense "...of a story or other narrative that attempts [to] explain the unknown in a fashion understandable with the culture seeking this understanding," as Paul Douglas Humphries defines in his excellent examination of the power of narrative and myth in national security. Paul Douglas Humphries, (2014). "The War on Terror in Postmodern Memory: Explanation, Understanding, and Myth in the Wake of 9/11," (Doctoral thesis). Retrieved from Georgetown University Institutional Repository.

21 Hopkins et al., "The myth of the biotech revolution," 1, 2 (2007).

more likely threats.” This official believed the “...WMD terminology contained an inherent bias that hyped the idea of terrorism with WMDs,”^{22,23}

[H]e held that the emphasis...“skewed priorities and misdirected resources within counterterrorism. Appropriating more money for initiatives aimed narrowly at a chemical or biological threat, especially the worst case scenario of a mass casualty attack, may mean less money for efforts that combat terrorism in general (and that could save more lives).” And this had a pronounced impact on the way counterterrorism policy was implemented: “[With respect to] emergency preparedness, exercises, that sort of thing—just about any scenario ... involving the military, the FBI, police departments—it was always a chemical or biological exercise, never a conventional kind of thing.”

The U.S. government’s approach to cybersecurity may be the most recent example of hype driving attention and resources away from much more likely threats with proven consequences. In June 2015, the Office of Personnel and Management (OPM) announced that its information network had been breached by suspected Chinese hackers, with some reports suggesting connections to the Chinese government. Officials have estimated that the personnel records of 21.5 million people were compromised, including personal information used for sensitive national-security background checks. But with the U.S. Government Accountability Office designating federal information security as a “government-wide high-risk area” for almost 20 years²⁴ and the U.S. intelligence community *publicly* warning that cybersecurity was among the top threats confronting the U.S. government for at least the past five years,²⁵ why was such sensitive information about so many people apparently so easy to acquire by simply hacking OPM’s network?

At least one observer believes that the somewhat extravagant promotion of cyber threat is to blame. Adam Elkus writes of what he calls an “illusory cybersecurity paradox.”²⁶

22 Wright, “Terrorists and Biological Weapons,” 87 (2006). Also see, “The Experience of the Japanese Aum Shinrikyo Group and Biological Agents,” in *Hype or Reality? The “New Terrorism” and Mass Casualty Attacks*, ed. Brad Roberts (Alexandria, VA: Chemical and Biological Arms Control Institute, 2000), 159–168.

23 Ibid.

24 United States Government Accountability Office, “Federal Information Security: Actions Needed to Address Challenges,” testimony before the President’s Commission on Enhancing National Cybersecurity by Gregory C. Wilshusen, September 19, 2016.

25 See James R. Clapper, Director of National Intelligence, “Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence,” February 10, 2011.

26 Adam Elkus, “The devastating breach of U.S. government data highlights an illusory cybersecurity paradox,” *Business Insider*, June 18, 2015.

Why is cybersecurity simultaneously so hot and yet so devastatingly neglected? Despite the immense amount of energy and activity that we pour into understanding the nature of cybersecurity and cyberpower more broadly, we persist in ignoring boring but immensely consequential flaws in our information architecture. The longer we refuse to examine real cyber threats rather than fantasies of super-hackers and apocalyptic scenarios of cyber-doom, the more vulnerable we become to hackers like those that carried out the OPM breach.

Elkus concludes that for government officials, it is easier to warn of a catastrophic “cyber Pearl Harbor” than actually dealing with “...the boring but necessary drudgery, for example, of modernizing a decrepit and decaying federal information technology base or ensuring that basic security protocols are observed.”²⁷ Mobilizing “against a myth” does not require the “harsh choices or sacrifices...In contrast, cleaning up the systematic dysfunction in OPM and other agencies [would] require a harsh and swift hand and plenty of pink slips... The longer that our government cyber-specialists chase the shadow of looming cyber-doom and ignore the festering wounds and gaping weaknesses in its own information architecture, the more that something genuinely cyber-catastrophic occurring becomes a self-fulfilling prophecy.”²⁸

Ignoring the more mundane for the more compelling story is not unique to threat assessment. Sociologist Wayne Brekhus has argued that “...the extraordinary draws disproportionate theoretical attention from [social science] researchers...ultimately [hindering] theory development and [distorting] our picture of social reality.”²⁹ Brekhus explains that by focusing on certain things while ignoring others—the “marked” versus the “unmarked”—actors will attend to and thus “mark” those items leaving “unmarked” the ignored ones. This marked–unmarked relationship has five basic properties that perpetuate stereotypical thinking.

1. The marked is heavily articulated while the unmarked remains unarticulated.
2. The marking process exaggerates the importance and distinctiveness of the marked.
3. The marked receives disproportionate attention relative to its size or frequency, while the unmarked is rarely attended to even though it is usually greater.
4. Distinctions within the marked tend to be ignored, making it appear more homogenous than the unmarked.
5. Characteristics of a marked member are generalized to all members of the marked

27 Ibid.

28 Ibid.

29 Wayne Brekhus, “A Mundane Manifesto,” *Journal of Mundane Behavior* 1, no. 1 (February 2000): 89.

category but never beyond the category, while attributes of an unmarked member are either perceived as idiosyncratic to the individual or universal to the human condition.

Brekhus argues that the problem for social science is that all of these properties are “accentuated and reproduced” in research. “Although many specific studies, by themselves, are not inherently a problem, the cumulative effect of numerous studies focusing on the marked is to reproduce a stereotypical and extreme rather than accurate picture of social reality.”³⁰

Within the professional ranks of intelligence analysts, ignoring the more mundane for more compelling potential threats is commonplace and, at a minimum, a result of the rewards and incentives environment. National-level intelligence analysts (like those at Central Intelligence Agency) are incentivized to produce products that reach senior government officials; mundane findings are not likely to meet dissemination threshold and reach top government officials. Quantity matters too—the more the better. Johnston described the impact the focus on getting to senior officials has had on analytic work and intelligence analysis.

A key finding of his ethnographic study of the intelligence community’s analytic culture is that analysts see promotion opportunities directly tied “...to the number of daily products they generate and the amount of social capital or direct consumer influence they amass, most often when their work is recognized by senior policymakers.”³¹ The cumulative effect Brekhus warns of is almost certainly present. Moreover, the press to produce daily products (mostly defined as “current intelligence”) leaves analysts little time—or incentive—for longer-term, more in-depth research and analysis through which they would develop their own specific expertise, question the existing analytic line, and contribute to the community’s knowledge base.³² Consequently, many feel they are just “reporters”³³ rather than experts whose analytic judgment is respected and heard. With a nod to Brekhus, reporters do not write mundane headlines if they want to get published and read.

Similar biases persist in the world of scientific research, of which published results often directly impact national security S&T threat assessments. Scientific researchers need to publish impressive results in prestigious peer-reviewed journals and be cited by other researchers to have the impact that is critical to a progressively successful career. Even

30 Ibid, 92.

31 Johnston, *Analytic Culture in the U.S. Intelligence Community*, (2005), 16–17.

32 As part of the Director of Central Intelligence directed assessment of the intelligence produced before the war in Iraq, Former Deputy Director of Central Intelligence Richard J. Kerr concluded, “The fast-paced world of current intelligence leaves little time for careful examination of assumptions, alternatives to accepted lines of analysis, or discussion of sources and evidence. Moreover, quick, rapid-fire responses to policymaker queries often give the impression of certitude about analysis and sources that discourages thoughtful examination of the analytic line. This was one of the chief problems evidenced in the examination of the analysis on Iraq.” See Richard J. Kerr, et. al., “A Holistic Vision for the Analytic Unit,” *Studies in Intelligence*, unclassified edition, 50, no. 2 (2006).

33 Ibid, 27.

tenured researchers have to secure research funding, a highly competitive proposition and one heavily dependent on previously published work. Publish or perish. And what typically gets published in these journals is “positive findings,” results that back a particular study’s hypothesis. Negative findings typically are not of interest. As journalist David Freedman explains, “This leaning toward studies with positive results is known as ‘publication bias,’ and researchers are so resigned to it that they typically don’t even bother to submit for publication studies with negative results...”³⁴ Freedman describes how this environment leads to an interesting proposition:³⁵

So researchers are pressured to come up with study results that are both interesting and positive. But [John] Ioannidis, among many others, is quick to note a problem: the more surprising, novel, and exciting an idea, the less likely it is to be right. An idea that seems highly likely to be true, that is utterly plausible, is probably not going to seem exciting—it’s the implausibility that often provides most of the novelty and enthusiasm.

Other researchers describe this phenomenon as “scientific regress”³⁶ or an “inevitable evolution of bad science” and conclude that without “changing incentives across the complex science ecosystem,” there will be no effective change. This system includes “[i]nstitutions, funders, editors, societies, and researchers themselves...”³⁷ This “evolution,” that is scientists passing along these “successful” practices to students they train, results “[o]ver time [in] the very culture of science [being] sculpted by natural selection.”³⁸

Curious Incidents?

So it would seem the lack of expected attacks utilizing advanced S&T—as forecasted by analysts incentivized to not miss a potential threat and rewarded for calling out the possibility of high impact attacks—is not so curious after all. In the context of such an assessment environment, what can we conclude about the threats to civilian populations from BW and MANPADS? First, threat narratives that stress the ease of acquisition and use, along with the near-catastrophic impact potential, neglect to objectively examine the critical—and central—role the people who would use such weapons play. As discussed

34 David H. Freedman, *Wrong* (New York, NY: Little, Brown and Company, 2010), 110–111.

35 *Ibid.*, 111.

36 William A. Wilson, “Scientific Regress,” *First Things*, May 2016, accessed October 12, 2016, <https://www.firstthings.com/article/2016/05/scientific-regress>.

37 Ed Yong, “The Inevitable Evolution of Bad Science,” *The Atlantic*, September 21, 2016, accessed October 11, 2016, <http://www.theatlantic.com/science/archive/2016/09/the-inevitable-evolution-of-bad-science/500609>.

38 *Ibid.*

earlier, and as we continue to see, rare is an assessment of threats from S&T that includes much discussion on who may actually make the decision, commitment, and expend significant effort and resources to actually acquire and successfully employ these technologies.

In his analysis on the potential for WMD terrorism not long after the 9/11 terrorist attacks, John Parachini offered a more balanced perspective. Parachini concluded in 2003³⁹ that the “evidence” of genuine terrorist interest in and commitment to WMD (to include BW) was sparse and “...several of the empirical cases frequently cited in the media and scholarly literature proved to be apocryphal.”⁴⁰ In his investigation, Parachini offered a conceptual framework for assessment of terrorist WMD threats with a clear emphasis on specific adversaries, not the technology.

Mindset of group leaders: Are leaders of a group predisposed to certain impacts or effects that can only be delivered by unconventional weaponry, such as BW? Parachini cites the cases of Aum Shinrikyo, Larry Wayne Harris, James Dalton Bell, and Masumi Hiyashi as examples of “...individuals [who] harbored a fascination with poison and disease.”⁴¹

Opportunities: Do threat actors seize an opportunity to use an unconventional weapon not out of some ideological motivation but because it was available and met an immediate need? Parachini cites the Tamil Tigers’ use of chlorine against government forces in 1990 as such an example. Moreover, “Aum Shinrikyo, Al Qaeda, and the Tamil Tigers all operated in permissive environments, where they could utilize the power of unconventional weapons without much interference from their host state.”⁴²

Technical hurdles: Simply put, “Only in a very few cases have groups been able to amass the skills, knowledge, material, and equipment to perpetrate attacks with unconventional weapons on a scale that comes close to that of the danger posed by terrorist attacks with conventional explosives.” One of those groups was Aum Shinrikyo and, as Parachini observes, it “...failed in all 10 of its biological weapons attacks.”⁴³

Similarly, human factors drive a group to select MANPADS to attack civilian aviation and not the weapon technology itself. As part of a workshop convened to investigate why some predicted S&T threats have not manifested with impacts to international security as forecasted, an expert participant said that many factors must each be satisfied for

39 It is safe to say that in 2003 offering a more skeptical assessment of potential terrorist threats was a clear minority viewpoint. Also, for a balanced perspective shortly before 9/11, see Brad Roberts, editor, *Hype or Reality? The 'New Terrorism' and Mass Casualty Attacks* (Alexandria, VA: Chemical and Biological Arms Control Institute, 2000).

40 John Parachini, “Putting WMD Terrorism into Perspective,” *The Washington Quarterly*, Autumn 2003, 41.

41 Parachini, 43.

42 Ibid, 44.

43 Ibid, 45.

an individual or group to successfully employ MANPADS. Consistent with Parachini's framework, this expert asserted that:⁴⁴

These factors include adversary group preferences and beliefs, ability to recruit operatives and deliver weapons to an appropriate attack site, and ensuring the functionality of the weapon. Emphasis was placed on assessment of each actor individually, to comprehend the decision-making processes that lead groups to choose MANPADS to attack an aircraft as opposed to suicide bombs or cargo bombs inside the aircraft. These decisions do not take place in a vacuum, and individual factors as well as news coverage and political environment may all weigh on the preferences and motives of an individual group.

Key leadership decisions would include: does a mass casualty attack meet group objectives? Is aviation preferred over other mass casualty targets? Is there an appropriate aviation target accessible, such as U.S.-flagged, VIP transport? Does the group have high confidence in the effectiveness and reliability of a particular weapon? Further considerations include: does the group have the capacity to employ MANPADS? Can it recruit and train operatives effectively? Select appropriate attack sites with target access consistent with weapon-operational requirements? Can it deliver weapons to operators at an appropriate attack site? Can the group withstand Western and host-nation military, counterterrorism, and law enforcement pressures? And finally, once the decision has been made to use MANPADS, does the group have or can it acquire MANPADS? Is the weapon complete and functional?⁴⁵

What Can Be Done?

Brian Jenkins neatly summed up the problem with threat warnings years before the current state of worry about the dangers from S&T. "Threat Assessment based on infinite vulnerabilities, conjured foes, worst-case scenarios, and the wrath of our children can degenerate into a fact-free scaffold of anxieties and arguments—dramatic, emotionally

44 Center for Global Security Research, "Dogs That Haven't Barked: Towards an Understanding of the Absence of Expected Technological Threats," (Livermore, CA: Lawrence Livermore National Laboratory, July 2016), 8.

45 Author conversation with workshop participant, July 7, 2016.

powerful, compelling, but analytically feeble.”⁴⁶ This analytic feebleness really does seem to be why many so-called threats from S&T simply are not as warned. Until significant changes are made by the organizations that employ the people who produce threat assessments and warnings, it is highly likely that assessment of S&T threats will continue to warn early and often with misleading results. Analysts are likely to continue to underestimate the technical difficulties, overestimate the interest and commitment of adversaries to technology and our vulnerabilities to it, remain blind to (or at least continue to ignore) known analytic biases, and respond to incentives for early warning of speculative threats by producing more assessments with the cumulative effect of warnings that distort reality for decision-makers, likely leading to bad policymaking—if they listen at all!

What is required in order to improve analysis and the qualities and performance of the people who conduct it is well known but difficult to accomplish. Numerous assessments and studies have been conducted—typically in the wake of some analytic or warning “failure”—over decades by esteemed government officials, academics, and experienced practitioners.⁴⁷ Many offer very consistent guidance for improvement and require significant changes in culture, practices, rewards and incentives, recruitment and development, management, and consumer expectations. And therein lies the rub. It will remain easier and bureaucratically and politically safer to continue to warn misleadingly than to address the underlying assessment shortcomings. Writing of needed intelligence reforms, Robert Jervis concluded:⁴⁸

The reforms I have discussed are feasible. But they are not cheap and will not eradicate intelligence failures. They are in the nature of investments and call for putting resources, time, and energy into the reforms. This would require sustained commitment throughout the IC, starting with its top leaders. Unfortunately this may not be forthcoming. Inducing new ways of thinking and interacting will be disruptive, the tasks are undramatic, and the benefits are uncertain and delayed. Logic and the history of the IC (and other organizations) give few grounds for optimism.

46 Brian Jenkins, April 1999. As quoted by Susan Wright in “Terrorists and biological weapons: Forging the linkage in the Clinton Administration.” *Politics and the Life Sciences* 25, no. 1–2 (2006). Jenkins offered a more complete assessment in his testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform, October 20, 1999: “Today’s risk assessments begin with identifying vulnerabilities, positing a foe, and creating a hypothetical scenario. While perfectly legitimate, this approach entails some analytical risks. One problem is that vulnerabilities are infinite in modern society; hypothetical foes can easily be conjured, and the scenarios are invariably worst cases. This creates another analytical problem. Since risk equals the probability of an event times its consequences, focusing on only the most horrendous events overwhelms any estimate of their likelihood. The possibility of occurrence becomes irrelevant unless the threat can be dismissed with a high degree of confidence which, of course, it cannot.”

47 More recent studies include *National Research Council, Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences*, Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security, Board on Behavioral, Cognitive, and Sensory Sciences, Division of Behavioral and Social Sciences and Education. (Washington, DC: The National Academies Press, 2011); Jeffrey R. Cooper, “Curing Analytic Pathologies,” Center for the Study of Intelligence, December 2005. See also Jeffrey M. Bale and Gary Ackerman, “Recommendations on the Development of Methodologies and Attributes for Assessing Terrorist Threats of WMD Terrorism,” Center for Nonproliferation Studies, Monterey Institute of International Studies, undated.

48 Jervis, *Why Intelligence Fails* (2010), 196.

While it may be difficult to argue with Jervis's realism, the current state of the S&T threat assessment environment is such that without some improvement, there will continue to be more and more concerns about emerging and evolving S&T added to a growing list of threats. Artificial intelligence, additive manufacturing, genetic engineering, directed energy, and many others already are topics of concern—and warning—along with the many legacy threats, like BW and MANPADS. Clearly this situation does nothing to improve national security decision-making and, in fact, is likely to degrade it by overwhelming decision-makers with an increasing number and expanding array of threats. Not to mention the negative impacts on limited collection and analysis resources.

So what, then, can be done practically? There are very real limits on improvement. Even at its best, threat warning will never be perfect. As a former Assistant Director of Central Intelligence for Analysis and Production put it, threat assessment is “... analysis—not clairvoyance. Our intelligence analysis may be as good as it gets.”⁴⁹ But of course there are always things that can be done to improve, even if only incrementally. As mentioned earlier, improving intelligence analysis has been a topic of study for decades. Recommendations on improving quality and rigor of the analytic discipline, to include using more of the methodologies of the social sciences, have been generally consistent and recognized as difficult to implement.

But with leadership commitment and investment of resources, time, and energy, incremental improvements will be gained and those likely will have significant impacts over time. Within the U.S. intelligence community there have been efforts to make structural and methodological improvements. In the immediate aftermath of the 9/11 terrorist attacks, the CIA established the Red Cell, an analytic team set up specifically to provide national leadership alternative analysis “...to challenge conventional wisdom in the intelligence community and mitigate the threat of additional surprises...”⁵⁰ Intelligence agencies maintain professional schools with intelligence-analysis curricula.⁵¹ Most recently the Office of the Director of National Intelligence has established a partnership with the National Academies of Sciences, Engineering, and Medicine with the goal that the new relationship will “...help the intelligence community improve how it collects and analyzes information ...[along with] help picking out useful and relevant research, as well as grasping where there is a lack of good science.”⁵²

49 Mark Lowenthal and Ronald Marks, “Is U.S. Intelligence Analysis as Good as it Gets?” *War on the Rocks*, accessed October 23, 2015, <http://warontherocks.com/2015/10/is-u-s-intelligence-analysis-as-good-as-it-gets/>.

50 Micah Zenko, “Inside the CIA Red Cell,” *Foreign Policy*, October 30, 2015, accessed October 27, 2016, <http://foreignpolicy.com/2015/10/30/inside-the-cia-red-cell-micah-zenko-red-team-intelligence/>.

51 For example, The Sherman Kent School for Intelligence Analysis at CIA; Director of National Intelligence's National Intelligence University (managed by the Defense Intelligence Agency).

52 Jeffrey Mervis, “Spy agencies team up with National Academies,” *Science*, October 12, 2016, accessed October 27, 2016, <http://www.sciencemag.org/news/2016/10/spy-agencies-team-national-academies>.

And in the scientific community there are moves to directly address the issue of publication bias, with many journals now publishing “Registered Reports.” These published reports are a result of a “...system of ‘pre-registration,’ where work is evaluated on the back of [the] ideas and plans, before any actual work is carried out. [The scientists] commit to carry out the plans to the letter, and journals commit to publishing the results come what may, [reducing] the capacity and incentive to mess with studies to boost one’s odds of getting a paper [published]. It also moves the focus away from eye-catching results ... towards solid, reliable methods.”⁵³

Despite its flaws, the oft-used “batting average”⁵⁴ metaphor for intelligence analysis may indeed be most appropriate in considering the value of devoting sustained management attention to an enduring effort to improve the quality of analytic methodology, technique, discipline, and culture. Consistently making even incremental improvements in the practice of analysis will pay dividends over time. These improvements must be of the fundamental nature these earlier groups have called for and not just organizational structural changes. As Jervis rightly observed, genuine substantive improvement will require sustained commitment, beginning with leadership that can incentivize, reward, and further nurture the skills and practices required for more accurate threat assessment. National security decision-makers should expect no less.

53 Yong, “The Inevitable Evolution of Bad Science,” 2016.

54 See Stephen Marrin, “Evaluating the Quality of Intelligence Analysis: By What (Mis) Measure?” *Intelligence and National Security* 27, no. 6 (2012); Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (Columbia University Press, 2007); and Jeffrey A. Friedman and Richard Zeckhauser “Why Assessing Estimative Accuracy is Feasible and Desirable,” *Intelligence and National Security* 31, no. 2 (2016): 178–200.

Chapter 4

Emerging Trends in Big Data and Artificial Intelligence: Directions for the Intelligence Community

James Canton

Emerging trends in information technology come at an important time given the complexity of the national security landscape, the geopolitical environment, and the myriad global threats facing the United States. The U.S. is embedded within a milieu of global change that is punctuated by terrorist plots, information warfare, state and non-state cyberattacks—factors that all complicate the job of national intelligence.¹ The complexity of these national security challenges renders many current methods and information technology tools inadequate. To cope with this multifaceted and rapidly changing environment, the U.S. intelligence community (IC) must be at the forefront of understanding, developing, harnessing and integrating the next generation of information technology innovations. In particular, new tools for utilizing big data and artificial intelligence are becoming essential to ensuring the IC's priority goal of avoiding strategic surprise.²

This chapter examines big data and artificial intelligence (AI), two emerging information technology tools that have the potential to influence significantly, if not transform, the IC.³ The future implications of combining big data and AI to intelligence operations offers the potential to accelerate the agility of the IC well beyond the capabilities afforded by currently available information technology. The combination of these two innovations can improve situational awareness, and get the right information to the right people at the right time

1 M.A. Goodman, "9/11: The Failure of Strategic Intelligence." *Intelligence and National Security* 18, no. 4 (2003): 59–71.

2 K. Lim, "Big data and strategic intelligence." *Intelligence and National Security* 31, no. 4 (2016): 619–635.

3 Cortney Weinbaum, "The Ethics of Artificial Intelligence in Intelligence Agencies," *Rand Blog*, last accessed October 27, 2017, <http://www.rand.org/blog/2016/07/the-ethics-of-artificial-intelligence-in-intelligence.html>.

to help them make more informed decisions. The new information tools give operators massive reach-back and predictive capability to assess rapidly changing situations.⁴

Although most of the applications referred to here are from the private sector, where many of the largest AI and big data investments and talent are concentrated, the implications for the intelligence community are similar in many ways. Competition among adversaries is intense. Superiority and the projection of influence and power are accelerated by innovative new technologies. As with a number of other innovations such as virtual reality, next-generation computing, synthetic biology, and genetics, the private sector has made the largest investments, but the government can gain access to those investments through public-private partnerships with leading technology innovators. Imagine a force of AI tools: virtual analysts, digital agents, software bots operating throughout the globe, computer networks, drones, robots with decision technologies that sense, analyze, predict, and interdict threats in real-time—all active in the steady state, long before a crisis.

To make the most of these technical innovations will require equally bold innovations in how the IC does business. Now is the time to prepare for this eventuality, as AI and big data advances demonstrate outcomes that are growing and provide a clear value proposition.

From AI to Deep Learning: The Evolution of Thinking Machines

Defining AI

In this chapter, AI refers to the development and use of computers and networks that mimic human learning, reasoning and sensing capabilities. AI encompasses cognitive capabilities that draw from cars, robots, factories, hospitals, airplanes, ships, drones, and weapon systems.⁵ The speed of AI and automated analysis outpaces humans today in deployed systems for finance, manufacturing, and telecommunications. High-speed trading by software bots or programs moves faster than humans and trades billions of global financial assets daily in nanoseconds. AI that uses cognitive software may enable or capture visual, auditory, olfactory, motor, and geolocational sensing data. AI is already used in machine-to-machine communications and industrial controls that run much of the financial, telecommunications, and Internet infrastructure around the world.

On the broadest level, AI machines and their programs are learning to reason, embrace an early stage of cognitive capacities to process data, and enable decision-making. These characteristics enable the analysis of massive data sets, revealing future trends and patterns, and yielding predictive insights. Such insights can then be applied to achieve desired outcomes—or prevent unwanted ones. More specifically, experts define two types

4 N. Hare, and P. Coghill, “The Future of the Intelligence Analysis Task,” *Intelligence and National Security* 31, no. 6 (2016): 858–870.

5 P.R. Cohen, and E.A. Feigenbaum, *The Handbook of Artificial Intelligence* (Stanford, CA: HeurisTech Press, 2014).

of AI: narrow and strong AI. Narrow AI applications are designed to be limited to specific tasks that do not have the full range of human cognitive or learning capacities. Strong AI or general intelligence is envisioned as having in the future equal, if not superior, cognitive capacities to humans.

In the private sector, AI is fast becoming an important business tool for increasing competitive advantage, creating new products, and understanding the customer, and in formulating and executing business strategy. The automation of human decision-making and decision support for humans, especially predictive analysis, is an emerging use case for organizations using AI to gain a competitive advantage. The analysis of data by the use of AI is yielding new insights into both known and previously unknown problems. These applications are occurring in a wide array of domains, from finance and logistics to medicine.⁶

Moving forward, the capacity to develop foresight, embed cognitive capacities of human-like reasoning to make smarter decisions and analyze information is poised to increase exponentially.⁷ AI systems, especially those that execute deep learning, get smarter over time given their capacity to engage trial and error cognition; moreover, by digesting data, the AI can establish proof sets to validate its own effectiveness. Self-learning machines are being used to improve the decisions that they offer to their human operators. Soon, cloud-based AI will be pervasive via mobile apps and cloud computing, with access to infinite amounts of data to advise human decision-making.⁸

Development and Examples of AI

One relatively early example of AI capabilities in accessing and analyzing billions of data sets is the use of these technologies in research studies, trials, and patient care, which has led to a revolution in health care. Cancer research and treatment has been a proving ground for accelerated self-learning machines, as the answers lie in massive data sets that humans could not possibly process. AI systems can read and analyze 30 billion documents in three months—faster than any number of humans could do in a lifetime.⁹

In the past few years, AI has developed more rapidly, and in ways that are fundamentally different from its inception. Indeed, decades passed in which experts made little progress on AI. Previously, rules-based expert systems, fuzzy logic, and natural language processing characterized AI; for the most part, these AI systems were not very “smart.” But while the

6 H. Chen, R.H.L. Chang, and V.C. Storey, “Business intelligence and analytics: From big data to big impact,” *MIS Quarterly* 36, no. 4 (2012): 1165–1188.

7 Joel Garcia, “Machine Learning and Cognitive Systems: The Next Evolution of Enterprise Intelligence (Part I),” *Wired*, last accessed October 27, 2017, <https://www.wired.com/insights/2014/07/machine-learning-cognitive-systems-next-evolution-enterprise-intelligence-part/>.

8 K. Ayoub, K., K. Payne, K., “Strategy in the Age of Artificial Intelligence.” *Journal of Strategic Studies*, 39, no. 5–6 (2016): 793–819.

9 “Oncology and Genomics,” *IBM Watson Health*, last accessed October 27, 2017, <https://www.ibm.com/watson/health/oncology/>.

history of AI has been long, and rather slow in innovation, it now has new direction and momentum. Breakthroughs started to occur after people began trying new approaches to AI, including machine learning, deep learning, and neural networks. When used in combination, these advances enabled computers to recognize, learn, and adapt the way living things do.¹⁰

The Defense Advanced Research Project Agency's (DARPA's) Synapse project was seminal as an early effort to support a group of computer companies (IBM, Qualcomm, and Hewlett-Packard) to investigate neural networks, or microchip architectures that were based on brain cells. This project was one of the key developments that led to harnessing AI and making it more of a deliverable that business could eventually develop and apply in specific, but ever broadening, applications.

Microsoft's Oxford, Google's DeepMind, Baidu's Minwa, Amazon's Alexa, and Apple's Siri are examples of multi-billion-dollar investments in AI that are still in the early stages of development and deployment. AI that depends on machine intelligence, machine learning, and natural language processing has an infinite capacity to adapt, learn, and evolve; these qualities distinguish it from earlier efforts in AI that were limited to rule-based technology, and did not offer the performance, scale, or capacities of this current technology.

Minwa is a large data-crunching, image-recognition AI engine with a 36-server platform, 6.9 terabytes of host memory and a 0.9 petaflop peak performance. (It is likely that this platform has been enhanced since this chapter was last reviewed.) Produced by Baidu, Minwa is their AI project that when combined with their commercial reach in the Chinese economy may rival AI efforts at Google and Amazon. Minwa is made up of over 72 processors and 144 graphics processors.

Google DeepMind combines machine learning and the pursuit of neuroscience as a model for accelerating decision-making of their bot technology as it streams across the web. Reading a billion emails and mining transactions allows Google to remind you to pick up your kids, when that game is now available on live streaming video, and much more. As Google owns Nest, the home energy and security system, and is rolling out Google Home (another talking AI like Amazon's Alexa), the potential is great for Google to dominate the next-generation web environment. The idea of creating a big data, analytics, and AI ecosystem for Google is a logical extension of what Google is planning. Google has been building the best general-purpose learning algorithms in the industry—the potential for Google's use of AI could outpace other competitive efforts, given that they own in excess of 80% of the global online search business.¹¹

10 Will Knight, "5 Big Predictions for Artificial Intelligence in 2017," *Technology Review*, last accessed October 17, 2017, <https://www.technologyreview.com/s/603216/5-big-predictions-for-artificial-intelligence-in-2017/>.

11 "Machine Intelligence," *Research at Google*, last accessed October 27, 2017, <https://research.google.com/pubs/MachineIntelligence.html>.

IBM's Watson processes over 500 gigabytes, or the equivalent of 1 million books, every second, and it is growing. As Watson becomes a cloud-based AI, it can be expected that petabyte analysis can be exponentially increased by 100 times by 2020 or before. Watson is a first-generation cognitive computer that offers the largest thinking platform yet deployed by any organization. IBM invested \$1 billion to employ the Watson business unit to focus on big global challenges. Watson's combination of AI and big data technologies is producing significant early-stage results. Health care is just one focus. IBM has built an Oncology Advisor that is doing both diagnostics and treatments of certain cancers. The Memorial Sloan Kettering Cancer Center (NY) and the MD Anderson Cancer Treatment Center (TX) are early adopters of this innovation. Watson will next move on to meeting challenges in finance, manufacturing, retail, and other markets.

Project Oxford is Microsoft's investment in the world of AI and deep learning. Although somewhat late to the industry, and having lost the desktop market to Facebook (another big AI investor), Oxford is engaged in several key areas, including image, facial, text, and speech recognition. Microsoft hopes to integrate the technology into its computer operating systems and smartphone software. The recent pivot is to offer self-service application programming interfaces (APIs), basically software programs that can be plugged into applications for enabling AI development, using mostly machine learning to do things that humans used to do. This should enable the AI industry to use Oxford to develop apps and programs for various commercial uses.

Amazon's Alexa is a personal assistant, similar to Siri, that engages with consumers to research, search, and buy. The Echo or Dot is a \$33 plug-in device that awakens to your voice. Alexa is also a general-purpose AI that plays music, geo-locates information, and solves problems by searching the web, based on consumer voice control. Numerous companies (e.g., IBM's Blue Mix) have adopted this approach, offering plug-and-play, easy to cut-and-paste programming APIs to fuel the reasoning capacities for running analytics, big data, and prediction for health care, finance, manufacturing, and many other industries. This self-service approach to enabling big data and AI applications will accelerate the proliferation of inexpensive, fast, and agile new innovations.

In the near future, we will see AI programming AI. This development will be a watershed in the advancement of computer science: machine intelligence that designs other platforms, and has the cognitive awareness and reasoning ability to make things operate in ways that are "smarter." This is the future of programming—AI that enables humans and operates autonomously to invent, alter, program, and design the next generation of technology. AI will be used to create new tools that will transform every industry.¹²

12 Y. Gil et al., "Amplify scientific discovery with artificial intelligence," *Science*, 346, no. 6206 (2014): 171–172.

Connections to the IC

These new developments differ from prior iterations of AI, the drivers of which were rules-based systems that did not scale and missed key insight opportunities. Today, thinking systems that learn are everywhere in our society, including things like voicemail, robots, stock trading bots, personal authentication software, and self-driving cars. AI reads our x-rays, determines who gets into college, who gets hired or insured, and who runs much of the communications, Internet, electronic commerce, and asset trading conducted on the planet today.¹³ AI is incorporated into the software that runs the chips that companies such as Tesla use to enable their self-driving cars—far in advance of regulations being fully defined or in place to guide and govern the effects and implications of such technology. The IC may be in a similar position.

The tools that AI leaders are currently developing will enable human operators to gain advantages to see the unseen, even reveal the future. Data artifacts—video, email, voice, geolocation, social media, transportation, sensors—all tell a story that we need to understand and use to build predictive forecasts. We currently produce more data in ten minutes than we did in all of human history up to year 2000.¹⁴ Today we measure data by zettabytes—that is, a billion terabytes.¹⁵ The Internet of Things (IoT) network that processes, distributes, broadcasts, and collects big data will require increasingly advanced AI. Even the network nodes, chips, sensors, and software that will run IoT networks via the cloud will be AI-enabled; in fact, this is already happening, as machine-to-machine (M2M) communications evolve.

We are in the early stage of the Global Connectivity Revolution that is creating disruption and changes to the private sector, consumers, and governments. There is an important window of opportunity for leaders to move with agility to embrace and understand the implications of a globally connected citizenry, workforce, and threat environment. The Global Connectivity Revolution will uproot every aspect of the way markets work, people exchange currencies, businesses operate, and governments engage—and big data and AI will be the central drivers of change.

This co-evolution of a system in which AI and humans cooperate in a world of billions of gigabytes of data per minute, generated from multiple domains, demands a rethinking of the profession of intelligence. So much data requires a new type of intelligence analytics that currently seems to be in the early stages of definition and deployment.

13 H. Chen, R.H.L. Chang, and V.C. Storey, "Business intelligence and analytics: From big data to big impact," *MIS Quarterly* 36, no. 4 (2012): 1165–1188.

14 MG Siegler, "Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003," *Tech Crunch*, last accessed October 27, 2017, <https://techcrunch.com/2010/08/04/schmidt-data/>; "Data, Data Everywhere," *Economist*, last accessed October 27, 2017, <http://www.economist.com/node/15557443>.

15 "The Zettabyte Era Officially Begins (How Much is That?)" *Cisco Blogs*, last accessed October 27, 2017, <http://blogs.cisco.com/sp/the-zettabyte-era-officially-begins-how-much-is-that>.

The Big in Big Data

Big data refers to the increasingly large amounts of information, and increasingly larger data sets, that our interactions with the world produce, including: video, images, email, geolocation and sensing data. Big data also refers to predictive analytics, or the processing of large amounts of data to extract meaning, to address a mission or a purpose.¹⁶ Big data collection, storage, simulation, analysis, and prediction has become recognized for its increased strategic value worldwide in the private sector and in government. The global penetration and proliferation of the Internet and the connectivity of mobile, cheap, powerful devices has accelerated the generation of big data.

There are three types, or phases, of data that are available for utilization. The first phase is legacy data, which is historical data; it is reflective of past occurrences that can be collected and analyzed. The second phase includes real-time transaction analysis, such as that occurring each moment of each day. The third phase is predictive data analysis, which results from the collection and analysis of multiple data sets determined by the task at hand, or even combines legacy with real-time to gain a forecast of the emerging future. AI works on that data to produce patterns that suggest future behaviors or forecasts of events and probable outcomes.

These large data sets have brought insights from massive populations where the aggregate data from online communications, transactions, and interactions can be captured, analyzed, and even forecasted to gain insights into users. Virtually every company's business model has been updated to include big data and AI, and to consider developing new business models based on these innovations. Given the upside business potential, banking, pharmaceuticals, retail, media, consumer goods, hospitality, and manufacturing are leading the charge in integrating big data and AI.

As one primary example, new GPS data have prompted new questions about the health of the population based on big data analysis of living in certain geographic target states. Big data on public health can identify the populations in particular U.S. states that will be most at risk for diabetes and heart attacks. These geo-medical maps show the clustering of risk factors for living in the south and southeast of the U.S.¹⁷ Future big data insights may lead to understanding why certain dietary lifestyles, health care uses, population behavior, and even weather may be predictive of risk for various diseases in certain geographies. Before these data were available, experts examined the entire U.S. population based on age and gender, but not geography.

In the sciences, analysis of petabytes of data about genomics, agriculture, and ecosystems, which experts have never collected before or analyzed together, may yield discoveries

16 I. Emmanuel, and C. Stanier, (2016). "Defining Big Data," in *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies* (New York, NY: ACM, 2016).

17 Esri, "Geomedicine: Geography and Personal Health," by Bill Davenhall, August 2012.

that in the past were not possible.¹⁸ Doctors, researchers, and epidemiologists can better understand patterns of disease to work toward developing new methods of disease prevention. Big data image patterns can help us design cities for safety and sustainable growth. Big data can improve agricultural yields by analyzing soil, water, and atmospheric and plant genomics to improve yields.

The private sector is embracing big data as a way to develop a deeper understanding of what past behavior and predictive forecasts could accelerate business productivity. But more radical uses of big data are emerging. Businesses are formulating entirely new business models that challenge the traditional concepts of business. Uber, for example, is valued at close to \$50 billion and could not function without the data generated and analyzed over the Internet to produce real-time communication between its drivers and customers. Amazon depends on constant data analysis to power its retail web services 24/7, everywhere on the planet. Google's search engines formulate real-time predictive data aligned with your online search query behavior and can now mine billions of people's emails. Google, Amazon, Apple, Uber, eBay, and other companies have more access to more consumer information, transactions, communications, and behaviors than any government agency in the world.

Sources of Big Data Are Exploding

Where does all this data come from? Huge reserves can be found on the Dark Web, which is the uncharted and largely unknown part of the web thought to be much larger than the public Internet. It is the home of legacy data, outdated, forgotten and discarded from websites, old email, and everything that has occurred in cyberspace since its origins. Hackers, terrorists, and criminals often use the Dark Web to mask illicit activities like credit card fraud, illegal media, and drug and arms sales. The quantity of data found in the Dark Web may eclipse the known or public web by 100 times;¹⁹ these data are ripe for various actors to exploit.

Despite this copious data on the Dark Web, the most easily accessed sources of data derive from the day-to-day interactions that increasingly define modern life. A partial list of open source data includes the following:

- 1) Video streaming (applications, websites, conferencing, networks)
- 2) Social networks (Facebook, Twitter, LinkedIn, Baidu, WhatsApp)
- 3) Emails
- 4) Cloud computing storage and platforms (i.e., energy, financial, commercial, health care, transportation)
- 5) Internet of Things (routers, networks, sensors, chips, M2M, P2P)
- 6) Geospatial information (GPS, satellite, IP, geocached)

18 Y. Gil et al., "Amplify scientific discovery with artificial intelligence," *Science*, 346, no. 6206 (2014): 171–172.

19 The Data Team, "The data of the dark web," *Economist*, July 14, 2016, last accessed October 27, 2017, <http://www.economist.com/blogs/graphicdetail/2016/07/daily-chart-8>.

- 7) Video cameras (IP, private, satellite, commercial, public, private, security)
- 8) Videogames: mobile, online, network, and single player (game servers)
- 9) Apps: streams, stores, and networks
- 10) Dark web domains and dark networks (illicit online communities, auctions, exchanges, markets)
- 11) Industrial and manufacturing systems, local and networked
- 12) Financial transactions (banks, commercial, sovereign, individual)
- 13) Telecommunications user transactions (VoIP, P2P, M2M)
- 14) Search engine usage (i.e., keywords, images, audio, video)
- 15) Telecommunications networks (IP, cellular, POT, satellite, mesh)
- 16) Mobile and online web chat and messaging information
- 17) Digital crypto-currency transactions (Bitcoin, Ethereum, P2P, P2M, M2M, mobile, online, offline, local device)
- 18) Health care information and transaction devices and networks (quantified self, commercial, personal fitness)
- 19) Mobile and internet image networks (storage, collaborative, cloud)
- 20) Cross-border sovereign and commercial transaction and information flows (air, sea, land supply chains, logistics, distribution networks)
- 21) Cloud storage networks for every government and industry
- 22) Media networks (entertainment, business, government, public)
- 23) Physical information storage (not digital, online or accessible by network)
- 24) Human genetic information databases
- 25) AIs (chatbots, trading algorithms, digital agents)

Future sources of exploitable data will likely include:

- 1) Space-based infrastructure data (celestial orbiting cities, off-world cities, satellites, habitats, planetary instillations, ships, energy, communications)
- 2) Full visual-spectrum planetary data-sensing (ultraviolet, infrared, etc.)
- 3) Neuronal signals data traffic (wireless MRI capture)
- 4) Virtual and augmented reality: virtual geo-intelligence, VR-GPS
- 5) Smart data meta-media tagging of all information sensors and assets
- 6) Wearable and embedded communications devices (local and cloud-based)
- 7) Personal DNA and biometric signature identification

Some of the most interesting big data insights will come from the convergence of data sets from multiple sources. When you combine data from multiple sources, the result is a data mashup that could reveal patterns that would be impossible to detect using only one or two data sets. New insights into behavior, events, trends, and transactions provide non-obvious insights that may yield important insights about populations, entities and even

opportunities.²⁰ For example, cross cuts of geolocational, demographic, and consumer preference data could help answer key questions about individual and group preferences and behaviors.

The Proliferation of AI Weapons of Mass Disruption

We have entered a new era where AI and big data has fueled a new type of information warfare. Fake news, Internet trolls, and propaganda bots, with automated software enabling all of them, influence elections, referendums, and shape public policy today. The hacking of facts and the reorganization of information into propaganda has a new electronic face—the Internet. Over 1,000 software bots, known as Internet trolls, were designed and then delivered information to millions of people online. This trend is the beginning of the wave of influence that we should expect in the future; it is an era where information warfare is not targeted at nations at war, but at nations and non-state actors for the purpose of influencing hearts and minds—all via news, sophisticated AI, and big data.

With many state and non-state actors acquiring big data and AI, we are headed into a new era where information and cyber intelligence could replace boots on the ground as the modus operandi of warfare. We should assume that smart and data-rich technologies may become a disruptive force that could challenge traditional assumptions of what intelligence does and should do in the future. We are at the beginning of this new era, where big data and AI may redefine conflict and reshape the very nature of intelligence operations.²¹

New investments, especially by the private sector, offer considerable potential for furthering research and development of big data and AI, with broad advantages for the IC. As these investments move beyond the common tools to improve enterprise productivity in computing, internet, cloud computing, sensors and information technologies, a newer, more competitive landscape will emerge that enables expanded capacities in knowledge engineering, geospatial intelligence, autonomous robotics, and mobile computational and analytic system designs. These advancements will result in new action paradigms, such as “Prediction as a Service” and cognitive forecasting as routine intelligence capacities. Big data and AI will even enable military kinetic operations. The convergence of emerging technological trends—geo-intelligence, the Internet of Things, post-Moore’s Law microchips, smart sensor proliferation, quantum computing, memory computing, robotics, autonomous thinking machines, and self-learning machine intelligence—represent challenges for every intelligence professional everywhere in the world.

Increasingly, threat actors who are not bound by law or bureaucratic rules are able to act with impunity and agility. A perfect example of this phenomenon is the prevalence of state

20 E. Gray et al., “Small Big Data: Using multiple data-sets to explore unfolding social and economic change,” *Big Data & Society* 2, no. 1 (2015): 1–6.

21 N. Hare, and P. Coghill, “The Future of the Intelligence Analysis Task,” *Intelligence and National Security* 31, no. 6 (2016): 858–870.

and non-state cyber-hacking—using pedestrian computers and routine online access, with minimal capital and technical resources—to take down or impair multi-billion-dollar banks, entertainment companies (Sony), leading retailers (Target), and U.S. government agencies (DOD, etc.). We have apparently accepted the instability and vulnerability to cyberattacks as routine, as if we should expect these attacks to penetrate our infrastructure, government, and private sector. We seem to be in the process of accepting cyber-hacking as the new norm. This expectation is unwise, and leads to unacceptable damage to U.S. security. AI and big data, however, can help bridge the strategic latency gap, to vastly improve both offensive and defensive capabilities.

Of course, technology dangers are not new. Disruptive technological trends have been observed throughout history. The decline of England, Spain, Germany, and France in the Colonial era, when ships and trans-oceanic trade defined geopolitical power and global markets, provides many examples of disruptive technology. Today, we navigate the great sea of the Internet where mobile commerce, big data and digital technology rule. The startling metric of leading companies in terms of stock market value that were replaced from even 2008 to 2016 is an object lesson in the impact of disruptive innovation on industry.²² Some companies adapted and survived, but many did not. Wang Computer made public claims that the word processor was the future. Kodak gambled important market shares on film and the camera. American carmakers thought hybrid engines were a fad.

Other companies embraced the market disruption that the ability to use big data brought. Amazon disrupted the book publishing industry, and then took aim at the entire retail marketplace. Apple revolutionized home computers and cell phones, then took on the online music business. GE has embraced robotics and is integrating sensors into their industrial controls to connect to other industrial control systems. Facebook and LinkedIn created a new world of social networking, and Netflix is disrupting the movie and cable industries. Kickstarter and Indiegogo provide a totally new concept for investment and funding, while Kaggle offers crowd-sourcing contests sponsored by corporations and government agencies to solve large data problems.

Much as these companies have done, the ability to predict, disrupt, and adapt may determine the future of the intelligence community. The competitive global landscape will no longer be secured by economic robustness, sovereign power, or hegemonic influence. Reactive and responsive actions may not be enough. The IC must become a predictive organization with the capabilities to harness foresight brought by AI and big data.

Navigating the Big Data Future

By 2020, over 20.8 billion mobile devices and over 100 billion intelligent things will generate data at a rate that outpaces our ability to use existing technologies to process,

²² "Market Fair Value," *Morningstar*, last accessed October 27, 2017, <http://www.morningstar.com/market-valuation/market-fair-value-graph.aspx>.

store, manage, or secure these data.²³ Current computational technology, which in only three to five years will be legacy systems, cannot meet the challenges that the big data universe poses. The fundamental architecture of computing has not changed in more than 60 years. Computational technology will soon reach physical and computational limits that the data and AI requirements we desire will outpace. New memory computing platforms that IBM's Watson cognitive cloud computing, Google's DeepMind, and the emerging quantum computers offer can approximate the computational technology needs of big data in the near future.²⁴ The IC will require advanced computing architecture to keep pace with the growth and diversification of data needed to conduct the intelligence mission.²⁵

How Private Sector Companies Are Leveraging the Fusion of AI and Big Data

Efficiencies and innovations born from AI and big data are creating entirely new businesses and business models.²⁶ As with the evolution of the internet, where organizations going online to transform their business services and operations have had a transformative effect on the global economy, the next phase of this transformation is AI and big data. Here are some examples of new business models companies are creating based on the insights, capabilities, and resources that AI and big data offer.

- Tesla's electric cars benefit from the NVIDIA AI chips that provide the self-driving functions currently on the market today.
- Waze uses a combination of big data and crowdsourcing that updates in real-time your GPS data from drivers willing to share insights.
- Amazon's recommendation engine, a form of AI, mines the big data of consumer preferences and then automatically suggests books and products in real-time based on your usage.
- LinkedIn uses big data and machine intelligence to analyze preferences where professionals can connect and share contacts, information, and news.
- Google created a free language translation service based on deep learning to showcase their AI.
- Netflix is using machine intelligence to auto-generate program suggestions based on consumer viewing, big data, and sentiment preferences.
- 23andMe offers crowd-sourced big data to analyze probable ancestry origins and

23 "How much Data Will The Internet of Things (IoT) Generate by 2020?", Planet Technology, last accessed October 27, 2017, <https://planetechusa.com/blog/how-much-data-will-the-internet-of-things-iot-generate-by-2020/>.

24 Jennifer Ouellette, "How Quantum Computers and Machine Learning Will Revolutionize Big Data," *Wired*, October 14, 2013, last accessed October 27, 2017, <https://www.wired.com/2013/10/computers-big-data/>.

25 Central Intelligence Agency, "An Interview with Dr. Ruth David, CIA's Deputy Director for Science and Technology," *Electronic Reading Room*, last accessed October 27, 2017, https://www.cia.gov/library/readingroom/docs/DOC_0005802387.pdf.

26 Stefan Biesdorf, David Court, and Paul Willmott, "Big data: What's your plan?", McKinsey Quarterly (March 2013), last accessed October 27, 2017, <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-whats-your-plan>.

health forecasts relevant to individuals.

- Kickstarter uses big data to determine buyer preference investments to determine new categories of investment projects that will appeal to their market.
- Kaggle offers online crowdsourced contests where they leverage big data insights from diverse industries catering to data scientists from diverse industries to solve big data problems for industry and government.

What is common to the leaders in the field of AI and big data is that they are all providing, using, and leveraging data over the internet to deliver new value for competitive advantage. The leveraging and reorganization of data to provide new solutions is redefining the nature of work, product offerings, how services deliver value, the roles of employees, and what business models companies adopt. The entire ecosystem of business, work, and customers is being realigned around the transformation of data as an enabler of every aspect of the enterprise, inclusive of marketing, operations, strategy formulation, sales, finance, and management. The data-centric enterprise is emerging, and it is changing the methods, operations, and strategy of business.

Failure to embrace how customers communicate about your brand over social media might risk competitive disruption by others. Failing to address employees' needs may affect talent and retention. Disregarding the early signals of a sea change in your industry—such as Kodak did with photography and bookstores faced with Amazon—could doom companies and industries.

Implications for the IC

These changes have clear implications for the way intelligence organizations will operate in the future, both internally and externally. For example, the hierarchical decision-making, secrecy, and bureaucratic red tape characteristic of governments will find itself out of step and unable to keep pace with the fast-paced innovation, rapid decision-making, risk tolerance, and ethos of individual responsibility associated with modern big data business practices. Operating with agility will require distributed network models of decision-making as one future possibility.

Job number one of the intelligence community is to provide strategic warning. In today's world, the early indicators of emerging threats will be embedded in the data sets that carry within them information about the intentions of individuals, groups, and nations. The adoption of modern business practices will empower a new generation of intelligence professionals—or outmoded, top-down methods will stifle them.

Nobody expects the government to transform overnight to mimic the private sector. There is time to prepare for major new developments, as we are not yet at the point where our tools can make sense of the sum of all information produced by humans and machines, which is forecasted to reach over 44 zettabytes by 2020, according to the International

Data Corporation (IDC), a market research firm.²⁷ Add to this the Internet of Everything, as Cisco forecasted, to include the total value of all data, people, processes, and things reaching \$14.4 trillion by 2022.²⁸ These trends are accelerating, and our tools are straining to catch up. The private sector is leading the way, but governments face a daunting task of retrofitting these new tools and practices into antiquated, brick-and-mortar organizations. Public-private partnerships, such as those described elsewhere in this volume, will be essential to help government agencies, and especially the IC, keep pace with the new business practices that are defining the international security environment.

What might the future hold for Big Data Intelligence, the post-convergence reality of big data and AI? What seemingly impossible challenges could we tackle with the improved capabilities that this type of computational power will yield?

AI, Big Data, and the IC: Developing a Predictive Strategic Awareness in an Era of Thinking Machines

The advantages for the IC from the fusion of big data and AI come at an important time given the upsurge in terrorism, complexity of the forces at play in the geopolitical landscape, and global threats that face the U.S. The increasing attacks on soft targets, the complex post-superpower era, and the emergence of rogue and non-state actors as surrogates for nation states are all drivers of what is likely to be an extreme future. The IC needs the advantages that AI and big data could afford in accelerating and fortifying the job of preventing strategic surprise.

The use of big data and AI to enhance the predictive awareness of intelligence could be a vital resource for the intelligence professional, as better tools that enable acquisition and smarter analysis of data could lead to more effective and actionable results. Non-obvious transactions as outcomes brought by AI in diagnostics could be instrumental in identifying the precursors of immature or emerging threats. Sensing early-warning patterns to mitigate threat could be accelerated by the use of these tools.

Current developments show great potential to bridge the strategic latency gaps that are growing. New memory-based computers with advanced architecture having 8–10 times more speed over existing computers, processing 10 billion transactions per second, cognitive computers that are digesting 30 billion documents an hour (soon to be digesting this amount of information per minute and then per second!), and eventually a new generation of quantum computers will greatly enable the IC to meet the challenges of the

27 "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," *EMC Digital Universe with Research and Analysis by IDC*, April 2014, last accessed October 27, 2017, <https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm>.

28 "Internet of Everything," *Cisco*, last accessed October 27, 2017, <https://www.cisco.com/c/r/en/us/internet-of-everything-ioe/tomorrow-starts-here/index.html>.

future. A deeper relationship with the private sector and a more agile procurement system to keep pace will be required.

Seven AI and Big Data Forecasts for the IC

I would not be doing my job without forecasting what may come that may possibly influence the future of AI and big data and its impact on the IC. We are entering an era of an acceleration of exponential technologies of which AI and big data will become performance tools for the IC and everyone else. Allies and adversaries will be traversing this path—some faster than others. Here are seven trends that I speculate may shape this future.

1. Autonomy

The rise of autonomy born from smarter AI, general-purpose thinking machines is a likely future that will affect the IC. What will this mean? I think speculating about a world where autonomy drives prediction as an end product of AI and big data is realistic and not hard to understand based on current AI innovations. Self-driving cars and autonomous drones are here today. Within a very short time, autonomous robots will be common in society and the battlefield. Autonomous systems that collect, analyze, advise, and predict are coming faster than we realize. The intelligence supply chain, workflow, and business processes may be transformed by autonomous AI. By mimicking human reasoning and automating parts of the intelligence supply chain, AI may enable human operators' performance in entirely new ways not currently possible. A central issue with autonomous thinking machines is whether we can trust AI to make decisions of accuracy and validity. Trust, control, and efficacy proof sets are three issues that will shape the autonomy of AI in the near future, and the validity of AI.

2. The Big Problem with Big Data

Every minute, an explosion of data of all types inundates our world. We don't have the capacity to locate, capture, store, analyze, or make sense of the data we have today. We need AI and big data analytics to better plan for even larger data tsunami coming in the near future. Humans will not be able to fully manage the enormity of big data, or fully digest and extrapolate insights that future AIs must be able to perform to help us. We see this trend now in AIs being trained to digest the thousands of research papers on disease faster than legions of scientists can do in a fraction of the time. It is not difficult to forecast the implications of why we will need to plan ahead. We have to get ready to manage a future with much bigger data that will require smarter AI capabilities to discover relevant, actionable, and manageable insights.

3. A New Strategic Appreciation of Complex Problem Solving

We are faced with a plethora of complex social, economic, cultural, political, and security problems that increasingly defy our understanding. AI and big data analytics will perhaps produce new insights that will lead to better threat prediction and an appreciation of the

complexity of factors that make up intelligence. The IC should welcome this outcome. Tools that can appreciate higher degrees of complexity may lead to better solutions—smarter and more actionable IC product. Using advanced analytics and AI to mitigate strategic surprise will augment human performance, bridging prediction gaps in the intelligence process—getting the right info to the right people at the right time will make a difference. The advent of thinking machines that will enhance human analysis, even offering a new appreciation of cultures, ideology, motivation, behavior, and threat scenarios would be a welcome positive outcome for the IC in the future.

4. New Computing Architectures Will Accelerate AI

Much that will shape the future of AI and big data will come from new computing architectures. We are approaching the end of Moore's Law, the doubling of computing power every year. Even silicon chips will be replaced. Speeds faster than Moore's Law in the post-silicon era will be shaped by quantum computers, neuro-morphic chips, memory-based computers, and even optical computers that will enable processing speeds, power, and problem solving for AI and big data that are essential to future performance. I would forecast next-generation supercomputing prediction engines that will accelerate AI and big data analytics born from new chips and computing architectures that have superior performance of over 10–100 times over the next 5–10 years.^{29,30}

5. The Co-Evolution of Humans and AI: The Next-Generation Human Machine Interfaces

Wearable and downloadable AIs to augment the performance of the IC analyst may be coming faster than we realize. The co-evolution and merging of human and machine intelligence will become a widespread social and business trend over the next few years. As most organizational functions and performance move into the mobile cloud, access to AIs as an augmentation, a tool to enable human performance, is an emerging future scenario.

6. Prediction as a Service

In time prediction will be possible. For now, it is a work in progress, requiring the development of specialized capabilities designed for the IC. This advancement will not happen overnight, nor should anyone expect it to. There will be many more misses than hits on the way to proving the reliability of prediction tools from AI and big data. Training our thinking machines to learn and then trusting in their cognitive forecasts and decisions will take time to get right. This capacity will happen over time, as we make mistakes; overreliance on tech solutions deserves watching.

29 "Quantum Computing," *D-Wave: The Quantum Computing Company*, last accessed October 27, 2017, <https://www.dwavesys.com/quantum-computing>.

30 "Quantum A.I.," *Research at Google*, last accessed October 27, 2017, <https://research.google.com/pubs/QuantumAI.html>.

7. The Human Factor

Humans need to train, manage, educate, and enable AIs. The IC should look to the right balance of technology and humans to address the challenges of the future—one in which both advanced technology innovations and humans have an important role and mission. It would be prudent to keep in mind realistic expectations about the deliverables that AI and big data may bring and when.

Concluding Thought

Current evidence shows that AI and big data will be game changers in business and in government. The future will likely see smarter machines, the augmentation of humans and many changes in the way intelligence is collected and analyzed. We may very well be at the cusp of a transformation in intelligence. As complimentary toolsets, AI and big data offer new opportunities to manage a world in which complexity and threats will persist; realistically, these emerging tools should contribute to vastly better capabilities to deal with an extreme future.

We are entering a new era where threats based on the New Information War—the engineering of data, fake news, information warfare, cyber, the use of AI and big data for both offensive and defensive strategies—will become mission-essential to the IC. We are entering an era where these innovations will have a comprehensive impact on the future of warfare and intelligence. Better and faster prediction, autonomy, and analysis will become the strategic advantages that will make a difference. We will not be alone in embracing this future. A new competitive global landscape based on the obvious strategic advantages brought by AI and big data may tip more than just elections, but perhaps even tip the balance of global power.

Chapter 5

3D Printing: Acknowledging the Dark Side and Why Speaking Openly About Technology Threat Vectors Is the Right Answer

Jennifer J. Snow

In 2012, an enterprising young artist, Heather Dewey-Hagborg, embarked on an unusual project. While walking the streets of New York, she had noticed all the detritus left behind by everyday human activities. She began to wonder—what if someone were to collect samples of these random bits and pieces? How much might one learn about the people who had left them behind? Determined to find out, Dewey-Hagborg took a three-week crash course in biotechnology offered at the local Genspace, a biohacker public lab and education center. Then she hit the streets.

Over the next few weeks, she collected samples of DNA from trash including hair, chewing gum, and cigarette butts. Each sample was processed at the Genspace. Using a program she had written to import pieces of genetic code, Dewey-Hagborg was able to select for specific factors including hair color, eye color, gender, obesity factors, and even ethnicity. The program then translated the genetic code into a 3D likeness of the unknown person and printed the faces to scale on a 3D printer.

The Stranger Visions art display is one of the more powerful illustrations of the impact that radical leveling technologies (RLTs) are having on society today. RLTs are becoming a defining feature within the technology landscape and can be recognized by five key characteristics. These technologies tend to be anchored in the internet via collaborative, developmental, or operational necessity critical to function or application, while their employment results in broad decentralization of power, economic, or informational capabilities. RLTs are driven by the innovation and expertise of virtual communities and have a transformative, disruptive nature not just within their initial sphere of influence but also across a diverse set of societal and cultural processes and functions.

Finally, mature RLTs have the ability to produce generational leaps with transnational impacts, leading to sometimes severe transitional change.¹ The Stranger Visions example hints at these traits, providing a cautionary tale on future complexity, the necessity for balanced discussion concerning such technologies, and how these advances might be leveraged for both beneficial and malicious purposes.^{2-3,4}

Entering a New Era

Dewey-Hagborg's story is one of many that can be found among the hacker and maker⁵ communities today. Projects that normally would have required a doctoral degree and years of training to accomplish are successfully being undertaken by ordinary citizens and producing extraordinary results. A number of factors have contributed to the increasing accessibility of advanced technologies, some of which will be touched upon here. Yet despite recognizing the changing landscape, few outside the academic and technology communities are willing to engage in realistic discussions that help to educate and inform on these technologies and what they are capable of.

Science fiction writers foresee the inevitable.

—Isaac Asimov

That lack of discussion and understanding is leading down a dangerous path, one that results in reactive, ineffective policy solutions that will further undermine both U.S. and international security. We have entered a new era of technology, where just knowing about a capability is no longer enough. To be effective in protecting the public, the government will need to partner with technology experts, conduct persistent engagement efforts, and develop new types of policy and regulatory regimes to address an emergent cadre of threats.

The Stranger Visions story demonstrates the power of convergence, the combined (and sometimes unpredictable) effect that multiple RLTs can have. However, it is just as important to understand that individual RLTs are powerful in their own right. 3D printing is an accessible example of the exponential effects that a single technology can bring

1 Jennifer Snow, *Entering the Matrix: The Challenge of Regulating Forward Generational Technologies*, thesis (Monterey, CA: Naval Post Graduate School, 2015).

2 Heather Dewey-Hagborg, "Stranger Visions," *Heather Dewey Hagborg*, accessed May 7, 2015, <http://deweyhagborg.com/strangervisions/about.html>.

3 Heather Dewey-Hagborg et al., "DIY Guides to DNA Spoofing," *Biononymous.me*, accessed October 7, 2015, <http://biononymous.me/diy-guides/>.

4 Ellen Jorgensen and Heather Dewey-Hagborg, "New Generation of Bio-Hackers Make DNA Misbehave," *Newsweek*, June 26, 2014, accessed October 7, 2015, <http://www.newsweek.com/2014/07/04/new-generation-bio-hackers-make-dna-misbehave-256322.html>.

5 Makers are a community of Do-It-Yourself hobbyists born out of the 1970s Whole Earth Catalog movement. They seek to find new and innovative ways to solve interesting problems while also emphasizing a reuse and recycle culture. A maker can be someone who designs furniture, builds robots or is into 3D design and 3D printing.

to bear.⁶ Originally designed for rapid prototyping, today this RLT impacts a diverse array of processes. 3D-printed automobiles, jet engines, missile parts, prosthetics, skin, food, lasers, and more—the stuff of science fiction has become the new reality.^{7–8,9}

Much like in the movie *The Matrix*, 3D printing allows for the rapid production of any object a user can imagine, provided they have the materials necessary for creation. The level of skill needed to successfully employ this technology is minimal, and while not as immediate as the digital proficiency downloads featured in *The Matrix*, it is just as impactful.^{10,11} These capabilities can be used for a variety of creative projects, two of which are shared below to highlight the incredible agility of this technology.

The e-NABLE project is a global group equipped with 3D printers on a mission to provide free prosthetic devices to those in need. The project is centered on a community of makers, people who are part of a technology-derived version of the do-it-yourself community, who volunteer to both create and produce prosthetic designs. The online community matches volunteers with individuals who either lack access to medical care or who can't afford the high cost of professionally manufactured devices.

While the project began as a simple effort, it has far surpassed its initial goals, evolving to the point where makers are now providing advanced features: add-on devices and tools to assist recipients with everyday tasks like holding a paintbrush, opening jars, or using a cell phone effectively with a prosthetic. These projects cost around \$35 and have been professionally deemed equivalent to \$6,000–\$8,000 prosthetic devices available from the medical marketplace today. They are easy to repair, hold up well in a variety of environments, can be easily modified with a variety of tools, and provide unconventional custom-fit designs not available from commercial manufacturers.¹²

Three years ago, the first 3D-printed firearms were introduced onto the world stage. The Liberator, the original 3D-printed gun, quickly caught the attention of regulators. The battle

6 For a definition and history of 3D printing, also known as Additive Manufacturing, please visit the wiki: "3D printing," *Wikipedia*, last accessed October 27, 2017, https://en.wikipedia.org/wiki/3D_printing.

7 "3D Printing Could Revolutionise War and Foreign Policy," *Space Daily*, January 5, 2015, last accessed, October 27, 2017, http://www.spacedaily.com/reports/How_3D_printing_could_revolutionise_war_and_foreign_policy_999.html.

8 Louis Columbus, "2015 Roundup of 3D Printing Market Forecasts and Estimates," *Forbes*, March 31, 2015, last accessed October 27, 2017, <https://www.forbes.com/sites/louiscolumbus/2015/03/31/2015-roundup-of-3d-printing-market-forecasts-and-estimates/#4b11431e1b30>.

9 Terry Wohlers and Tim Caffrey, *Wohlers Report 2015: 3D Printing and Additive Manufacturing State of the Industry Annual Worldwide Progress Report*. Online: Wohlers Associates, 2015.

10 Cameron Colquhoun, "Plastic Terrorism: 3D Printing Will Transform Security," *Neon Century*, July 28, 2015, last accessed October 27, 2017, <http://www.neoncentury.io/blog/2015/7/28/plastic-terrorism-3d-printing-will-transform-security>.

11 Uwe Kylau, Kai Goerlich, and Robert Mitchell, "How 3D Printing Will Disrupt Manufacturing," *Digitalist Magazine*, July 28, 2015, last accessed October 27, 2017, <http://www.digitalistmag.com/executive-research/how-3d-printing-will-disrupt-manufacturing>.

12 "E-NABLE 2015: A Year of Hope," *Enabling the Future*, December 30, 2015, last accessed October 27, 2017, <http://enablingthefuture.org/2015/12/30/e-nable-a-year-of-hope/>.

between government and 3D-printed gun makers was akin to the peer-to-peer music battles between music giant MGM and Napster and had a similar end result: the creation of an anonymized (i.e., removing identifying particulars) community using decentralized, encrypted, computer-aided designs to evolve its products to the next level.¹³⁻¹⁴¹⁵ The innovation and creativity that followed the failed regulatory attempt was remarkable, although many of those operating in the mainstream missed most of it due to anonymizing behaviors. In a matter of weeks, the Liberator design went from single shot to firing eight .38-caliber rounds. After that, the design diverged as rifles, handguns, and finally fully functional lower receiver production for existing military-grade firearms were designed, tested, and produced all within the span of a year.¹⁶

Both of these cases highlight the inherent challenges and the amazing benefits of 3D printing. Until very recently, one would have needed an advanced technical degree to leverage such technology effectively, but today, cutting-edge technologies come in the form of prebuilt kits, supported by online forums and utilizing point-and-click capabilities that make them accessible to the masses. Both of these examples also feature a key strength of all RLTs: the open-source communities (OSCs) responsible for driving these technologies forward. Neglecting to understand the people and cultures involved in these technologies is a sure path to failure when attempting to apply policy or regulation.

The government currently lacks the access, expertise, and capacity to independently address the growing family of RLTs, some of which are advancing as rapidly as every six months under convergent conditions.¹⁷ To understand a given technology, one must also understand the people behind it. The rapid exponential evolution seen with these technologies makes it difficult to predict future capabilities, and risks and benefits become even harder to articulate in the presence of technological convergence. Because of these unknowns as well as the rapid pace of advancement, discussions surrounding policy, regulation, and threats from RLTs like 3D printing make for an intricate set of challenges. These challenges will require a collaborative approach between government and human technology drivers that consist of private-sector entities and at times small groups or individual citizens. That approach must start with balanced and open discussion.

13 Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York, NY: Penguin Group, 2006).

14 Devan Desai and Gerard Magliocca, "Patents, Meet Napster: 3D Printing and the Digitization of Things," *Georgetown Law Journal* 102, no. 6 (April 17, 2014): 1–30.

15 Andy Greenberg, "3D-Printing 'Encryption' App Hides Contraband Objects in Plain Sight," *Forbes*, November 4, 2013, last accessed October 27, 2017, <https://www.forbes.com/sites/andygreenberg/2013/11/04/3d-printing-encryption-app-hides-contraband-objects-in-plain-sight/#316aabd9631b>.

16 Andy Greenberg, "How 3D Printed Guns Evolved into Serious Weapons in Just One Year," *Wired*, May 15, 2014, last accessed October 27, 2017, <https://www.wired.com/2014/05/3d-printed-guns/>.

17 Jennifer Snow, *Entering the Matrix: The Challenge of Regulating Forward Generational Technologies*, thesis (Monterey, CA: Naval Post Graduate School, 2015).

Balancing the Discussion

In the first annual Silicon Valley Comic Con, Dr. Astro Teller and his wife Dr. Danielle Teller hosted a talk entitled “AI vs. Superbabies.” The intent was to walk the audience through artificial intelligence and advanced genetics, provide a framework

for understanding these technologies and help to dispel fears about them. While the witty banter was enjoyable between the two technology protagonists the couple portrayed, the end result was a good lesson in how both the government and the private sector are failing to address a key issue: technology transparency.¹⁸

Facts do not cease to exist because they are ignored.

—Aldous Huxley

The first and most important step one can take in ensuring a smart approach to technology is to balance the discussion. At the end of the talk, Astro Teller made a striking comment: “...all the more reason not to slow down progress because of how you feel. Scientific advancements are neither good nor bad; they are just tools for the advancement of human agendas.” There are several important components here that need to be unpacked and examined, because they are and will continue to be central to current and future technology discussions. First and foremost, technology and science are indeed agnostic. Applying labels that cause fear or just emphasize the positive can muddy the waters, making frank discussions harder than they need to be.

Secondly, the rate of technological advancement today is such that trying to halt it would be like trying to catch a Tesla in a motorhome. It simply isn’t possible. And as seen in the Liberator example, efforts to restrict RLTs using traditional methods are generally ineffective and result in continued but hidden evolutions. The final elements are perhaps the most important, as they touch on how people feel about technology and “human agendas.” Astro and Danielle advocate for people not to fear these technologies and to take a positive perspective on technology in general. Yet it was quite clear in the questions from the audience that they were not satisfied with this. Why not? Because it failed to address two factors: capability and intent, the engines behind many human agendas for technology.

Understanding capability and intent is perhaps one of the biggest challenges facing governments today. In many cases, these technologies are being advanced by, with and through the digital environment, a place where Old Power rules are not viable unless supported by the online communities using and evolving these technologies.¹⁹ These days, civilians have access to technologies first, so they understand them in depth; they are there at a technology’s birth, and they help it to grow and progress. The government lacks this

18 “AI Versus Superbabies!”, *Astro Teller*, digital video, directed by Astro Teller, Silicon Valley Comicon, 2016, accessed June 6, 2016, <http://www.astroteller.net/talks/ai-vs-superbabies>.

19 Jeremy Heimans, “What New Power Looks Like,” TED Talk, video, TEDSalon, Berlin, June 2014.

same access, unable to thoroughly understand the technology's true capabilities, which limits understanding of the intent behind the technology.

The Liberator, meant to be a statement about digital freedom of expression by the cypherpunk community²⁰ became much more once subjected to government regulation attempts.^{21,22} Had the intent behind the project been understood, there may only have been 100,000 Liberator downloads, the evolution of the gun designs would not have gone underground and Disarming Corruptor, the 3D design encryption tool, would not have been created.^{23,24}

As more individuals and small groups begin to leverage RLTs to gain parity at the national and even regional levels, the inability of policy to adequately address such groups indicates that it is time to rethink governance and regulation on a global scale. With the help of technology community members who can best explain true technological capability and intent, a representative, forthright discussion on RLTs can begin before a threat develops, allowing for a proactive response. Providing a balanced perspective is necessary for educating and informing the populace and enabling innovation while still keeping public safety and ethics central.

Failure to openly address potential threat vectors can make a technology seem more menacing and can overshadow the potential for it to be used for good. It can also deny government and law enforcement the opportunity to engage with technology experts on areas of concern, resulting in uninformed reactive policy, unnecessary restrictions, and dangerous gaps in which ignorant or malicious actors may operate to cause harm. It is the responsibility of all technology users to have open, transparent discussions about what technology can and can't do and how, as a community, government and human technology drivers can work together to mitigate potential threats while maximizing benefits. That means talking through the negative applications occurring today and trying to anticipate future threats together, especially where those discussions may save lives.

20 For background on the cypherpunk movement go to this wiki: "Cypherpunk," *Wikipedia*, last accessed October 27, 2017, <https://en.wikipedia.org/wiki/Cypherpunk>.

21 Danton Bryans, "Unlocked and Loaded: Government Censorship of 3D-Printed Firearms and a Proposal for More Reasonable Regulation of 3D Printed Goods," *Indiana Law Journal* 90, no. 2 (April 2015): 901–934.

22 Andy Greenberg, "Feds Tighten Restrictions on 3D-Printed Gun Files Online," *Wired*, June 11, 2015 last accessed October 27, 2017, <https://www.wired.com/2015/06/feds-restrict-3d-printed-gun-files/>.

23 Liat Clark, "Disarming Corruptor Distorts 3D Printing Files for Sharing of Banned Items," *Ars Technica*, November 5, 2013, last accessed October 27, 2017, <https://arstechnica.com/information-technology/2013/11/disarming-corruptor-distorts-3d-printing-files-for-sharing-of-banned-items/>.

24 Greenberg, "3D-Printing 'Encryption' App," *Forbes*, 2013.

Acknowledging the Dark Side

3D printing, like all RLTs, has a dark side. Many discussions avoid addressing these aspects openly, mostly because people are uncertain of what to do about them

or because they lack a clear understanding of the technology. This is exactly why these discussions need to happen. Already, 3D printing capabilities are impacting counter-proliferation regimes, counterterrorism efforts, and the fight against organized crime in ways that need to be addressed both nationally and internationally.

There's a dark side to everything.

—Prince

3D Printing and Counter-Proliferation

In 2014, the decommissioned Sellafield nuclear power plant in Britain made big news across the 3D printing community. For the first time, a private company was using 3D scanning and printing capabilities to design unique one-off solutions to help save money and solve nuclear-specific challenges. 3D metal and plastics printing was used to recreate old parts or to design new configurations that helped increase safety and cut costs while also reducing part production times by as much as 87%. 3D scanning allowed for easy reverse engineering of broken parts and in some cases allowed designers to create more efficient structures.^{25,26}

In 2015, the American Physical Society printed a story warning of the potential for 3D printing to be used in the proliferation of advanced weapons design and for nuclear components. The ability to take a component that has always required multiple months and a full production line to make and instead produce it to the same specifications in under four hours is a definitive game changer.^{27,28} The first example of those fears was realized in 2016, as the Chinese National Nuclear Corporation (CNNC) announced the successful 3D printing of a nuclear fuel assembly component, the CAP1400. Multiple 3D

25 Oliver Gomez, "3D Printing to the Rescue of a Nuclear Power Plant," *3D Printing Pin*, May 16, 2014, last accessed October 27, 2017, <http://www.3dprintingpin.com/3d-printing-to-the-rescue-of-nuclear-power-plant/>.

26 Sellafield Ltd Leads the Way with Revolutionary 3D Technology," *The UK Government Web Archive*, May 12, 2014, last accessed October 27, 2017, <http://webarchive.nationalarchives.gov.uk/20170712123618/http://www.sellafieldsites.com/press/sellafield-ltd-leads-the-way-with-revolutionary-3d-technology/>.

27 Bruce Goodwin, "Additive Manufacturing and High-Performance Computing: A Disruptive Latent Technology," abstract, American Physical Society, San Antonio, Texas, March 5, 2015.

28 Michael Lucibella, "Manufacturing Revolution May Mean Trouble for National Security," *APS Physics* 24, no. 4 (April 2015): 1–5.

experts responded by saying it could take “up to 10 years” before 3D printing becomes a mainstream process in nuclear component production.^{29,30}

The experts, however, failed to specify whether this assessment was based on 3D printing as an independent technology or as a result of a convergence of technologies. Since 3D printing is evolving exponentially, not only is it producing new capabilities every 18–24 months, but the production time and costs are dropping too. A 3D-printed item that takes four hours and \$27 in materials to produce in 2016 will take just under eight minutes and cost roughly \$3 to produce in 2026. That is before considering the possibility that technological convergence may further decrease these factors.³¹ Trying to predict what comes next for these increasingly fast-paced technological evolutions and what they mean for security, the global economy, governance, and society is a difficult prospect even for those actively involved with the technology.^{32,33,34}

3D bio- and chemical printing is another challenging area. The FDA approved the first 3D-printed drug for sale in 2015, providing insight into how 3D printers are going to revolutionize science for the masses. The drug, an anti-seizure medication called SPRITAM, was not just a simple printed pill. The company had been able to restructure the chemical composition so that the pill dissolved more quickly or could provide a tailored dosage for a specific patient, and fine-tuned, replacing the typical mass-produced “one size fits all”

29 David Dalton, “China’s CNNC Uses 3D Printing to Produce Fuel Assembly Component,” *NucNet*, January 18, 2016, last accessed October 27, 2017, <http://www.nucnet.org/all-the-news/2016/01/18/china-s-cnnc-uses-3d-printing-to-produce-fuel-assembly-component>.

30 Alec@3Ders.org, “Chinese Experts Unveil First 3D Printed Nuclear Fuel Element, Could Be Widely Used in 10 Years,” 3Ders.Org, January 14, 2016, last accessed October 27, 2017.

31 Brian Krassenstein, “The Moore’s Law of 3D Printing . . . Yes, It Does Exist, and Could Have Staggering Implications,” 3DPrint.com, June 28, 2014, last accessed October 27, 2017, <https://3dprint.com/7543/3d-printing-moores-law/>.

32 Jeremy Heimans and Henry Timms, “Understanding ‘New Power,’” *Harvard Business Review*, December 1, 2014, last accessed October 27, 2017, <https://hbr.org/2014/12/understanding-new-power>.

33 Kevin Maney, “The Law Can’t Keep Up with Technology . . . and That’s a Very Good Thing,” *Newsweek*, October 31, 2015, last accessed October 27, 2017, <http://www.newsweek.com/2015/11/13/government-gets-slower-tech-gets-faster-389073.html>.

34 Vivek Wadhwa, “Laws and Ethics Can’t Keep Pace with Technology,” *MIT Technology Review*, April 15, 2014, last accessed October 27, 2017, <https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/>.

dosages.^{35,36,37,38,39} So what happens when someone decides to take the Chemprinter, a 3D chemical printer created in 2012, and put it to work making ecstasy, cocaine, heroin or other illicit drugs?⁴⁰ The ability to use open-source software to create new chemical structures is the stuff of four years ago.

Today, it is possible not only to 3D print drugs but also to vary their signatures, changing the composition of chemicals to make them less detectable by law enforcement or producing a dangerous punch by incorporating new chemicals into previously unproducible structures.⁴¹ This allows for inexpensive, easy production of reconfigurable drugs by enabling users to apply advanced chemical-engineering techniques via point-and-click, prebuilt, open-source packages. These same techniques can also translate to the ability to streamline chemical and biological warfare programs, enabling tactical-level production by small groups who can “contract out” for the required expertise via dark web operators and prepackaged downloadable solutions.

Dr. Jill Bellamy, director of Warfare Technology Analytics and author of *The Biological Warfare Blog: Black Six* discussed the potential next step in this series of evolutions:⁴²

35 Dominic Basulto, “Why It Matters that the FDA Just Approved the First 3D-Printed Drug,” *Washington Post*, August 11, 2015, last accessed October 27, 2017, https://www.washingtonpost.com/news/innovations/wp/2015/08/11/why-it-matters-that-the-fda-just-approved-the-first-3d-printed-drug/?utm_term=.f569efe59edc.

36 Eddie Krassenstein, “German Company Aims to Sell 3D Printed Drugs & a 3D Drug Printer,” 3DPrint.com, August 10, 2015, last accessed October 27, 2017, <https://3dprint.com/87977/3d-printed-drugs-2/>.

37 Robinson Meyer, “3-D Printed Drugs Are Here,” *Atlantic*, August 19, 2015, last accessed October 27, 2017, <https://www.theatlantic.com/technology/archive/2015/08/3d-printing-pills-spritam-drug-industry/401177/>.

38 Susan Scutti, “FDA Approves First Ever 3D-Printed Epilepsy Drug from Aprelia; Set to Create More Central Nervous System Pills,” *Medical Daily*, August 4, 2015, last accessed October 27, 2017, <http://www.medicaldaily.com/fda-approves-first-ever-3d-printed-epilepsy-drug-aprelicia-set-create-more-central-346004>.

39 Oliver Wainwright, “The First 3D-Printed Pill Opens Up a World of Downloadable Medicine,” *Guardian*, August 5, 2015, last accessed October 27, 2017, <https://www.theguardian.com/artanddesign/architecture-design-blog/2015/aug/05/the-first-3d-printed-pill-opens-up-a-world-of-downloadable-medicine>.

40 Tim Adams, “The ‘Chemputer’ that Could Print Out Any Drug,” *Guardian*, July 21, 2012, last accessed October 27, 2017, <https://www.theguardian.com/science/2012/jul/21/chemputer-that-prints-out-drugs>.

41 Mark D. Szymes et al., “Integrated 3D-Printed Reactionware for Chemical Synthesis and Analysis,” *Nature Chemistry* 4 (April 15, 2012): 349–354.

42 Jill Bellamy, “Emerging Technologies: Lowering the Threshold for ISIS Mass Casualty Terrorism,” *Biological Warfare Blog: Black Six*, January 25, 2015, last accessed October 27, 2017, <http://bio-defencewarfareanalyst.blogspot.com/2015/01/emerging-technologies-lowering.html>.

3D mass-production disposable drones would be a game changer for weapons of mass destruction and future terrorist methods and tactics allowing incredible versatility...In a scenario where mixed drones are used, some with conventional payloads, some with unconventional payloads, multiple strikes would be possible, and while the conventional attack would be considered immediate, there could well be long-term casualties either from loading the payloads with low-level radiological material (small aerial dirty bombs) or biological and chemical weaponized agents.

Such agents could well create multiple rolling outbreaks of pandemic disease or be used as stealthy force reducers/force multipliers. 4D technology, developed at MIT, could mean that printed payloads using biological agents could be weaponized based on target-specific data. This would obscure identification and remove some of the barriers which previously served to make this type of weaponization process the domain of state military labs. Essentially making it user friendly to terrorists.

These kinds of drone technologies exist today and are in use in places like Syria and the Ukraine, by rebel fighters and terror groups for surveillance, targeting, and conventional air strikes.^{43,44,45} The ability to produce simple synthetic biological agents and intermediate chemical agents is also becoming more of a concern thanks to significant down-skilling in the areas of synthetic biology and CRISPR/Cas-9 technologies. While biotechnologies are not at a high school level yet, technological convergence will see that point met within the next five years. Existing counter-proliferation regulatory regimes were designed with the state actor in mind.

But today, bad actors can be small groups, individuals or even ignorant actors who inadvertently use technology in a way that produces a threat. How to deal with these behaviors, how to develop technology policy that has teeth in both the physical and the cyber realms, and how to proactively prevent a crisis situation like the one Dr. Bellamy hypothesized are all topics that must be discussed and solved today. Counter-proliferation efforts in the future must be done hand in hand with technology drivers and technology users. Without their help, any policy put in place will likely have limited success. It is no

43 David Hambling, "ISIS Is Reportedly Packing Drones With Explosives Now," *Popular Mechanics*, December, 16, 2015, last accessed October 27, 2017, <http://www.popularmechanics.com/military/weapons/a18577/isis-packing-drones-with-explosives/>

44 Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat From ISIS: Exploding Drones," *New York Times*, October 11, 2016, last accessed October 27, 2017, <https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html>

45 Knut Torbjørn Moe, "Small Drones: From Cheap Toys to Terrorist Tools—Detection and Disruption Challenges," *The Journal of the Joint Air Power Competence Centre* 21 (Winter 2015), last accessed October 27, 2017, <https://www.japcc.org/small-drones/>.

longer enough simply to acquire the technology for national defense. Understanding and working with technology communities is a critical requirement to ensure the success of the U.S. Third Offset Strategy. This is true for counter-proliferation as well as counterterrorism and organized crime efforts.

3D Printing as a Tool of Terrorism and Organized Crime

The world of terrorism and organized crime is certainly no stranger to technology. In fact, the majority of these groups are adopting new technologies faster than most national governments and putting them to use in ways that best benefit their organizational agendas. Hezbollah, Hamas, Daesh, al-Qaeda, and other terror groups are using 3D-printed drones and drone parts to enable operations by providing persistent surveillance and reconnaissance capabilities, improved targeting capabilities, and airborne improvised explosive devices.^{46,47,48}

With the advent of 3D-printed explosives by nation-states, it is only a matter of time before similar technologies are developed by terrorist groups as well.⁴⁹ Leveraging multiple technologies may hasten success in this area, and while research and development efforts may cost lives, be assured that terrorists and criminals will not be deterred. An even easier path for them would be to hire a team of dark web hackers to steal blueprints for existing 3D-printed explosives and printers.⁵⁰

Criminal gangs are making and flying drones to move drug shipments across international boundaries or to smuggle drugs, phones, and other contraband into prison yards.⁵¹ Drones are being used to identify individuals working with police to conduct lethal actions against informants and rival crime gangs.⁵² Drones are also being used to case homes for burglaries

46 Yochi Dreazen, "The Next Arab-Israeli War Will Be Fought with Drones," *New Republic*, March 26, 2014, last accessed October 27, 2017, <https://newrepublic.com/article/117087/next-arab-israeli-war-will-be-fought-drones>.

47 Kelley Saylor, *A World of Proliferated Drones: A Technology Primer* (Washington, DC: Center for New American Security, 2015).

48 David Hambling, "ISIS Is Reportedly Packing Drones with Explosives Now," *Popular Mechanics*, December 16, 2015, last accessed October 27, 2017, <http://www.popularmechanics.com/military/weapons/a18577/isis-packing-drones-with-explosives/>.

49 Eleanor Hutterer, "Explosiv3design," *Los Alamos Science and Technology Magazine* 1663 (March 2016): 2–4, last accessed October 27, 2017, <http://www.lanl.gov/discover/publications/1663/2016-march/explosive-3d-design.php>.

50 Pierluigi Paganini, "Hacking Communities in the Deep Web," InfoSec Institute, May 15, 2015, last accessed October 27, 2017, <http://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/>.

51 John Hall, "Drones Smuggling Mobile Phones and Drugs into Prisons Could Belong to Criminal Gangs," *International Business Times*, December 19, 2015, last accessed October 27, 2017, <http://www.ibtimes.co.uk/drones-smuggling-mobile-phones-drugs-into-prisons-could-belong-criminal-gangs-1534148>.

52 Vanda Felbab-Brown, "Drugs and Drones: The Crime Empire Strikes Back," *Brookings.edu: Order from Chaos*, February 24, 2016, last accessed October 27, 2017, <http://www.brookings.edu/blogs/order-from-chaos/posts/2016/02/24-technology-in-fighting-crime-felbabbrown>.

or to spy on occupants.⁵³ Border patrol agents have seen the first 3D-printed modified weapons coming across the border, and the world's first 3D-printed machine gun plans are now on sale for \$150.^{54,55} But guns and drones are just the beginning.

3D-printed drugs, ATM skimmers, fake cargo container seals, and keys are common crime-related items seen today. In the future, 3D printing may even allow for the production and sale of synthetic life forms, and exotic, unregulated designer pets that could wreak havoc on the environment.^{56,57,58} Steven Kotler, director of research for the Flow Genome Project and author of *Tomorrowland: Our Journey from Science Fiction to Science Fact*, highlights these challenges in one of his presentations:⁵⁹

If you look at kind of the three biggest criminal enterprises in the world right now, it's arms dealing, drugs and [the] exotic animals [trade]... Well, we can use 3D printing to print guns already, right? That's already possible. There are people working on a 3D printer for drugs, right? The idea is prescription pharmaceuticals—you could print them in 3D. It's a chemistry-set 3D printer... Synthetic biology lets us create brand-new organisms from scratch, so do you want your exotic parrot or do you want something that's brand new... So what's interesting about this... it means that the three largest criminal enterprises in the world are going to be available to anyone... When we can use 3D printers and synthetic biology and when anybody can do it, it means that a lot of the illegal trades, right, the bottom's just fallen out. And what happens then we have no idea.

53 David Barrett, "Burglars Use Drone Helicopters to Target Homes," *Telegraph*, May 18, 2015, last accessed October 27, 2017, <http://www.telegraph.co.uk/news/uknews/crime/11613568/Burglars-use-drone-helicopters-to-identify-targe-homes.html>.

54 Paul Ingram, "CBP: 3-D-Printed Full-Auto Rifle Seized at Lukeville Crossing," *Tucson Sentinel*, February 8, 2016, last accessed October 27, 2017, http://www.tucsonsentinel.com/local/report/020816_3d_printed_gun/cbp-3-d-printed-full-auto-rifle-seized-lukeville-crossing/.

55 Bridget Butler Millsaps, "Cody Wilson Announces Impending Release of 3D Files for \$150 Machine Gun; Some Fear He Is 'Making Things Easier' for Terrorists," *3DPrint.com*, January 25, 2016, last accessed October 27, 2017, <https://3dprint.com/116658/wilson-3d-files-machine-gun/>.

56 Jelmer Luimstra, "Criminals Use 3D Printers to Mass-Produce Skimming Devices," *3DPrint.com*, March 24, 2014, <http://3dprinting.com/news/criminals-use-3d-printers-mass-produce-skimming-devices/>.

57 "Criminal Use of 3D Printing Involved in Stolen Cargo," *Roanoke Trade*, September 18, 2015, last accessed October 27, 2017, <https://www.roanoketrade.com/stolen-cargo-3d-printing-criminal/>.

58 Steven Kotler, "Vice Wars: How 3-D Printing Will Revolutionize Crime," *Forbes*, July 31, 2012, last accessed October 27, 2017, <http://www.forbes.com/sites/stevenkotler/2012/07/31/the-democratization-of-vice-the-impact-of-exponential-technology-on-illicit-trades-and-organized-crime/#35b8631125e7>.

59 Steven Kotler, "Printing Guns, Drugs, and DNA Weapons: Organized Crime Is Being Decentralized," online video, *BigThink.com*, 2015, last accessed October 27, 2017, <http://bigthink.com/videos/steven-kotler-and-the-future-of-criminality>.

No Easy Answers

As we move forward into this new era of technology, it is imperative that we ask good questions so that we can then find the best answers. In many ways, poorly developed policy and the use of outdated regulations are making these problems more challenging. The 3D-printed gun example is just the first of several recent stories that indicate the need for updated, smart tech policy. Reliving the peer-to-peer music battles but with new technologies ensures the development of dangerous blind spots that can work to the advantage of malicious actors. Anonymizing actions, compliance without effect, the “Streisand effect,” and motivation crowding effects should be avoided;⁶⁰ if any of these is present when implementing policy, that is a good indicator that a different approach is warranted.⁶¹

Good questions outrank easy answers.

—Paul Samuelson

When applied to the counter-proliferation mission set, these effects make the environment infinitely more complex. Understanding what new technologies are out there and how they will impact and shape society is important and will promote a proactive approach. This will mean there is time for proactive planning to develop sound policy instead of reacting to a potential threat and making the situation worse. It will mean that proactive thought processes are in place to instill ethical practices and a culture of accountability among tech producers and consumers. Most importantly, proactive action (whether in the form of education, ethical design, standardized safety protocols, or collaboration with technology community partners on self-regulation and self-policing options) will allow for the grassroots identification and prevention of ignorant or malicious actors before a technology can be leveraged to illicit purpose.

So how do we bring global state and non-state actors together on the development of international authorities to address complex issues like how 3D printing could be leveraged for chemical or biological weapon production? How do we get non-state actors to participate in and adhere to national or international agreements? What types of new models need to be developed based on today’s technologies to help guide these processes, and how do we design them in such a way that they can evolve alongside these technologies and remain impactful five or ten years from now? And how do we proactively ensure that threat vectors are addressed without limiting innovation? These are the kinds

60 Compliance without effect occurred in the case of the Liberator 3D-printed gun. The government requested the take-down of the design and Defense Distributed complied, but despite their compliance the digital design proliferated and evolved into new designs. The “Streisand Effect” is based on the release of photos of Barbara Streisand’s beach house, which Streisand tried to have removed from the internet. Her actions attracted additional unwanted attention resulting in the proliferation of the photos online. Finally, the motivation crowding effect takes a moral calculation (i.e., stealing music is bad) and turns it into a risk/benefit calculation (free vs. potential of getting caught). When MGM tried to punish Napster users, their legal actions contributed to the belief that peer-to-peer downloading was justified and resulted in widespread proliferation and anonymizing activities.

61 Danton Bryans, “Unlocked and Loaded: Government Censorship of 3D Printed Firearms and a Proposal for More Reasonable Regulation of 3D Printed Goods,” *Indiana Law Journal* 90, no. 2 (April 2015): 901–934.

of questions that need to be asked, but the answers will be hard. Exponential technologies create an equally exponential operating environment that will require thoughtful, persistent engagement to address successfully.

Three areas that can immediately be implemented include the establishment of collaborative effects, regulatory effects, and active effects. A firm foundation in collaborative effects between government and the various self-regulating communities that exist can overcome many potential challenges before they begin. Education and outreach, ethical design, established safety protocols, and teaming with technology partners ensure that values and norms are in place to help limit ignorant actors and deter potential malicious actors.

Additionally, many technology groups already self-regulate and have in-house standards that community members must abide by.⁶² This is the first line of defense, and if an actor or group is identified as a possible threat to public safety, community members will be able to identify them long before government intelligence apparatuses will. Keeping the door open and enabling anonymous-threat tip capabilities to protect those who do report will help mitigate and provide early identification of possible threat actors.⁶³

The next step is to revisit existing policy and regulatory regimes both nationally and internationally. Many of the loopholes exploited today by terrorists and criminals exist due to a lack of collaboration and shared laws at the nation-state level. Identifying where policy needs to be revised, conducting focused policy development to address new areas, and establishing a counter-proliferation model that brings in the exponential effects of emerging technologies are all crucial to the future of global security.⁶⁴ Technology community members, drivers, and users must be part of these processes. They are able to very quickly inform on what types of policy will or will not work and why. As participants in crowdsourced policy efforts alongside government teammates, they will have buy-in and will be more likely to aid in the establishment and effectiveness of new policy in the digital environs.

Active outreach efforts provide additional options for community members to engage in areas of high interest to counter-proliferation, counterterrorism and cyber-threat mitigation efforts. Engaging with hackers to find new ways to improve systems security and the health of the internet allows the government to gain expertise, find creative open-source solutions,

62 For a basic primer and additional readings on cyber culture go to this wiki: "Cyberculture," *Wikipedia*, last accessed October 27, 2017, <https://en.wikipedia.org/wiki/Cyberculture>.

63 Snow, *Entering the Matrix* (2015).

64 A quick example is illustrative here of the changes seen in the proliferation environment. For the first time industrial-level operations are achievable via one or more 3D printers. As an intelligence analyst, I may be focused on interdicting specific devices regulated by Wassenaar that are now made in a garage via remote means with significantly reduced pattern-of-life signatures. It is important to bring in the right technology expertise to determine what can be regulated, what is outside of government control, and what new methods of detection and interdiction upstream of the threat vector or within the online environment itself can be employed to prevent or reduce the likelihood of this technology being used for bad purposes.

and save money. The use of cyber bounties is already paying significant dividends.⁶⁵ A logical next step would be to expand these efforts to introduce a “cyber privateer” clause, creating a network of technology experts who could be surged to support the government during times of crisis or on specific areas of concern. Finally, the continued development and expansion of public/private fusion centers offers a neutral space for intelligence sharing on natural disasters, national security, and regional terror-type events.⁶⁶

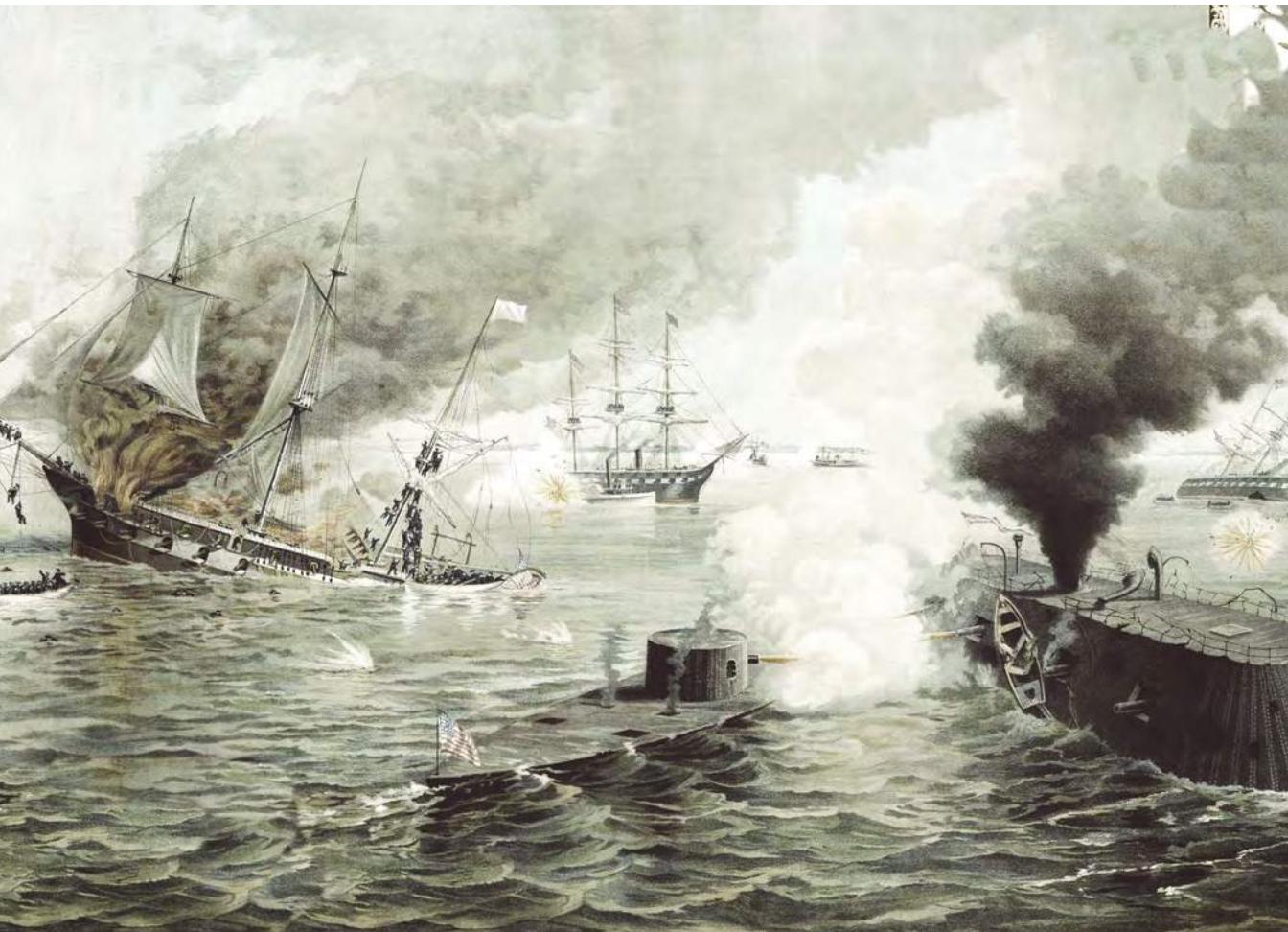
⁶⁵ For examples of successful government and corporate bug bounty programs please visit the following sites, last accessed October 27, 2017: https://en.wikipedia.org/wiki/Bug_bounty_program; <https://bugcrowd.com/list-of-bug-bounty-programs/> <https://www.united.com/web/en-U.S./content/Contact/bugbounty.aspx>; <https://techcrunch.com/2017/01/31/googles-bug-bounty-2016/>

⁶⁶ *Ibid.*

2

The White Side:

Latent Technology Trends and Timelines



Chapter 6

New Technologies and International Order

Paul Bracken

Around the world, more advanced technologies are being brought into the armed forces than at any time since the 1950s. Back then, the two superpowers deployed nuclear weapons, jet aircraft, guided missiles, radar, atomic submarines, spy satellites, and digital computers.

It is useful to recall just how sweeping were the changes this had on the international order. World politics split into two arenas: the two superpowers—and everyone else. Only the United States and the Soviet Union could operate at the top level. They had military capacities that made it look hopeless for others to even try to play their game. U.S. allies ponied up enough to remain allies, but that was about all. They had a clearly subordinate relationship to Washington. Bloc discipline was tight, as allies needed the superpowers for security.

This tiering of states into two groups slowed what had happened so many times before in history: the move to a multipolar international system.¹ A reasonable analyst looking at the world in 1948 might have expected this, if they projected from previous patterns. But it didn't happen. So, one of the most interesting effects of technology in the 1950s was that it worked *against* the return of a multipolar system.

I raise this to show just how powerful the effects of technology can be on international order. And to underscore how different things are today. There is a large, new set of advanced technologies now. Cyberwar, drones, hypersonic missiles, artificial intelligence, data analytics, computerized recognition technologies, cheap sensors, the Internet of Things. These technologies promise to change the character of war, and that is how they

¹ Some definitions are in order. By a "multipolar world" I mean an international order wherein economic, technological, and military power are distributed among several countries, as distinct from a unipolar or bipolar order where it is concentrated in one or two. I do not suggest that the current international system is strictly any one of these, however. In some ways the current system is unipolar, in others it is multipolar, and in still others it is nonpolar—no one has power.

are usually analyzed. This essay, however, focuses not on war, at least not directly on war. My argument is this: *technology now is abetting—not holding back—the move to a multipolar world.*

In the Cold War it was the reverse. Then, technology offset the “natural” political forces toward a multipolar system. The technologies, atomic weapons, long-range bombers, and a bit later, long-range missiles, were hard to produce in large numbers and required advances in other fields like engineering, guidance, and quality control. And obviously the obvious candidate countries with technology potential, Germany, France, and Japan, had their industrial and technology sectors destroyed in the war.

Technology today is hastening multipolarity. My argument is that multipolarity is proceeding not for purely technology reasons alone but for economic and political reasons. However, this confluence of factors has a different pattern today than it did in the late 1940s through the 1960s. International trade, for example, has lowered the deterrent to entry in many of the technologies relevant here. Cyber, drones, laser guidance, and many others are not that difficult to obtain any longer.

There is an argument that only wealthy, technically developed countries could master some advanced technologies. Nuclear weapons are an example, sophisticated cyber arsenals are another. Space weapons may be another, and this may also be the case for hypersonic weapons. It may well be that only the United States, Russia, and China could master these technologies to deploy them at scale. But it seems to me that even if this is the case, it would mean that only they could engage in high-end warfare with them. At a lower level of intensity these systems are not useable. Maximum-effort war between major powers is one area where all-out nuclear, cyber, and space attacks matter. A war between the United States and China is an example. I would grant this possibility. But this seems to me so unlikely as to not undermine my point. At any rate, a conflict at this level of intensity would change so many other features of world order that it is in an altogether different category.

Many countries now have educated populations, wealth, and technology, so that they can build and operate complex technologies. Politically speaking, the bloc discipline that held in the bipolar world of the Cold War has long since dissolved. This means that the United States or the UN or even a condominium of major powers—were this to come into being—would have a difficult time disarming a country like Iran, North Korea, or Israel.

More countries not only can ignore U.S. leadership, increasingly they don't feel that they can trust the United States to come to their defense were this to become necessary. This encourages them to innovate in the new technology space.

To add to all of this, geopolitical uncertainty about what the emerging world order will look like is larger than it was in the 1950s. One thing you could say about the 1950s was that it was clear as to which camp, East or West, a country was in. This is no longer the case. No one any longer knows the names of the “camps.”

Because of all of these factors a logical course of action for a country is to hedge against the uncertainties by investing in the new technologies of defense “just in case” the future takes a bad turn. This is why so many countries are going into the new technologies.

Technology Dynamics

Technology has its own dynamics. There are rhythms, patterns, and even fads and fashions in it. They arise from the nature of the technologies and the interactions of one technology with another. There are many examples of these dynamics: Moore’s Law; the shift from mainframe computers to PCs to tablets and smartphones; the evolution from propeller to jet to hypersonic aircraft; the decrease in the physical size of electronic systems; the synergy of technologies for creating new applications. Independent of politics, these dynamics likely would have taken place for more or less internal technological reasons.

Let’s consider some of these dynamics for the advanced military technologies now coming into being. The technologies of greatest significance are listed in Table 1.

Most of the items in the table are familiar to students of military technology and are the topic of discussion in other chapters of this book, and in many other sources. My focus here is not on explaining how each of these can impact war, but on the collective impact of these technologies. In other words, I want to examine what happens when *many* new technologies come into being—how their *combined* impact affects international order.

However, two items on the list, recognition technologies and nuclear weapons, may need some elaboration and elucidation. First, recognition technologies refers to computerized systems such as automatic license plate readers, facial-recognition cameras and software, iris scanners, voice recognition, and vibration analyzers that distinguish between different automobile or boat engines. These technologies are widely available, in the United States and in other countries. Walmart, for example, has installed facial-recognition cameras at the entrance to many of its stores. Automatic license plate readers can scan thousands of license plates while driving around a city, and compare them to a hot sheet of numbers stored in the cloud. Today, they are routinely deployed throughout the United States.

Recognition technologies are included on the list because they can be incorporated into a larger system to track people, target command and control, and monitor the movement of

Drones (air, sea, undersea)
Nuclear weapons
Cyber
Precision strike
Hypersonic missiles
Anti-satellite weapons
Big data analytics
High-performance Computing
Additive manufactured weapons
Artificial intelligence
Stealth
Genetic engineering
Recognition technology

Table 1: Military significant advanced technologies.

many kinds of vehicles. Such a system could be useful for intelligence, warning, or attack, if it were linked to weapons like precision-strike systems and integrated into the data output of the recognition technologies.

Nuclear weapons are also included on the list. They are not new, obviously. But they are included because of my focus on global order. In particular, nuclear weapons could be combined with other technologies on the list to change how nuclear weapons are thought about. This could have considerable impact on international order. For example, if items on the list provided a country with the ability to track another country's nuclear missiles, it would lower the threshold of nuclear war. It would also allow a country to attack enemy nuclear forces with a conventional, non-nuclear attack.

Or consider another combination of items on the list with nuclear weapons. One of the most important uses of cyberattacks in high-intensity war is likely to be blinding the sensors and warning systems of the enemy. At present this method is drones with kinetic attack. But cyberattack allows zero-warning strikes. There are no signs of attack until the actual strike. Or consider one more possibility: Hypersonic missiles could be employed to reduce warning time in a kinetic attack. In the Cold War the United States fielded the Pershing 2 missiles in Europe. This was considered highly destabilizing in that they could strike Moscow, the key command and control node of Soviet nuclear forces, in about ten minutes flight time. This was considered a way to paralyze the Soviet high command to allow enough time for ICBMs and other nuclear strikes to destroy Soviet nuclear forces before they were launched.

Combinations of cyber, hypersonic missiles, and stealth could radically change the nuclear context of the major powers with each other. It could also provide a first-strike capacity against the secondary and barely nuclear powers.

Other technologies on the list are not entirely new. Yet they are "advanced" because their performance has so drastically improved relative to earlier versions of the technology. Precision strike, for instance, has been around since the late part of the Vietnam War. But precision strike has gotten a lot better in recent years. Today, it can respond to fleeing targets, ensure lower collateral damage, and destroy wider types of targets than the laser-guided bombs of the 1970s and 1980s. Soon, it may be able to hit mobile targets, given the advances in tracking discussed above.

One thing the list immediately suggests is that the horizontal spread of the technologies to many countries is well underway. The technologies on the list are not just for one or two major powers, as in the 1950s. Today, you don't have to be a superpower to fly drones and launch cyberattacks. Even subnational groups have them.

This points to an important conclusion, one that in many ways we are so close to that we may overlook. It follows from the sheer number of new technologies and their spread to many countries and even groups: *the monopoly that major powers once held in advanced military technology has broken down*. There was a time when only major powers could

deploy dreadnoughts, armored divisions, and atomic bombs. It was certainly not a peaceful or stable world. Germany, France, Britain, Japan, Russia, and the United States all fought big and small wars. But in these the smaller, weaker sides couldn't technologically challenge the major powers. This has had a significant impact shaping the international order as it evolved over the past two hundred years.

In the Vietnam War, Hanoi never directly attacked the United States homeland. Indeed, Hanoi couldn't reach key U.S. allies like Japan and the Philippines. Today, North Korea is trying to deploy a nuclear missile that can reach the west coast of the United States and beyond. Pyongyang already has missiles that can cover all U.S. allies, like South Korea and Japan.

Pakistan and Iran, likewise, fly drones that can spot the major ships and army groupings of their enemy. They probably don't have a good process to do this. But they might get lucky and destroy a large valuable target. This is quite a significant change in historical pattern. Small countries can pack a big punch, possibly a nuclear punch. They will lose a war with the United States. But the United States would strongly prefer to have no war at all. Washington is thus likely to be much more cautious in dealing with states that have this capacity. A major power going up against a seemingly weak opponent runs the risk of a significant setback. This possibility is likely to make major powers mount larger campaigns than would have been the case in the past, or, alternatively, to make the major power avoid crises altogether. This is because a crisis could lead to an escalation, and a "lucky hit."

When major powers fight each other in limited conflicts a similar logic may apply. Things could get out of hand quickly, and this discourages the power with less commitment to avoid taking the risk of a confrontation in the first place. Russian occupation of the Crimea and part of the Ukraine and China's island construction program stand out here as examples. While these are important American interests, they are more important to Russia and China, respectively. The United States faces an opponent in each instance that could bring more advanced technologies to bear if they chose to do so. Russia could intensify cyberattacks or fire on U.S. aircraft with deadly effect. China could further militarize the artificial islands in the South China Sea. Beijing might, for example, deploy tactical nuclear weapons on these islands for "defensive" purposes.

In the context of the other advanced technologies that China deploys, this would make the consequences of some inadvertent escalation with the United States much more dangerous. It illustrates my contention that there are really major consequences stemming from the combination of the technologies on the list with nuclear weapons. Technology provides escalation options of a kind that simply didn't exist two decades ago.

Let's consider a different kind of technological dynamic, but one that is still related to advanced technologies. Additive manufacturing and high-performance computing further accelerate the erosion of the onetime major power monopoly over advanced military technologies. These technologies flatten the knowledge curve needed to produce items on the list. An additive manufacturing system that produces heat-seeking missiles is an

example. Perhaps this system only produces the key components of these missiles, the ones that are difficult to manufacture because of engineering or quality-control weaknesses. A country like North Korea would not need the advanced engineering, quality control, and precision manufacturing that has stopped them from making advanced missiles in the past. These features could be incorporated into the software and computing of additive manufacturing.

Another important technological dynamic arises from simply noting how long the list of items in Table 1 is. It is more like the 1950s than, say, the 1970s or the 1990s. The advent of so *many* technologies—all at once—has several consequences. Adding all of these to U.S. forces is complicated. There is likely to be a tendency to add them without an overall roadmap for their integration with each other, or for their impact on maintenance, training, and operations. The French in the 1930s, for example, added armor and air to their army. But they didn't conceptualize how these new technologies impacted strategy and training. The Germans did, and the result was the French defeat of 1940, even though the French had more tanks than the Germans.

The large number of technologies is likely to have far-reaching consequences. In particular, the potential for synergy is enormous. The number of permutations and combinations rise geometrically with the number of technologies on the list. Modern arms races and strategy are driven by synergy. In the 1950s it was the synergy from the combination of inertial guidance, compact nuclear warhead designs, and solid-fuel rocket engines that led to the Polaris nuclear submarine system. In 1950 it was not clear that any of these technologies would develop, let alone that their synergy would lead to a new class of weapons and entirely new strategies. Polaris created the nuclear strategy of secure second strike, the 24/7 alert, mutually assured destruction (MAD), and limited nuclear options. That is, secure second strike had been around as a concept. But Polaris allowed the strategy to be executed through construction and operation of these submarines.

The items in Table 1 have a feature that's especially important for synergy, and one that makes synergy quite different than all earlier history. *They are IT loaded.* Earlier innovation eras were based on working with “big iron.” Changing the shape of metal objects in complicated ways—for submarines, tanks, aircraft—defined the synergy space. The IT-loaded character of the new technologies means that they can be combined much more easily than bending or cutting big iron. Modular software interfaces, like the TCP/IP protocol and application program interfaces (APIs) are central for synergy now. They are the software analog to interchangeable parts of the industrial age.

Two examples of synergy stand out as especially interesting. One is leadership tracking. In the Cold War there were efforts to track Soviet leaders by bringing together diplomatic intelligence, hacks of mobile radio phones in Soviet leaders' limousines, and direct

observation of vehicle traffic in and around Moscow.² Today this system looks charming in its simplicity. The potential today for advanced technologies to improve on this task is considerable. Here is where the recognition technologies like automatic license plate readers, facial-recognition software, and engine trackers could revolutionize war. These technologies could be combined with hacks into key leaders' mobile phones. This package could be supplemented with hacks of security cameras, police radio chatter, and other inputs. The revelations around the 2016 U.S. presidential election campaign reinforce the importance and sensitivity of this new capability.

This would allow tracking at scale, something the old leadership monitoring in the Cold War could never do. Hundreds of leaders could be tracked. Instead of watching a few limousines, hundreds or thousands of vehicles could be tracked. For a hypothetical example, the top one hundred military officers and leaders of a country could be tracked. To do this would require another technology in Table 1. Big data analytics involves manipulating large databases made up of very different kinds of information. A database of moving targets, automatic license plate readers, hacked security cameras, and cell phones is readily within the reach of today's data management programs. Indeed, this is essentially what Uber, Federal Express, Amazon Web Services, and Walmart do in their daily business.

An intelligence system that tracked vehicles or groups of individuals could provide warning of an impending enemy move. In a crisis there are likely to be "bunching" patterns of people and vehicles. Such patterns could be studied over the years for insights about the enemy alerting process and wartime positioning of forces. Indeed, to even call this "intelligence" is not quite right. Because the information flows are so central to targeting, i.e., resource allocation, the line between intelligence and operations is blurring.

A second example of synergy is to apply this "tracking capacity" to finding enemy missiles. Over the past twenty years mobile missiles have become the preferred basing mode for almost all countries. The United States stands out as one of the few countries that hasn't chosen to go down this road. But China, North Korea, Pakistan, India, Israel, Saudi Arabia, and others have all fielded mobile missiles. This choice is driven from the experience in the 1991 Gulf War. In that conflict virtually all fixed Iraqi targets were destroyed by U.S. air strikes. Only the mobile subsonic cruise unarmed decoys (SCUDs) avoided these attacks.

The technologies described here can be used for tracking mobile missiles. Cell phones, hacked security cameras, license plate readers, and facial recognition can be combined into synergistic packages, supported by big data analytics to keep up-to-date tabs on mobile missile locations and moves.

²This program also listened into the radios of the Moscow police for indications of leadership movement. The program was called Gamma Guppy and it was revealed by a journalist in 1971. Among other things, the program provided some warning of the Soviet invasion of Czechoslovakia in August 1968. Gamma Guppy is described in Matthew Aid, *The Secret Sentry: The Untold History of the National Security Agency* (Bloomsbury Press, 2009), 144–145.

The most important targets of all are missiles armed with nuclear warheads. Mobile missiles have large vulnerabilities to begin with.^{3,4} For example, they require complicated command and control and they are very expensive to operate compared to fixed missiles. Since countries that have gone nuclear in recent years generally have “small” arsenals compared to those of the superpowers in the Cold War, the number of aim points is not particularly great. In the Cold War the sheer number of nuclear weapons was so great that it effectively made a first strike against them infeasible.

The situation in the second nuclear age is different. Nuclear forces are generally small, numbering at most in the dozens or hundreds, while the technologies to track them are becoming quite sophisticated. The effect of this is to seriously jeopardize the second-strike capability of many of the new nuclear weapons states. This leads to crisis instability for essentially “technical” reasons: namely, it creates a fear that a first strike will take out one’s nuclear deterrent. This is a technical development, separate from political and psychological factors that influence crisis behavior. Together, they are likely to add considerably to the problem of nuclear stability.

Interaction of Politics and Technology

How new technologies shape the international order is an important question. Yet it’s surprising how few efforts are made to address it. Most discussions of technology are narrowly framed. They analyze war—that is, the usage of these systems in combat. This is different from international order. Cyberwar, to take an example, is examined in terms of two countries launching and defending cyber strikes at each other. This is a reasonable way to begin an analysis.

But it overlooks an important feature of the technologies: the *synergies* among them. What happens when cyber is combined with other technologies, like precision strike or anti-satellite weapons? Or, what happens when cyberattacks are focused on a rival’s mobile nuclear missiles? New and unexpected combinations of these technologies create new missions that are different from the individual technologies alone. It’s this combined impact, the synergies, that shape the international order.

What is overlooked in much of the war/arms control literature is the larger strategic impacts that technology can have. Technology contributed in the Cold War to remaking world order into two arenas of competition: the superpowers and everyone else. The very notion of power in the international system was defined in terms of these two groupings. Just as technology has its own trends, so does international politics. What is interesting is how the two interrelate, one with the other.

3 See Paul Bracken, “The Cyber Threat to Nuclear Stability,” *Orbis* 60, no. 2 (2016): 188–203.

4 See Paul Bracken, “The Intersection of Cyber and Nuclear War,” *The Strategy Bridge*, January 17, 2017, last accessed October 27, 2017, <http://thestrategybridge.org/the-bridge/2017/1/17/the-intersection-of-cyber-and-nuclear-war?rq=bracken>.

The sheer number of technologies now coming online in so many countries is likely to produce a situation wherein *technology develops more quickly than the strategy for using it*. This is hardly unusual, and likely represents most periods of great technological change.

Most people would prefer to have this the other way around—that is, for some grand strategy to drive technology. I can agree and wish that it were so. If technology were strategy-driven there would be more restraint. It would allow for incremental strategies, and approaches that didn't threaten the security of other countries, civil liberties, or the international order itself. We would be better off. Yet in an era of rapid innovation as we are now in, the convergence of technologies and geopolitical uncertainty make this unlikely. The advantages of holding back on new innovations to signal restraint to other parties has to be weighed against the disadvantages. Repeated attempts at U.S. restraint over the last several years have been met with advances in cyberwar probes and many other technologies by China and Russia, and also North Korea and Pakistan. Faced with both technological *and* geopolitical uncertainty, the risks of falling behind lead many nations to compete for the latest innovations. Significant arms competition is under way around advanced technologies in South Asia, the western Pacific, by Russia, China, and in the Middle East. Of course, the United States is now doing this as well.

However, there is a reluctance by the United States to acknowledge this development. Doing so undermines the premises of the post-Cold War international order. In the United States and Western Europe there is an aversion to calling attention to the political changes now underway in world order. In particular, there is a U.S. desire to avoid any use of the term "arms race" to describe what is taking place in many parts of the world because it connotes a dangerous build-up, reminiscent of the Cold War.

Regional arms races in East Asia, South Asia, and the Middle East underscore a rejection by other countries of the role of the United States as the guarantor of global order. If there were a high degree of acceptance of U.S. security assurances, there would be little reason for countries to develop the new military technologies. The United States would solve the nuclear problem on the Korean peninsula and stabilize South Asia so that Pakistan wouldn't need a nuclear defense. Clearly, the United States isn't fulfilling this role, and for this reason many countries are investing in the new technologies themselves.

Moreover, there is an argument that was first advanced in the 1990s by intellectual and academic establishments at the seeming peak of the new global order. The argument was that challenging the United States for global power status "wasn't worth the candle." That is, that it cost too much and offered too little gain from the effort. It was argued that the United States supplies a "public good" of global order, and that China and Russia should welcome this. An American-led global order got them off the hook for paying for the order they needed to flourish, and which they benefited from. They would "free ride" on this order, the argument went, and the United States was bound to lead even while recognizing that others were not contributing their fair share to the global order.

China and Russia showed few signs of ever actually believing any part of this story. More, they were not trying to replace the United States in a global role. Rather they were challenging the U.S.-led order in regions where they were strong and the United States was weak, namely those geographic areas close to them. It was a lot like the Soviet Union challenging the United States in the Caribbean in the cold war. It could be done, but the odds were stacked against success.

The existence of simultaneous arms races in South Asia, East Asia, the western Pacific, the Middle East, and parallel technological arms races in anti-satellite weapons, hypersonic missiles, cyberwar, drones, and nuclear weapons (Pakistan, North Korea, Israel, perhaps Iran) undercuts the U.S. contention that the basic world order of the 21st century is largely agreed upon. It says that there is a fundamental uncertainty about this order in the minds of others. As many countries invest in advanced technologies, this abets a further dispersion of power, which moves the international order to one of multipolarity.

Especially significant in all of this are nuclear weapons seen in the context of the technological revolution of Table 1. If multipolarity is to mean anything, it means that most of the major powers in it will have their own nuclear forces—in fact, most of them do already. The United States, Britain, France, Russia, China, and India belong in this major power group. Japan and possibly Brazil stand out since they are not nuclear weapon states.

What is unknown—what is unthought about—is how the other technologies on the list might reshape the nuclear balance among major powers. Perturbations of this balance arising from, say, cyber or drones, could have a disproportionate impact on U.S. nuclear modernization because they could change the public perception of what constitutes national security.

The U.S. election in 2016 indicates a shift in the alignment of U.S. domestic and international politics. Instead of the dominant themes of the post-Cold War order, and the necessity of U.S. global leadership, there appears to be a move to negotiation with other major powers (Russia) and an unwillingness to carry the burden of victory in the Cold War alone. At least, arguments in this direction, arguments that international stability rather than global leadership is what matters for the United States, are getting a greater hearing than at any time since the immediate aftermath of World War II.

The spread of advanced technology counters the image of a world system with a sole superpower, the United States, as the least bad alternative supplier of international order. As this evolves, the United States could shift gears and frame the new technologies in a very different way. Instead of seeing the new technologies as a way to lead a world seeking its leadership, the United States could gradually accept the security requirements of a multipolar order. In many respects this is a much easier task than leading the world. At any rate, it has fewer of the contradictions of trying to preserve a unipolar world achieved by American technological leadership.

Conclusions

For the next decade or so it seems quite likely that strategy will lag technology, and that many countries will invest in the advanced technologies without a clear thought of goals or plans as to why they are doing so. The real reason is that they fear falling behind, and because they may look weak if they lack certain of the new technologies.

The United States is in a special position. It looks willing now to redefine the problem of international order away from something it designs to one that gradually allows a multipolar system. This has enormous implications for advanced technology that are for the first time being debated. The idea that technology can offset both smaller force structure and declining domestic support for global intervention seems to be recognized as something that just isn't feasible. The new program of using advanced technology for keeping international order in a world where major powers have lost the monopoly they once had has yet to be worked out.

Chapter 7

New Is Not Always Better

David S.C. Chu, with the assistance of Allison Fielding Taylor¹

Our Framework and the Assumptions It Implies

A premise of our volume is that economic models can be brought to bear on the challenge of threat warning. “By understanding the rational requirements of a threat actor, the range of technology necessary to fulfill objectives will be narrowed and thus become tractable for analysis.”²

Competing economic assumption sets, however, can affect *which* economic model is selected as the forecasting tool, or how the selected model is employed, and thus the forecast offered. An oft-told joke about economists recounts the experience of a graduate student returning to his alma mater, a decade after earning his degree. He seeks out his favorite professor, who is proctoring an examination. Taking a seat, he glances at the exam questions, and is startled to discover that they’re identical to the ones posed to his class years ago. When the exam concludes and he engages her in conversation, he naturally inquires, “Why are you repeating the questions? Aware of what you’re asking, students will have prepared their responses in advance—this won’t really test their knowledge.” She smiles, “Remember, in economics we don’t change the questions—we just change the answers!”

Assumptions, of course, drive both model selection and answers. One key assumption is that the application of new technology to military problems will produce better answers.

¹ The ideas advanced in this chapter reflect solely the conclusions of the authors and should not be seen as representing the Institute for Defense Analysis or its sponsors.

² Report of the Expert Advisory Panel Workshop, *Strategic Latency and Warning: Private Sector Perspectives on Current Intelligence Challenges in Science and Technology* (Livermore: Lawrence Livermore National Laboratory, January 8, 2016), 13. Also available at: <https://cgsc.llnl.gov/content/assets/docs/StrategicLatencyReport.pdf>.

Analysts are drawn to “the new” by this assumption of superior results (especially since we’re not familiar with the new technology’s drawbacks). But is new consistently better? Put differently, the “old” may be capable of generating new answers, and may thus pose a more serious challenge to us than anything “the new” can produce. Moreover, if history is any guide, our ability to forecast how “the new” will play out is shaky indeed.

Can a discussion of alternative assumption sets (and alternative models) help us understand the relationship between new technologies and military prowess? The attractiveness of the rational economic model is that it organizes an otherwise confused landscape for the intelligence community. But it may be even more powerful to examine the assumptions being employed to determine if the model we have in mind will indeed produce answers that are accurate, and useful to the decision-maker.

Exploring the Framework

One assumption is that decisions about technology are being made by a nation-state (or something approximating one), reflecting the further implicit assumption that only a nation-state can mobilize and direct the resources to create any significant technological threat.

A first issue, therefore, involves who is making the decisions, and the mindset brought to bear by those parties. The assumption of nation-states is consistent with recent concerns related to Russia and China. But looking at the range of conflicts in which the United States has been involved since the late 1890s, it’s remarkable how many times we’ve faced something different—an insurgency, or recently, metastasizing terrorist challenges. For insurgents and terrorists, theories of group decision-making and group dynamics may be more powerful predictors than the rational maximizer of the economic literature. Moreover, even for a nation-state, “non-rational” factors may be important. Military history offers many examples of slow technological adjustment—e.g., the continuation of horse cavalry well after the advent of mechanized platforms.

A second issue is the kind of technological developments that should be the focus of the intelligence effort. Are we interested in “new” technology, or technology whose application is particularly disruptive? A number of the current challenges certainly do not involve new technology, or even high technology—Russia’s “little green men,” China’s building island bases in the South China Sea (perhaps not all that different from what the United States did to Diego Garcia), and the difficulties that Improvised Explosive Devices (IEDs—really, mines) pose for the United States in Iraq and Afghanistan.

A third issue is the reliability of any forecasts we could plausibly construct. The Global Positioning System offers a case in point. Participants in the January 1981 debate among outgoing Carter Administration appointees confided that the Department of Defense leaders struggled to find a compelling military rationale for approving the system, eventually concluding that while the case was not as strong as they’d prefer, the incoming Reagan Administration might as well be given something at least this useful on which to spend

a larger defense budget, versus some of the other enthusiasms that might be funded!³ We all know now how transformational it was—with many if not most of the non-military applications likewise not perceived at the time.

In 2008 a *Wall Street Journal* reporter took a look at the technology forecasts that paper had offered ten years earlier:⁴

Now that the results are in, it's clear that the prognosticators were on safest ground when predicting details about the raw capabilities of high-tech devices. But the seers had a harder time predicting how this fast-changing technology would alter people's habits...

Even those with the foresight to invest in the development of new technologies may not appreciate their potential, or act quickly enough to exploit the possibilities presented—especially if the enterprise is currently successful with a different approach. The continued affection of the United States Navy for the battleship right up to (and past) December 7, 1941, despite having developed the aircraft carrier, is an obvious example. Likewise well known is the story of Kodak. It invented and patented the first digital camera in 1975. But with its dominant position in both U.S. analog camera and film sales, it stuck with those technologies—and went bankrupt in 2012.⁵

That pattern raises a fourth issue: Rather than emphasizing forecasts of how new applications of technology might undercut any military advantage we enjoy, should the emphasis be on the agility of our reactions to new developments? We might especially hone our ability to react to non-state actors. They could well present the most difficult challenges, because they are the least likely to observe the norms of nation-states to which we are accustomed, and that shape our thought patterns. As others have pointed out, few took seriously the prospect of using civil airliners as weapons before 9/11 (particularly with pilots possessing very limited training). Non-state actors are typically not well understood, and they may have less to lose if an unusual approach fails to work, thus being more willing to try it. Their amorphous character makes forecasting “next moves” especially problematic.

The balance of this chapter takes on these four issues—really, four questions—about how technologically based initiatives by opponents might unfold. It briefly discusses in its

3 Author's conversation with a key participant.

4 George Anders, “Predictions of the Past: How did we do the last time we looked ahead 10 years? Well, you win some, you lose some,” *The Wall Street Journal*, January 28, 2008, last accessed October 27, 2017, <http://www.wsj.com/articles/SB120119993114813999>.

5 Avi Dan, “Kodak Failed by Asking the Wrong Marketing Question,” *Forbes*, January 23, 2012, last accessed October 27, 2017, <http://www.forbes.com/sites/avidan/2012/01/23/kodak-failed-by-asking-the-wrong-marketing-question/#780decb57dd7>.

conclusion what the potential answers to those questions might imply for our policies.

A First Question: How Rational Are Decision Makers?

The inconsistencies of human decision-making have long troubled economists. One of the famous puzzles is why people both gamble *and* buy insurance. From the economist's perspective, one behavior or the other is rational, but not both, under standard assumptions about consumer preferences.⁶

Economists ground their calculus of choice in the preference functions of those making decisions. A variety of elements shape those preferences, often bundled up under the heading "cultural factors." Those factors may have historical antecedents—for example, the difference in legal philosophies between those countries that adopted the Napoleonic code, and those that preserved the Anglo-Saxon tradition. Likewise, you see significant differences across countries in whether and how excellent service should be rewarded (to tip or not, how much, etc.). Societies may create differing regimes to address common problems, or to accommodate religious or political standards—for example, Islamic banking, or French versus German decisions on energy sources (nuclear vs. renewable emphasis).

The United States is certainly not immune to these "cultural" constraints on rationality. Witness the controversy that erupted when the American military started to create a weapon that would blind opposing soldiers, but allow them to live. The ensuing domestic political uproar forced cancellation of the program.^{7,8} (Weapons that kill or completely incapacitate remain acceptable, however!)

Such constraints may vary across elements of a society or organization thought otherwise homogeneous in their preferences. Certainly that's true of the American military. One constraint is simply the desire for bureaucratic independence. That's presumably the explanation for one of Secretary of Defense McNamara's most amusing failures: the drive to select a single belt buckle for military uniforms. Notwithstanding possible savings from what one would think is a mundane item not subject to significant separate opinions, Mr. McNamara failed to get the individual military services to agree.⁹

6 As Kenneth Arrow phrased it, "This assumption [of diminishing marginal utility] may reasonably be taken to hold for most of the significant affairs of life...but the presence of gambling provides some difficulty in the full application of this view." Kenneth J. Arrow, "Uncertainty and the Welfare Economics of Medical Care," *The American Economic Review* LIII, no. 5 (December 1963): 959.

7 "Pentagon Cancels Controversial Laser," *L.A. Times*, October 13, 1995, last accessed October 27, 2017, http://articles.latimes.com/1995-10-13/news/mn-56562_1_laser-weapons.

8 *Protocol on Blinding Laser Weapons (Protocol IV to the 1980 Convention)*, 13 October 1995, International Committee of the Red Cross, last accessed October 27, 2017, <https://ihl-databases.icrc.org/ihl/INTRO/570>.

9 "Buckles and Beer." *Chicago Tribune* April 1, 1964: p. 16. Also available at: <http://archives.chicagotribune.com/1964/04/01/page/16/article/how-to-keep-well>. Last accessed October 27, 2017.

More serious are the disagreements that affect the design of military platforms and/or their employment. Two immediately come to mind: The Navy's refusal to consider a single-engine aircraft in the Lightweight Fighter Competition of the 1970s, and the difference in attack helicopter tactics between the United States Army and Marine Corps. In the former case, the disagreement precluded buying a common aircraft for the Air Force and the Navy (as readers know, the Air Force developed the F-16, the Navy the F-18). In the latter case, as may be less well known, the Army continued to deploy and upgrade "scout" helicopters to identify targets for its Apaches, while the Marine Corps disdained any such "requirement" for its attack helicopter force.¹⁰

A classic example of the power of ex ante preferences over choices is the long struggle to persuade American military leaders to accept unmanned platforms (cruise missiles, unmanned aerial vehicles (UAVs)). Even after the deployment of UAVs, the United States Air Force insisted that rated pilots "fly" them (and observe the same medical limitations that applied to pilots flying at altitude), while the other services used enlisted personnel (and relied more heavily on automation to control the flying article).¹¹

The leader's preference can take a military service down an unproductive path. Perhaps the best recent case is the Army's pursuit of a new generation of networked vehicles, the Future Combat System. Senior career Army technical experts concluded at an early stage that this approach could not succeed, but felt powerless to confront the Chief of Staff's agenda and preclude what was later seen by many to be a serious error.¹²

Perhaps a more fundamental error in technology management is the focus on the platform vice the system, or how that system is employed in a military operation or campaign. Those larger subjects inevitably involve other issues, including logistics (what some argue should be the focus of strategists)¹³ and the human dimension of warfare ("human capital" as it's often termed), a subject to which we return in the conclusion of this chapter.

There are at least two implications of these bounds on "rationality" that affect forecasting how others might adopt technology to their purposes. First, it would be powerful to understand the cultural context, so to speak, in which they make their decisions. Do we understand the constraints that their societies may impose on them, both limiting acceptable choices and channeling their energies in particular directions? Second, do we understand how these constraints may differ across the principal elements of the enterprise

10 In the debate over this issue during the 1980s, General Jack Vessey (then Vice Chief of Staff and the senior Army officer present) volunteered that the Army's preference probably reflected the cavalry tactics that it honed on the 19th century frontier (Author's recollection).

11 The Air Force Chief of Staff acknowledged that service cultures affect the solutions they recommend: "...we each approach a problem from a slightly different perspective based on our service culture, which is a byproduct of the domains we're responsible for." From "An Interview with Gen David L. Goldfein.," *Strategic Studies Quarterly* 11, no. 1 (2017): 11.

12 Author's exchange with the Deputy Under Secretary of the Army for Operations Research.

13 Michael Schrage, "When Logistics Beat Strategy," *Fortune*, February 1, 2013, last accessed October 17, 2017, <http://fortune.com/2013/02/01/when-logistics-beat-strategy/>.

making the choices, much as they differ across major elements of the American military? Understanding these channeling forces may importantly improve our ability to characterize the set of likely choices. While such understanding will not necessarily produce a forecast by itself, it may allow us to characterize the likely future space, narrowing the range of uncertainty, and among the elements of that space, facilitating probabilistic assessments of what is more likely, and what is less so.

Moreover, this approach to forecasting may help us deal with the reality that opponents to U.S. security interests will arise outside of nation-states. It may be more difficult to understand these cultures, but focusing on the history and norms of the insurgent or terrorist group may help us understand the directions it's likely to take, and those it may reject.

Indeed, this emphasis on behaviors (vice rationality) invites considering how we might apply a recent enthusiasm of some: behavioral economics, or “freakonomics” as one author entitled it.¹⁴ This approach to thinking about human decision-making has gained considerable favor in the business world (e.g., leading to an emphasis on “opt out” versus “opt in” policies in designing benefit programs to which you would like employees to subscribe). It has received far less attention as a way to think about problems in the military sphere; perhaps we should reflect on how it might be helpful.

As a broad generalization, American military doctrine assumes we can control behaviors by attacking “targets” and the opponent’s ability to command and control its forces (“leadership”). We therefore invest in capabilities designed to carry out campaigns with these ends in mind. We’re also intrigued by exchange ratios, whether those are expressed in terms of casualties or the cost of producing an effect as opposed to its countermeasure. But what if these design parameters misunderstand the motives that drive our opponents?

To take an example from our own history, the Revolutionary army won few battles (i.e., killed a disappointing number of targets, and suffered from a poor exchange ratio). Granted, it avoided disaster. But as some historians now argue, Washington’s major achievement was keeping it intact, something that Great Britain had to deal with—a burden that it eventually deemed unattractive.¹⁵ In today’s struggles with terrorist non-state actors, we, like the British, win many battles, but seem unable to bring the war to a successful conclusion. Worse, some of our “successes” appear only to have spread the affliction to new locations. Like the British, our cultural definition of rationality misdirects our energies, leading to

14 The collection of *Freakonomics* books by Steven D. Levitt and Stephen J. Dubner are described & available here: <http://freakonomics.com/books/>, last accessed October 27, 2017.

15 As the Mount Vernon website observes, “To the world’s amazement, Washington had prevailed over the more numerous, better supplied, and fully trained British army, mainly because he was more flexible than his opponents. He learned that it was more important to keep his army intact and to win an occasional victory to rally public support than it was to hold American cities or defeat the British army in an open field. Over the last 200 years revolutionary leaders in every part of the world have employed this insight, but never with a result as startling as Washington’s victory over the British. The Mount Vernon website echoes the conclusion of Ron Chernow in his Pulitzer-prize-winning biography *Washington: A Life* (New York: Penguin Books, 2010), and that of other historians.

erroneous conclusions about the technologies our opponents might employ, and what our best responses might therefore be.

A Second Question: How Rapidly Is Technology Changing?

Contemporary observers of military affairs argue that technology is changing rapidly, with the implication that we must respond appropriately.¹⁶ A good deal of attention is focused on developments related to information technology, especially those facilitating rapid decision-making, and the ability to fit significant computing power in very small spaces. Paired with advances in sensors that have taken place over the last century, these developments create the possibility of autonomous systems, an enthusiasm the Defense Science Board has endorsed.¹⁷

The belief that technology is changing rapidly leads naturally to a call for the Department of Defense to lead that change in directions advantageous to its interests. Indeed, Deputy Secretary of Defense Robert Work, reflecting that perspective, has called for a “Third Offset” in military technology, to give the United States a decided advantage over its possible opponents.¹⁸ A Long Range Development Program was constructed to pursue such technological advantage, with initial investments proposed in the President’s Budget Request for Fiscal Year 2017.

Vaclav Smil’s *Creating the Twentieth Century*, however, argues for just two great bursts of technological change across history—one in the Han dynasty (involving agricultural implements, horse power, and the use of iron), and the second in the two generations preceding World War I (involving material and chemical processes, energy sources, and prime movers).¹⁹ He acknowledges the later development of nuclear fission, but argues its limited commercial application makes it much less significant to human activity—even though it has had a transformative effect on the nature of potential warfare.

16 Department of Defense, Defense Science Board. *DSB Summer Study Report on Strategic Surprise*. (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, July 2015), 1. Also available at <https://fas.org/irp/agency/dod/dsb/surprise.pdf>. See as well the various statements by Deputy Defense Secretary Robert Work, e.g., *Remarks by Deputy Secretary Work on Third Offset Strategy As Delivered by Deputy Secretary of Defense Bob Work, Brussels, Belgium, April 28, 2016*, last accessed October 27, 2017, <https://www.defense.gov/News/Speeches/Speech-View/Article/753482/remarks-by-d%20deputy-secretary-work-on-third-offset-strategy>.

17 Department of Defense, Defense Science Board. *Task Force Report: The Role of Autonomy in DoD Systems*. (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, July 2012). Also available at: <http://www.fas.org/irp/agency/dod/dsb/autonomy.pdf>, last accessed October 27, 2017.

18 “Offset,” in Mr. Work’s construct, refers to decisive U.S. advantages in the Cold War that compensated for the numerical superiority of Soviet forces in the center of Europe. The first offset, in this interpretation of history, involved tactical nuclear weapons, the second, precision targeting of munitions. *The Third U.S. Offset Strategy and its Implications for Partners and Allies*, as delivered by Deputy Secretary of Defense Bob Work (Willard Hotel, Washington, DC: January 28, 2015). Transcript available at: <http://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies>, last accessed October 27, 2017.

19 Vaclav Smil, *Creating the Twentieth Century: Technical Innovations of 1867–1914 and Their Lasting Impact* (Cary, NC: Oxford University Press, Inc., 2015.)

A review of economic history would certainly agree that productivity gains in the commercial economy—for which technological change is one important source—occur discontinuously, whether that’s over the course of particular periods or over the long haul. There have been periods of history where major regions experienced no change in productivity—the millennium preceding the Industrial Revolution in Western Europe, for example. Likewise, Robert Gordon’s magisterial history of the American economy argues that the hundred years recently concluded were a period of unusual productivity gains for the United States (derived in no small part from the innovations cited by Vaclav Smil among other factors), unlikely to be replicated in the generation ahead, much as we might have assumed that’s the norm, and thus the foundation of our political expectations.²⁰

If technology is *not* changing that rapidly, an emphasis on those changes that are occurring may be a mistaken strategy. Certainly we should be alert to any possibilities they create. But a larger set of possibilities may await us by asking how we might better use the technologies we already understand. Engineering—using in an improved manner what we already know, or combining those technologies in a more effective way—may be a dominant approach.

It’s certainly likely to be less risky. As the troubled development of the newest aircraft carrier for the U.S. Navy demonstrates, pursuing several new technologies at once can be a recipe for difficulties.²¹ And the new technology may create a different set of vulnerabilities, as the present-day worry about cyber exploitation so pointedly embodies.

Moreover, new technology may not always provide an edge in solving military problems, as the long controversy over close air support illustrates, pitting the U.S. Air Force preference for a more “modern” aircraft against the older set of technologies embodied in the A-10 (or even the venerable Skyraider).

Put differently, technological change enlarges the set of ideas available to us in solving military problems. It’s a supply effect. What we pursue is also driven by demands—what military problems are we trying to solve, and what physical items embedding technology might be part of solutions? And as the previous discussion of rationality argues, the technological choices we make may be shaped by the assumptions we bring to bear in understanding how our demands interact with what technology can offer.

An example from the early history of passenger jet aircraft illustrates nicely the relationship between assumptions and technological choices. The British developed the Comet aircraft postulating it would have to take off from existing airports, with their relatively short runways. That required an aircraft whose power requirements relative to its size made

20 Robert J. Gordon, *The Rise and Fall of American Growth: The U.S. Standard of Living Since the Civil War* (Princeton, NJ: Princeton University Press, 2016.)

21 Frank Kendall, Under Secretary of Defense for Acquisition, Technology and Logistics, has concluded, “With the benefit of hindsight, it was clearly premature to include so many unproven technologies in the GERALD R. FORD.” Frank Kendall, Under Secretary of Defense for Acquisition, Technology and Logistics, *Memorandum for the Secretary of the Navy. Subject: CVN 78 GERALD R. FORD Class Aircraft Carrier Program*, August 23, 2016.

it expensive to operate. Boeing, in contrast, essentially assumed that an economically attractive aircraft would trigger the necessary investment in longer runways. There were other factors involved, of course, including the subsidy to Boeing from the U.S. Air Force tanker program. But we all know how that contest turned out: the more ambitious assumptions produced the template for jet aircraft that the international community has followed down to the present day.²²

A Third Question: How Should One Characterize the “Market” for Military Technology?

Decisions about military technology take place within an institutional setting—a “market,” to keep up the economics analogy. That may be formal (a Ministry), or informal (the process of some non-state actors). Thinking about the decision-making process as a market allows us to bring to bear insights about how such markets might work.

Technological forecasts focus on the supply side—what might be possible. Equally if not more important may be the demand side—that is, the preference functions of decision-makers that drive the capabilities they’d like to have, and how they’d like to create those capabilities. Significantly informing those preference functions may be (and should be) the operational concepts implicitly or explicitly assumed by those making decisions.

Preference functions will probably vary across communities within the institution, or the institutional process that is the locus of decision-making. Uniformed leaders in an established military are likely to have views informed by doctrine, and doctrine may be importantly influenced by that military’s history. It should be no surprise, then, if uniformed leaders seem inclined—as the critics put it—to fight the last war. Such a perspective favors approaches and platforms that were last successful, with changes adopted as technology permits to correct perceived shortcomings or enhance perceived advantages (e.g., range, accuracy, lethality). Certainly that characterizes American decisions since the end of the Cold War—largely improving upon what was deemed successful in the long struggle against the Soviet Union.

Political leaders may have different views. They may be willing to challenge doctrinal norms, and use their political skills to override countervailing military judgment. It was civilian leadership, for example, that led to a shift in the basing of U.S. nuclear bombers from vulnerable positions in Europe to airfields in the northern United States, capitalizing on the concept of aerial refueling.²³

22 For a discussion of British vs. U.S. design choices see Grant Simons, *Comet! The World’s First Jet Airliner* (South Yorkshire: Pen & Sword Aviation, 1988.) See also http://www.dmflightsim.co.uk/vickers_vc10_history.htm, last accessed October 27, 2017.

23 The seminal civilian analysis: Albert Wohlstetter et al., “Selection and Use of Strategic Air Bases.” (Santa Monica, CA: RAND Corporation, 1954), last accessed October 27, 2017, <http://www.rand.org/pubs/reports/R0266.html>. The shift is summarized in: Steven L. Rearden, *Council of War: A History of the Joint Chiefs of Staff (1942–1991)* (Washington, DC: Published for the Joint History Office, Office of the Director, Joint Staff, Joint Chiefs of Staff, 2012.)

That is not to argue that the judgment of political leaders is necessarily superior. Secretary McNamara's unsuccessful insistence on a common Navy/Air Force fighter bomber, procured under a fixed price regime (the infamous TFX), is a classic example.^{24,25} Navy Secretary Lehman's advocacy for the V-22 provides a somewhat different case in point. Not originally the Marine Corps' choice for replacing its vertical lift capability—although advocated by some in industry—he successfully insisted on its selection. To Secretary Lehman's leadership credit, the Marine Corps united around it, and fended off Secretary of Defense Cheney's challenge to its costly nature.²⁶ In the event, actual costs of the V-22 far exceeded those that underpinned Secretary Cheney's concern.²⁷

A third group of participants and their preference functions may be especially important in understanding military technology choices. You might call them entrepreneurs—those arguing for a different design choice, although often within the context of accepted notions of warfare and warfare platforms. A variety of examples from the American experience during the Cold War come to mind—the Lightweight Fighter Competition (which led to the F-16 and the F-18), Admiral Rickover's role in building a nuclear-powered Navy, and the development of the Aegis missile system. That the entrepreneur was able to prevail typically reflected backing from political leaders, who saw promise in the design choice, and who in backing that choice were not fundamentally challenging the nature of military needs.

Characterized in this manner, military markets may be quite stable over long periods of time—and significant disruption may only occur as a result of a major loss of confidence in existing practices (e.g., from overwhelming defeat of forces so constituted, perhaps due to the failure of the assumed operational concepts) or a technological development so overwhelming it can't be ignored, much like the atomic bomb transformed the political/military calculus.

A Fourth Question: What Does It Take to Deploy “New” Technology?

Quite apart from the question about how “new” the technology might really be, to the extent that a different technology is selected, what elements of the execution process are likely to promote success?

Judging from the American experience in the Cold War, at least six elements are critical:

24 Arnold Lewis and Michael Durao, “Is the Common Fighter Really a Pipe Dream?” *Beowulf Defense & Security*, February 28, 2011, last accessed October 27, 2017, <http://www.beowulfdefense.com/1/post/2011/02/is-the-common-fighter-really-a-pipe-dream.html>.

25 “Tactical Fighter Experimental TFX,” *GlobalSecurity.org*, last accessed October 27, 2017, <http://www.globalsecurity.org/military/systems/aircraft/txf.htm>.

26 On Secretary Lehman sale, see Robert Bryce, “Texas’ Deadly \$16 Billion Boondoggle,” *Texas Observer*, June 18, 2004, last accessed October 27, 2017, <https://www.texasobserver.org/1679-texas-deadly-16-billion-boondoggle-even-dick-cheney-couldnt-kill-the-v-22-helicopter/>.

27 *Ibid.*

First is the issue of the original choice: have you really considered a reasonable range of alternatives to meet mission needs, and is the alternative selected truly superior? The history of systems acquisition is pockmarked with unfortunate choices—choices that were clearly not well thought through for their operational plausibility (think Maginot Line), their broad applicability (the Army's Gama Goat, overly focused on the specifics of South Vietnam's rice paddies), or their tactical viability (e.g., TV's *Maverick*, Division Air Defense (DIVAD)).

Successful choices may enjoy a long life—the AC-130 gunship is an example. That example also illustrates how combining older technologies in a new package—basically a howitzer mounted in a C-130—can produce dramatically improved results. And it underscores the importance of a second element: incorporating the technological choice in a viable operational concept.

A third element is the importance of manufacturing reliable articles. The Soviet Union often produced designs of considerable sophistication. But they were equally likely to break down in field operations.²⁸ Ensuring the system will perform reliably, and that its maintenance will not impose an undue burden on military forces, is essential to force effectiveness.

Moreover, it is the system that is important, not just the specific component embodying new technology—a fourth element in pursuing success. Nowhere is this better illustrated than in the search for effective missile defense. While much attention is paid to the missile in the defensive system, and its kill mechanism, much of system effectiveness will depend on the sensors the system deploys, including their ability to deal with decoys.

A fifth element, for which American performance in World War II is the frequently cited example, is the ability to mobilize the resources necessary for production. That was true not only at the “macro” level; it was true for individual systems and suppliers. For example, those who designed the Jeep—creating a storied success of American war production—lost out in the actual contest to manufacture it because they could not put together a production line, especially on the scale that was needed.²⁹

Ultimately—the sixth element in success—you must be able to deploy the chosen article effectively. Iraqi versus American performance in the first Persian Gulf War offers a recent case in point. The Iraqis actually possessed some quite advanced equipment, but they were not able to utilize that equipment well, for a variety of reasons. In contrast, United States forces displayed a high degree of proficiency in using their equipment—a tribute in many

28 See, for example, James Dunnigan, “Russia Curses Its Crappy Engines,” *Strategy Page*, September 21, 2014, last accessed October 27, 2017, <https://www.strategypage.com/dls/articles/Russia-Curses-Its-Crappy-Engines-9-21-2014.asp>.

29 D. Denfield and M. Fry, *Indestructible Jeep* (New York: Ballantine Books, 1973), 31–36, 41, 46.

respects to its “human capital”—that has deeply influenced the military investments of a number of major powers.³⁰

The morale of military units, including their willingness to fight, and the importance of effective leadership are repeatedly raised as issues in military history. But the human-capital element of success reaches beyond these two points, and embraces at least two others, both characteristic of the contemporary American All-Volunteer Force: How able are the individuals in the ranks, and how proficient are they in carrying out their responsibilities?

Coming out of the difficult lessons of the 1970s, the United States made two crucial decisions in its military personnel policies: it would set high cognitive standards for enlisted personnel, and it would insist on extensive and realistic training. The favorable results of these policies can be seen in the performance of units in the field, and the degree to which other militaries have attempted to emulate that outcome with similar steps.

Implications

As the response to the first question argues, if the decision challenge is anticipating or responding to the actions of a competitor or opponent, it is critical to understand the competitor’s objectives, viewed in its political and cultural context, not ours. That includes the constraints under which the competitor is operating. From our point of view, the competitor’s choices may not look rational, but they may be very rational from that actor’s perspective. Recent reviews of North Korea’s actions provide an excellent example.³¹

As one thinks about creating more useful intelligence forecasts, the answer offered to the third question argues we should pay particular attention to leader communities within competitors and opponents, and to the institutional mechanisms within which they are making decisions. Are they pointing in new directions? To what extent do their literatures indicate either support for new directions, or opposition?

A focus on competitor objectives, and the leader communities, will help guard against undue fascination with new technology as the pre-eminent problem. As we have seen in the long “wars on terrorism,” it is the mine (a very old idea) that has proved especially challenging, now known by the new name of “Improvised Explosive Devices” (IEDs).

A thoughtful consideration of objectives is not just the starting point for an intelligence forecast. It’s equally important for thinking about our own choices. As the response to the third question argues, we may be too conservative in our choices—too wedded to the

30 This point has been made by a number of observers, including MAJ Gilberto Villahermosa, *Desert Storm: The Soviet View* (Foreign Military Studies Office, Fort Leavenworth, KS), last accessed October 27, 2017, <http://fmso.leavenworth.army.mil/documents/RS-STORM.HTM>.

31 Max Fisher, “North Korea, Far From Crazy, Is All Too Rational,” *New York Times*, September 10, 2016, last accessed October 27, 2017, http://www.nytimes.com/2016/09/11/world/asia/north-korea-nuclear-missile-programs-rational.html?_r=1.

tried and true. That's especially perilous if the circumstances that made those choices appropriate in the past have now changed enough that the same approaches are unlikely to yield commensurate benefits in the future. Decision-makers might wish to give more "voice" to the "entrepreneurs."

But how to choose among the contending ideas? Economists would argue that competition offers a good way forward. In that regard, the consolidation among defense suppliers during President Clinton's first term might be seen as a strategic mistake, at least from this perspective.³² In reinvigorating competition, the genius lies in structuring events that yield insights on mission accomplishment, not just technical parameters—and performance of the *system* being proposed, not just a single platform or weapon. Critical to that performance evaluation is the operational concept—how will the systems be used to achieve military objectives?—and the contribution of success in meeting those objectives to the outcome of any campaign supporting larger national security goals.

Without competition, the institutional structure of U.S. weapons development favors continuity and stability, not disruption. For most major platforms, the marketplace is at best an oligopoly, with high entry costs for new players. Besides the physical capital requirements, federal contracting rules require specialized expertise to play successfully, and the complex technologies involved can present a daunting need for scarce human capital. And even if recent DOD efforts on the supply side succeed (e.g., DIUX), they do not address the demand-side failing.

How, then, might we create a competition among new ideas, and between new ideas and established practices? One possibility is competitive prototyping for particular missions. Competitive prototyping could encourage proposals that reassemble existing technologies in a better way, or proposals that advance a truly new technological approach in a cost-effective manner. Prototypes need not embed every feature of the envisioned product, just enough to test the effectiveness proposition. Prototyping also has the benefit of encouraging experimentation,³³ often the source of transformative military ideas (think the 11th Air Assault Division, out of which came the notion of using helicopters for tactical transport on a significant scale in a combat environment).³⁴

New entrants may find such prototyping attractive, but established producers may not. The reason is simple: relative to their capital investment, R&D is not an important source of profits. Rather, it's production. An emphasis on competitive prototyping might

32 Leslie Wayne, "The Shrinking Military Complex; After the Cold War, the Pentagon Is Just Another Customer," *New York Times*, February 27, 1998, last accessed October 27, 2007, <http://www.nytimes.com/1998/02/27/business/shrinking-military-complex-after-cold-war-pentagon-just-another-customer.html>.

33 Richard Van Atta et al. advance this combination of ideas—prototyping and experimentation—as a way to accelerate systems acquisition. See Richard Van Atta et al., *Assessment of Accelerated Acquisition of Defense Programs* (IDA paper P-8161, September 2016), vii–viii, 65–66.

34 Richard W. Kedzior, *Evolution and Endurance: The U.S. Army Division in the Twentieth Century* (Santa Monica, CA: RAND Corporation, 2000) Also available at: http://www.rand.org/pubs/monograph_reports/MR1211.html, last accessed October 27, 2017.

well encourage some degree of separation of design from production, which could be constructive (even if it is reminiscent of the Soviet system).³⁵

Competitive prototyping, however, should not be judged solely on the frequency with which new designs are adopted. Indeed, there's likely some optimal rate of failure, accepting the notion that we may learn as much from our failures as our successes (and perhaps occasionally more).

Both for forecasting what we might face, and deciding how to invest our own resources, the answer to the fourth question encourages a focus on two issues: can we (or the competitor) produce reliable articles, and can the training and other ingredients of human capital be assembled, so that the new developments can be exploited effectively?

Indeed, human-capital characteristics and the capacity to retrain quickly may be key ingredients in our ability to respond with alacrity to new and unexpected developments. Understanding promptly the characteristics of the new situation and translating that into a repurposing of what we already possess, perhaps through a revised training regime, may give us a faster response than focusing immediately on new technology—even if that new technology should be pursued as part of a long-range solution.

It will be easier to repurpose existing systems if their original design allows generically for such adjustment (e.g., through weight and power margins). As two incremental dynamic analysis (IDA) analysts argue, if we “prepare to be wrong,” we are more likely to get it right when confronted with a changed set of challenges.³⁶

Notwithstanding what we might do to improve our forecasts of competitor's choices, and mount anticipatory investments, inevitably surprise is likely to dominate. Indeed, to the extent that we anticipate and counter one development, our forecasts could move competitors in different—perhaps less well anticipated—directions. Thus, our ability to react quickly and effectively to unforeseen or misperceived developments will remain critical. The talent we need may be less a skill at strategic warning than strength in strategic adaptation—mobilizing resources not just to counter the immediate effects of the surprise (as the United States did with its Mine Resistant Ambush Protected Vehicles—MRAPS—in Iraq and Afghanistan), but to secure in the ongoing competition a decisive advantage for ourselves.

A long-term competition will produce different “answers” as the problem changes, and as our assumptions change. That reinforces the importance of being clear about our objectives. It also reinforces the importance of linking the concepts of operation within which systems and training are pursued to the military campaigns undertaken in pursuit of

35 Arthur J. Alexander, *Design to Price from the Perspective of the United States, France, and the Soviet Union* (Santa Monica, CA: RAND Corporation, 1973.) Also available at: <http://www.rand.org/pubs/papers/P4967.html>, last accessed October 27, 2017.

36 Prashant R. Patel and Michael P. Fischerkeller, *Preparing to Be Wrong* (IDA document NS D-5774, April 2016).

those objectives. What count are capabilities and outcomes, not systems or technologies per se. To adapt a trite truism, new is not always better—better is better.

Chapter 8

What's Old Is New Again: Nuclear Capabilities Still Matter—and Will for a Long Time to Come

Joseph F. Pilat

Introduction

What is needed and how long does it take for a state or non-state actors to acquire nuclear weapons? These related questions have been at issue in recent debates over the nuclear dangers posed by proliferation. They have been at the heart of the urgency surrounding, and consequently the means used to eliminate or manage these threats. The questions have arisen in recent years in the context of the time necessary for Iran to develop nuclear weapons, if it decided to do so.¹ The question has been central to the notion of a “cascading” nuclear threat, where the rapidity of states’ development of nuclear weapons is a critical factor underlying regional instability and the prospects of uncontrolled proliferation. In this context, these questions primarily appear in speculations about the timing required for possible Japanese or South Korean nuclear-weapon acquisition as a response to North Korean nuclear weapon and missile testing and brinkmanship. The impact of a non-state actor on the equation is less clear.

All of these issues involve nuclear latency. Technically, nuclear latency derives from the dual-use nature of the atom. One manifestation of strategic latency, it poses a threat that could result in strategic surprise. Nuclear latency can be viewed as the possession of most or all of the technologies, facilities, materials, expertise (including tacit knowledge), resources and other capabilities necessary for the development of nuclear weapons, without full operational weaponization. The issue also has to be seen historically: involving the full range of capability possessed by aspiring, existing, and former nuclear-weapon

¹ The views are the author’s alone, and not those of the Los Alamos National Laboratory, the National Nuclear Security Administration, or the Department of Energy.

states, and the possible diffusion of nuclear-weapon-relevant information via a number of outlets, including non-state nuclear supply networks, the internet, etc. While much of the discussion has focused on states that are manifestly latent, like Japan, South Korea, and other advanced industrial states, latency can be pursued and achieved covertly without the attention and potential consequences of an overt effort.

Iran has been a focal point of the latency debate. Even before the Joint Comprehensive Plan of Action (JCPOA), Iran was already a latent nuclear power and not even the removal of their entire nuclear infrastructure would eliminate this reality. However, the JCPOA limits or scales back important parts of Iran's program while recognizing and reinforcing this latency.² Latency will grow again as the specific measures of the JCPOA begin to expire. President Obama himself highlighted the potential difficulties that could arise from Iran's remaining nuclear capabilities in future years as the restrictions on stockpile size and centrifuges, as well as the enhanced monitoring and verification mechanisms, are phased out. He stated: "...a more relevant fear would be that in year 13, 14, 15, they have advanced centrifuges that enrich uranium fairly rapidly, and at that point breakout times would have shrunk almost down to zero."³ Senator Bob Menendez argued that if President Obama's statement "is true, then it seems to me that—in essence—this deal does nothing more than kick today's problem down the road for 10–15 years, and, at the same time, undermines the arguments and evidence we'll need, because of the dual-use nature of their program, to convince the Security Council and the international community to take action."⁴

As the Iran case highlights, latency is a reality for many non-nuclear-weapon states today, primarily as a result of spreading nuclear energy technologies and programs. Nuclear capabilities are now widespread and will increase with the growth of nuclear-power programs worldwide, especially those that involve direct-use nuclear materials such as plutonium and highly enriched uranium (HEU). Latency has already provided some level of

2 While Iran will be required to remove about two-thirds of its centrifuges from operation, including its more advanced IR-2 centrifuges, it is allowed about 5,000 IR-1 centrifuges to enrich uranium at Natanz, and 1,000 operational centrifuges at Fordow (which are not to be used to enrich uranium). Iran will not only be able to retain a substantial enrichment infrastructure, but it can also maintain an operational expertise in uranium enrichment. The agreement does not require Iran to destroy any IR-1 or IR-2 centrifuges. Iran is permitted to store centrifuges removed from operational status as a result of the JCPOA at the facility where they were previously operating. Iran would potentially be able to use these centrifuges after the 15-year period ends. Furthermore, Iran is permitted to engage in R&D on more advanced IR-6 and IR-8 centrifuges, but they cannot accumulate uranium on the basis of this R&D. The actual capabilities of these advanced centrifuges may not be as good as advertised. However, Iran may be able to further develop them by the time the restrictions established by the JCPOA expire. Iran's latent capabilities for plutonium production will be reduced significantly by the JCPOA. The core of the reactor will be removed and disabled, the reactor will be reconfigured from 40 to 20 MWt and use low-enriched uranium instead of natural uranium as fuel. These modifications in the design and operation of the reactor, if fully implemented, will reduce the amount of plutonium the reactor can produce and reduce its attractiveness. In the end, however, Iran's latency in this area would remain and it would retain the capability to produce plutonium at both Arak and Bushehr. In light of both the technical challenges and the difficulty of concealing its activities, it may decide to build another reactor, either overtly after 15 years or covertly, rather than utilize Arak or Bushehr.

3 "Transcript: President Obama's NPR Interview on Iran Nuclear Deal," *NPR*, April 7, 2015, last accessed October 27, 2017, <http://www.npr.org/2015/04/07/397933577/transcript-president-obamas-full-npr-interview-on-iran-nuclear-deal>.

4 Bob Menendez, "Menendez Delivers Remarks on Iran Nuclear Deal at Seton Hall University's School of Diplomacy and International Relations," Press Release, August 18, 2015, last accessed October 27, 2017, <https://www.menendez.senate.gov/news-and-events/press/menendez-delivers-remarks-on-iran-nuclear-deal-at-seton-hall-universitys-school-of-diplomacy-and-international-relations>.

virtual nuclear-weapon capabilities as a result of spreading nuclear energy technologies and programs. A continuum of latent capabilities exists, ranging from technology diffusion and the existence of nuclear energy programs to conscious decisions to develop or maintain militarily significant nuclear weapon capabilities. At one end of the continuum, in cases like Japan and South Korea, the latency is evidenced in their nuclear power programs and levels of technological and industrial development. Iran's latency had become clear as it mastered enrichment, and remains the case even after the JCPOA. At the other end, as noted, latency may also exist in states with clandestine programs, before a weaponization decision is taken, even in states with little technological prowess. In such cases, the latency may not be known and recognized as such. Latency in all these cases raises fundamental questions for nonproliferation and counter-proliferation, and especially for intelligence related to these missions.

Going nuclear is possible for states with little or no nuclear capabilities through an aggressive development program (with or without assistance from other states) as well as for latent states with advanced nuclear facilities, materials, and expertise that decide to "break out" and turn a virtual capability into an actual one. However, even though historical cases appear to be complex and influenced by unique developments, much of the discussion of the capabilities and time required for a nuclear weapon from development to delivery reflects a simplification of the issues.⁵ States or non-state actors either have or do not have nuclear weapons, it is asserted, and the resources/time required for those that desire but do not possess them is seen as a simple function of the resources and time required to produce nuclear weapon material.

In fact, states' weaponization, delivery and support capabilities are as critical as their efforts to acquire nuclear material. All of these activities provide an indicator of intent, albeit one with the low visibility and high ambiguity that present challenges for intelligence collection and analysis. The actual numbers and types of weapons being pursued and their means of delivery, along with the nuclear doctrine of a state, have not been adequately addressed and appear to have been seen as largely irrelevant to the equation.

In actuality, different states have different needs and capabilities, which lead to differing prospects, time frames, etc. There is no simple, canonical answer to the question of the capabilities and time required to obtain nuclear weapons. Any answer must recognize that states will be affected by the global and regional security environments, the nonproliferation regime and other factors. States will also be affected by the status of technology diffusion. While such factors are important, even more critical are state-specific considerations including motivation, levels of technical development, external assistance, technological choices (material production, design, weaponization, testing, etc.), requirements and roles for nuclear weapons, arsenal size and sophistication, and delivery systems of the

⁵ See, for example, Scott D. Sagan, "Nuclear Latency and Nuclear Proliferation," in *Forecasting Nuclear Proliferation in the 21st Century, Volume 1: The Role of Theory*, ed. William C. Potter with Gaukhar Mukhatzhanova (Palo Alto, CA: Stanford University Press, 2010).

proliferant. Any state or even a non-state actor pursuing nuclear weapons will face a series of challenges: financial, technical, political, diplomatic, and military. The analytical challenges are intensified by latency in all of its manifestations.

Going Nuclear: Latency and State-Specific Factors

Once a state or a non-state actor decides to develop nuclear weapons, the requirements are very different today than they were at the dawn of the nuclear age. This situation reflects the dramatically changed context in which such a decision would be taken, with obvious implications for the time it takes to acquire nuclear weapons. Seven decades ago, nuclear weapons were the exclusive preserve of the United States. The science and technology were not widely available. These capabilities were largely limited to a few advanced states, and nuclear material production was seen to be a key chokepoint. This situation was widely understood at the time to be real but short-lived; both the Baruch Plan and the Atoms for Peace proposal were grounded in a belief that the requisite knowledge and technological capabilities would spread inevitably and rapidly.

Today, science and technology diffusion via the Internet and other means has ensured global access to the knowledge of nuclear weapons. The rapid development of high-performance computing, additive manufacturing, and other enabling technologies could exacerbate the problem in the near future by reducing the technological challenges and costs, increasing the efficiency of the processes used, and making the entire project more difficult to detect.⁶ Any state that decided to develop nuclear weapons would have or could readily acquire the scientific and technological infrastructure necessary for that end. In part because of this diffusion, it is also the case that the requisite resources would likely be available due to decreasing costs of entry into the world of nuclear weapons. A state no longer needs to master all of the underlying technologies, with the demands on human and material resources that would require. Further, materials and the technologies required to manufacture them are now widely dispersed throughout the world and increasingly available via indigenous production, import and theft.

As latency has spread via technology diffusion, it has not been deeply affected by the international nuclear nonproliferation regime. Centered on the Treaty on the Nonproliferation of Nuclear Weapons (NPT) and the International Atomic Energy Agency (IAEA), the regime is based on the Atoms for Peace bargain, which offers assistance in the peaceful uses of nuclear energy in exchange for prohibitions on military applications of this inherently dual-use technology. Not only does the regime not prevent transfers of nuclear technology, but it is explicitly designed to encourage peaceful applications of nuclear energy. In practice, this NPT/IAEA mandate means that states can legally and legitimately acquire nuclear technologies/facilities that could be used for nuclear weapons. Perhaps

⁶ On the challenges of additive manufacturing for nonproliferation, see “3-D Printing the Bomb? The Nuclear Nonproliferation Challenge,” *The Washington Quarterly* 38, no. 3 (2015): 7–19.

more significantly, materials usable in nuclear weapons are not prohibited by the regime and can be stockpiled in significant quantities. These capabilities, as part of the NPT bargain, are controlled, but those controls are imperfect and can be terminated by the state under the provisions of the NPT.

Beyond the problems of controlling facilities and materials, knowledge and experience are wholly uncontrolled.⁷ These factors have been ignored in the nonproliferation calculus since the Acheson-Lilienthal report and the Baruch Plan. The Baruch Plan was the only proposal that encompassed, at least indirectly, international controls over nuclear weapon knowledge. It failed. One lesson of the Baruch Plan's failure is that knowledge and experience cannot be practicably addressed and effectively controlled under international safeguards or other mechanisms. Nuclear-related research could not be effectively controlled without undermining the principles of scientific freedom and national sovereignty.

Although latency has spread dramatically, it may not be decisive. Despite the global spread of nuclear technology, the worst fears about proliferation over the years have not been realized for a variety of reasons, the most important of which were the provision of nuclear security through Cold War treaties and national decisions to eschew these weapons because they were seen not to serve the security interests of states. The regime was also a factor in changing international perceptions of nuclear weapons and in reinforcing national non-nuclear decisions.

Although the global spread of technology has opened new possibilities for states, latent capacity is only one factor in a state's decision to go nuclear. State-specific factors are critical and can lead to a state with little capability to develop weapons while states with all the needed capabilities abstain. Key factors in nuclear decision making include:

Motivations

The historical motivations of a state to proliferate, largely independent of regime type, bear on the time required for developing nuclear weapons to the extent that they drive high-level political and military attention (prioritization), allocation of resources, and other elements of a weapon program. In principle, any motivation (e.g., security, status) could lead to a prioritized program and a maximum allocation of resources. But security is the most likely driver, particularly when a state faces what is or isn't perceived as a time-urgent threat. Even with high prioritization and resources, timing will be more dependent upon other factors. Although the technological level of a state remains important in this regard, it is less so than in the past, with the spread of decades-old nuclear technologies and the emergence of new nuclear and related enabling technologies from new enrichment methods to high-performance computing to additive manufacturing.

7 See Avner Cohen and Joseph F. Pilat, "Assessing Virtual Nuclear Arsenals," *Survival* 40, no. 1 (1998), 129–144.

In this context, the prospect of a state choosing an obsolescent or inefficient technology that it may expect to more easily master (and which may not be as well monitored as cutting-edge technologies), such as Iraq's exploitation of calutrons, can diminish the technological requirements for nuclear-weapon development. In any case, motivations can drive technology choices that do not minimize costs and time, but may reduce the risks of detection.

Level of Technological Development

The level of technological development of a state, particularly the scope and sophistication of any domestic nuclear program, has been a key factor determining the timing it requires to go nuclear. In all but the most advanced states, however, the actual time may be substantially reduced if the step of producing nuclear material is shortened or even made unnecessary due to theft or purchase. If this occurs, time would largely depend upon weaponization activities. This could take from months to a year or more, assuming serious work has not already been done.

Nuclear weapons are no longer a symbol of technological advancement. (This point is arguable; for some developing countries, including Islamic states, nuclear weapons could have huge domestic prestige value.) For most states, regardless of their level of development, some type of nuclear weapon program is theoretically possible. In the past, less developed states might have had to rely heavily on imports, foreign expertise, training, and assistance, because they were at the low end of the technological scale and hoped to succeed in a reasonable time frame. For these states, however, technology diffusion has made it easier and cheaper for them to proceed, with greater reliance on indigenous capabilities (perhaps with some external assistance). From the new technological starting point, using these means and assuming sufficient external assistance, these states may now even be able to pursue large, relatively sophisticated programs.

Accordingly, an advanced technical-industrial infrastructure—including nuclear-weapon-usable material production capabilities—is neither a necessary nor sufficient condition for nuclear weapon development. Despite the claims or suggestions of some, it is simply not a reliable indicator of motivation—a sure sign of the pursuit of nuclear weapons. Although technological prowess is a key factor, it is one that is changing as technology diffusion flattens the playing field to a degree. The capabilities of a state alone can no longer offer a reliably clear picture of the interest in and the time necessary for nuclear development.

External Assistance

One of the key factors in a state's ability to develop nuclear weapons or the material required for these weapons is its access to external assistance via imports or other forms of technological cooperation. Such access may be legal or illegal, and this aspect

of the equation has changed as international nuclear proliferation has developed.⁸ In either case, it can change dramatically the time requirements for nuclear weapons as, for example, access to imported enrichment components or other cooperation on enrichment technologies can reduce the time required to obtain weapon-usable material. Stolen or illegally obtained nuclear materials, along with the possible use of new (or old) technologies for material production have become even more important considerations in the proliferation time calculus.

Strategic Perspectives

Ultimately, political will and political-military calculations are critical to determining whether a state will decide on a nuclear-weapon program. Not only the motivation and the capability but also the strategies of a state are important. Considerations of strategy are important in assessing the roles of nuclear weapons and, consequently, such matters as the size and sophistication of a prospective nuclear arsenal. They have direct bearing on weaponization and testing requirements.

The questions raised by considering strategy are complex and difficult. Would a state need only crude weapons and delivery systems? Does yield maximization matter? What are safety, reliability, and other requirements? Would a state require a sophisticated arsenal with multiple delivery systems? For what purpose? As a political instrument? To ensure security? To provide the means to enable aggression? To augment the prestige of the regime and enhance its survivability? To deter a regional adversary or intervention by the United States or another state or states? To challenge the United States or another nuclear weapon state? All of these questions are considerations in defining what an individual state requires, and how long it may take, for it to be in a position to meet its requirements. They may provide a filter for determining a state's capacity to create a weapons program that meets its strategic needs.

In the case of Japan, for example, it is unlikely to develop an actual nuclear-weapon arsenal without also developing effective, dedicated delivery capabilities and command-and-control systems, and to have prepared for fully integrating these capabilities into the military. Given Japanese perceptions of vulnerabilities, deriving in part from its geostrategic position next to nuclear powers and proliferants, a nuclear capability might not emerge before effective active and passive defenses were deployed. Of course, some grave danger could, in principle, lead Japan to forego these steps. But it is difficult to imagine a threat that would force Tokyo to pursue nuclear weapons as rapidly as possible without considering its longer-term security requirements. Such a response could place Japan in even greater danger from Russia, China, or even North Korea. This is a possible rationale for latency, and pursuit of virtual weapons.

⁸ This evolution has not been taken fully into account in the literature. See, for example, Matthew Kroenig, *Exporting the Bomb: Technology Transfer and the Spread of Nuclear Weapons* (Ithaca: Cornell University Press, 2010).

Impact of the Nonproliferation Regime on Nuclear Latency

The impact of the nonproliferation regime has evolved, but is limited. The regime has changed the normative basis on which decisions to proliferate or to cooperate with proliferators are undertaken. It can also impose political constraints that may affect some if not all states, affecting resource and time requirements. Export controls and safeguards can make proliferation more difficult and costly and, it is presumed, delay the acquisition of nuclear weapons to some degree. However, nothing in the nuclear nonproliferation regime can prevent a state from acquiring nuclear weapons if it makes a decision to do so. Moreover, as noted above, the regime permits states to acquire nuclear technologies, facilities, and materials that could be used for nuclear weapons, thereby creating capabilities that affect the timeline for nuclear-weapon development.

Nuclear Weapons Development: From Decision to Delivery

Aside from human capability, including scientists, engineers and others, the basic technical requirements for building a deliverable weapon follow. In all cases, they are affected, but not determined, by latency.

Special Nuclear Materials Production

Although nuclear material production has never been the chokepoint envisaged in the 1950s, it has been and remains today the long pole in the tent of nuclear-weapon development.

The production of special nuclear material—plutonium (Pu) and HEU—continues to require specialized equipment, facilities, and expertise. Material production processes provide timelines for nuclear-weapon development that can be characterized to some degree. One can reasonably estimate construction/operation times for needed production of a quantity of Pu or HEU sufficient for a weapon—the IAEA's figures, labeled “significant quantities,” are 8kg of plutonium and 25kg of HEU—on the basis of the process being used. On this basis, if one assumes a parallel weaponization track, the estimated time for material production also provides an estimate of the time necessary to develop nuclear weapons.

In real-world cases, however, the amounts of material a state or a non-state actor would require, the technological starting point, and other factors would need to be factored into the equation. Some states with advanced nuclear power programs, especially if they entail a full fuel cycle, have the facilities in place for producing weapon-usable materials, or even large stockpiles of these materials essentially ready to go. On the other hand, the possibility of theft or purchase of illicit material from the former Soviet Union or other sources offers one scenario that would significantly alter any generic calculations and give any state or a non-state actor the possibility of rapidly acquiring the materials for nuclear weapons.

In a similar vein, the growing reality of cooperation among rogue states offers another path for obtaining weapon material or the capability to produce it without the technological, time, and other constraints of indigenous development. The weapons of mass destruction (WMD) and missile cooperation between North Korea, Pakistan, and Iran has been examined in the open literature. The question is whether that cooperation was limited to these or a few other states or provides a blueprint for the future. Clearly, there are a growing number of states that now possess or are developing WMD and missile-related technological capabilities and expertise. Will these capabilities be shared, and under what—if any—constraints? Will they wind up in black markets? In either case, they will erode export control efforts like the Nuclear Suppliers Group (NSG).

Finally, new technologies for enrichment and reprocessing, including pyro-processing, are being pursued. These technologies could offer advantages vis-à-vis detection. Moreover, other technologies, especially additive manufacturing, can decrease the required steps, the cost and the time needed for special material production and machining, although they do not get around the issue of obtaining the special material or other key materials (e.g., maraging steel).

The new technologies are not silver bullets, however, and may not be equally accessible to all states. In the same way, older technologies that might have been rejected in the past due to costs or inefficiencies could be used by states. Their attraction may be the greater prospect of mastering an old technology, or the belief that such technologies are not being monitored with the care afforded new technologies. After revelations of the Iraqi use of electromagnetic isotope separation, the latter rationale—that old technologies stand a better chance of evading detection—has some historical merit.

Plutonium

If a state is starting from the beginning, a plutonium path has long been regarded as requiring less time and technological sophistication than uranium enrichment to develop the material required for a weapon. Even though it was recognized that the design and production of a plutonium weapon would be more difficult than a gun-type weapon using HEU, this was viewed as secondary to the acquisition of the material. The idea that a non-state actor could pursue this path has largely been seen as not credible, if considered at all, both in terms of material production or fabricating a weapon.

In addition, although Pu production and reprocessing result in inherently higher radiation signatures than HEU production, a small production reactor and reprocessing facility (which may be only a large hot cell) are more easily hidden than a large reprocessing plant.

Reprocessing is a simple chemical process, and was fully declassified in the 1950s. The consideration of latency here must reflect that fact, even though a revival of interest in pyro-processing is occurring. While argued to be different from reprocessing, and “proliferation resistant” because the product is impure, pyro-processing creates weapon-useable material.

The U.S. government has officially stated that pyro-processing is reprocessing.⁹ Moreover, the process can be done in smaller facilities with less effluent releases than commercial reprocessing plants, making it more difficult to detect.

If a state has an operating declared reprocessing or pyro-processing plant, it has clear latent capacity and the possibility of going nuclear rises. However, even beyond the advantages of pyro-processing for reduced detection (and without sacrificing material quality), one or several large hot cells capable of producing one significant quantity (SQ, defined as the approximate amount of nuclear materials needed to produce a weapon) of Pu per year would likely never be detected, and the real latency of the state would not be known.

Highly Enriched Uranium

Gaseous diffusion plants are large, energy-intensive facilities that are readily detectable with national technical means of verification (NTM). Today, as reports of foreign assistance to the gas-centrifuge enrichment programs of Libya, Iran, and North Korea suggest, the spread of technology through lateral proliferation has altered the calculus. The possibility of proliferant states mastering this technology seemed unlikely until the last two decades, when the issue of external assistance came to the fore, and the option of gaseous diffusion enrichment was seen as difficult to conceal due to the large size and distinct, detectable signatures of the facility. However, gas-centrifuge enrichment facilities make it very difficult to detect HEU production due to the reduced size of the required facility and the low radiation signatures. This situation has altered the received wisdom of the most likely path to weapons for states. For a non-state actor, material production, especially HEU production using centrifuges, does not appear as a realistic option, although some argue that if the terrorists received sufficient HEU by purchase or theft they might be able to fabricate a simple gun-type device.

The spreading ability to produce HEU via gas centrifuge technology reduces but does not eliminate the differences between acquisition paths involving HEU and Pu on the basis of time and expertise required. For more advanced states, the differences between the paths are marginal. Even with foreign assistance, some states may confront challenges in pursuing this path to weapon material. Certainly, a non-state actor would face problems unless it was totally supported by the state on whose territory it could engage in such operations.

Today, the capability to enrich is a key element of latency. Any state with this capacity can develop weapon-useable and weapon-grade material. In the future, some enrichment technologies now being explored, including laser-based systems, could change the calculus entirely for states and even for non-state actors at the low end of the technological spectrum.

⁹ Daniel Horner, "Pyroprocessing is Reprocessing: U.S. Official," *Arms Control Today*, April 4, 2011, last accessed October 27, 2017, https://www.armscontrol.org/act/2011_04/Pyroprocessing.

Other Fissile Materials

Other fissile materials could be used in weapons, including U-233 and Neptunium. These materials are obtainable using the same processes that yield Pu and HEU, either enrichment or reprocessing. However, there may be additional technical difficulties in working with such materials. On the other hand, controls, accounting, and protection of these materials are far more limited than those related to irradiated and non-irradiated direct-use Pu and HEU.

Procurement of Specialized Equipment and Materials

Specialized, often dual-use equipment including precision milling, electronics, and diagnostic equipment have been necessary, as are neutron generators. For some of these equipment requirements, additive manufacturing may offer critical shortcuts and lower entry costs for an aspiring proliferant. In addition, nonnuclear materials such as energetic high explosives are required for all paths. Other needed materials include beryllium. For some advanced designs, deuterium and tritium may be required.

Weaponization

Weaponization comprises a series of nuclear-weapon development activities, from device design to component engineering to nonnuclear testing that together provide assurance that the nuclear explosive will perform as intended. These activities may be more or less taxing, depending on the type of weapon and the level of development of the state. States with highly developed munitions industries will have many of the needed capabilities in place. For a non-state actor, any weaponization would be crude, if it is possible at all. The challenges to states and even, to a lesser degree, non-state actors today no longer involve basic science but primarily engineering. These engineering challenges can be substantial and should not be dismissed, especially for non-state actors.

Although weaponization has its own time requirements, in most cases they will be shorter than material acquisition. New technologies like high-performance computing and additive manufacturing could be important in reducing the challenges of, and timelines for, weaponization. Moreover, they can in principle enhance efficiency and possibly reduce signatures. Cooperation with other states can reduce the time requirements, but it can be assumed that in most cases they will be undertaken in parallel with material acquisition and will not generally require additional time for the program.

Boosted and Thermonuclear Weapons

In addition to fission devices like the gun- and implosion-types used at the end of the Second World War, a state may also consider boosted or thermonuclear weapons. Boosted weapons use deuterium and tritium to increase the yield of fission devices. Thermonuclear weapons are devices in which a fission explosive (primary) is used to trigger

a thermonuclear or fusion reaction in thermonuclear fuel (secondary). These weapons have tremendous power compared to fission weapons.

Both boosted and thermonuclear capabilities pose greater technological and engineering challenges than fission weapons. As a consequence, they are likely to require more time to develop than fission weapons and most likely necessitate a testing campaign as well in order to be certain they will perform, and to perform to specification. Even with the diffusion of technology, only states at the higher end of the technological spectrum, with a robust latent capability, may be expected to be able to develop these weapons. For states at the low end of the technological spectrum, these weapons may not be a realistic option. For a non-state actor they are not credible at all.

Nuclear Testing

Nuclear testing was once the ultimate indicator of a nuclear-weapon capability, the line crossed by states to establish themselves as nuclear-weapon states. This is no longer the case, despite North Korea's repeated testing today. For states, nuclear testing may or may not be required for new nuclear weapons, depending upon the type of weapon chosen, the political and military role envisioned, the risks a state is willing to assume, and other factors. Nuclear testing is likely to be of no concern to non-state actors.

In cases where a single, relatively unsophisticated weapon is sought by a state and is envisaged as a means to intimidate adversaries, testing may not be required technically. States such as South Africa that developed gun-style fission weapons using HEU don't appear to have needed to test on technical grounds. However, South Africa was reportedly interested in preparing to test in the past, and possibly tested at one time.¹⁰ Testing may have been seen as useful politically to prove their capability, possibly for deterrence purposes. For more sophisticated weapons that are to be fully integrated into a modern military, testing is likely to be required. Political considerations may reinforce this need, or at least provide another rationale for testing. The Indian tests in 1974 and 1998 appear to have had political as well as technical drivers. In cases where testing is required technically, it will add to the time required to field the weapon—from months to years.

Weapon Production

If more than one or two crude nuclear weapons are required, there will be a need for a viable weapon production infrastructure. This might be extensive and costly with a large throughput or relatively small-scale operation, but it will require trained personnel, facilities, and equipment. The precise requirements depend on the size and sophistication of the arsenal, the availability of nuclear materials and weapon production lines, etc. The time

10 "The Vela Incident: South Atlantic Mystery Flash in September 1979 Raised Questions about Nuclear Test," *National Security Archive Electronic Briefing Book No 570*, last accessed October 27, 2017, <http://nsarchive.gwu.edu/nukevault/ebb570-The-22-September-1979-Vela-Satellite-Incident/>.

required for the establishment of the production infrastructure is a key consideration and will depend on a variety of factors, including domestic environmental and other factors. However, computer-aided design (CAD) programs with high-performance computing and additive manufacturing could reduce the technological challenges, costs, and time required, and increase the quality and efficiency of this effort.

Delivery Means

Delivery-system requirements determine the requirements for warheads, and are likely to influence size, sophistication, and other considerations. In turn, the time requirements for a nuclear weapon are affected by the means of delivery chosen. The requirements for a nuclear weapon that can be delivered unconventionally by non-state actors may be less than for one that can be delivered by a commercial airliner, other aircraft, or missile, unless the unconventional delivery requires miniaturization. Terrorists could in theory choose to bring components, high explosives, and expertise to a site physically near to a chosen target and assemble a weapon on site.

Assuming sufficient time and capability, this option would not have some engineering challenges associated with more conventional delivery requirements. On the other hand, the sophistication and presumably the time required for weapons that are delivered by aircraft or missiles increases. For the latter, testing becomes a significant issue and may be needed because if there are military requirements such as reduced size and maximized yield, this may raise questions about whether a weapon will work, achieve desired yields, and be properly delivered to its target. For ballistic missile development, some level of testing will be needed. However, this activity could be hidden in a space-launch program.

Addressing the Intelligence Collection and Analysis Problems

On the basis of the considerations outlined above, the real issues surrounding what it takes and how long it takes to go nuclear are state specific. Recognizing this reality, is there a way to enhance intelligence collection and analysis? In this context, it may be useful to look at several types of states and the indicators of weapon programs that not only point to intent but to the time requirements. With latency at the core, three types of states may be usefully identified.

For states with limited latency, and no or minimal nuclear energy activities, indicators include any activity related to nuclear energy beyond the medical and industrial use of isotopes, and any weaponization efforts such as high-explosive testing. For states at the low end of the technological spectrum, acquisition of weapons may require more than a decade. Moreover, the program may be in full or in part clandestine and difficult to observe. Both the time frame and the signatures of the program could be significantly affected by foreign assistance and imports.

For states with a significant but not high level of nuclear latency, key indicators include efforts to develop:

- large research reactors;
- sensitive fuel cycle capabilities, including enrichment and reprocessing;
- weaponization activities; and
- delivery capabilities (air, missiles, etc.).

In addition to such “objective” factors, subjective factors may also come into play. For example, any nuclear capabilities that are not consistent with a state’s extant capabilities or realistic projections of where it may go in the civilian nuclear energy sphere may be a sign of weapon aspirations. For these states, a range of about five years is feasible. Again, imports and other cooperation could be significant.

For wealthy industrial countries that possess high levels of nuclear latency, such as South Korea or Japan, indicators of a move to nuclear weapons (virtual or actual) may include:

- deliberate decisions to establish short lead-time capabilities to develop and produce nuclear weapons;
- possession or development of associated military capabilities to make weapons a strategic threat or to conduct military exercises; and
- development or deployment of active and passive defenses (for strategically vulnerable countries).

These states, with a robust nuclear fuel cycle and a strong industrial base, have some level of virtual capability, which relatively rapidly could be turned to weapons if a national decision is taken. If such a state needed only a small number of crude weapons, one could imagine manufacturing them in less than a year for the most advanced states. A larger arsenal of sophisticated nuclear weapons, mated to delivery systems, well-tested, and well-integrated into defenses would take considerably longer.

In this third category, indicators may be very different for states like South Africa that once possessed nuclear weapons and may have proven designs, mothballed production capabilities, and stored components and materials. For a country like Japan, however, starting afresh on the basis of advanced technologies may have some advantages over less-developed countries’ efforts to preserve old designs and systems. In this case, the advantage would be due to such factors as the difficulties associated with exactly replicating old designs, maintaining stocks of old components that may no longer be otherwise available, and preserving an accessible human knowledge base.

In addition to these three categories of states, non-state actors must be considered. No terrorist organization has yet shown any meaningful latency, especially the capability to

produce material or to develop and produce weapons, but the possibility of purchase or theft cannot be discounted.

What are the tools available?

The production of nuclear weapon materials, especially through misuse of or diversion from civil nuclear activities, is the focus of the nuclear nonproliferation regime's safeguards and export controls. There have been challenges to the regime, which is attempting to address difficult problems such as a state's ability to obtain enrichment and reprocessing capabilities or quantities of spent fuel (containing plutonium) and then leaving the treaty, noncompliance, clandestine facilities, the increasing role of non-state actors, and collaboration among proliferants.

The problem in dealing with specialized equipment and materials beyond Pu and HEU is that only small quantities may be required, with limited and ambiguous acquisition signatures. National Technical Means (NTM) are important. The International Atomic Energy Agency's Additional Protocol (AP), specifically information requirements and complementary accesses, may be useful. (Note that the prospect of successfully using complementary access here and in later references within this text is limited at best.) Sustaining support for the Nuclear Supplier's Group (NSG) dual-use trigger list is critical.

To address weaponization issues, the following tools are available: NTM; IAEA safeguards, especially if there is a connection to nuclear materials; visits to suspect sites under IAEA AP complementary accesses; and the NSG dual-use trigger list.

On testing, NTMs are the first line of defense, but the International Monitoring System being developed by the Comprehensive Test Ban Treaty (CTBT) Organization has increasing capability. Visits to suspected test sites would be possible if the CTBT enters into force—an unlikely prospect.

Latency complicates the intelligence challenges, and requires strategic thinking in the policy and intelligence communities on the following questions:

- What are the highest technological threats we can envision, and which are over the horizon?
- How do they track against the capabilities, motivations, strategies, and tradecraft of known and anticipated adversaries, including non-state actors?
- How do we see the development of the threat over time?
- What is the impact of disruptive technologies on collection?

Conclusion

The contemporary situation is quite different from that envisaged in the late 1940s, but concerns about widespread, continued proliferation by states remain. Since the 9/11

attacks, the concern about non-state actors obtaining or even fabricating nuclear weapons has risen.

Any state or non-state actor pursuing nuclear weapons will face a series of challenges—financial, technical, political, diplomatic, and military—that are decreasing to some degree by technology diffusion. Some of these challenges may affect the timing and success of a nuclear program. Some of these challenges may be met with little difficulty by states. For example, the financial costs of a weapon program may be significant but can probably be met by many states with sufficient incentives to develop nuclear weapons. Latency, reflecting the global level of technology diffusion and a state's access to that technology at a given time, affects the challenges and can greatly reduce the time needed for getting the bomb, as well as reduce or remove financial and technical constraints.

Moreover, latency can be an end in itself. Latency alone does not determine outcomes, however, as states and possibly non-state actors can pursue alternative means to their objective. For example, a state that is not advanced technologically or a non-state actor may obtain the capabilities it needs via technical cooperation with the IAEA or key states, imports, or theft. Increasingly, such states are also able to benefit by technology diffusion as well as to obtain a level of latency covertly through state support and non-state supply networks. Accordingly, the time required for going nuclear is specific to the state or non-state actor considering this move, but overall could be reduced by a capable proliferator exploiting access to available technologies. Abstract calculations are not particularly useful and can be undermined wholly by, for example, latency, foreign cooperation, or nuclear theft. Such circumventions are most likely in the case of states at the lower end of the technological development spectrum, and possibly also non-state actors.

Chapter 9

Backseat Driving: What Happens When Technology Outpaces Strategy?

Leo J. Blanken and Jason J. Lepore¹

Introduction

“The invention of invention.” Military historian Martin van Creveld coined this term to label one of the most important turning points in military (and human) history. He argues that at some time during the 19th century, nations began to include issues surrounding technological innovation as part of their grand strategy. In other words, technological progress stopped being an exogenous shock that sprang unplanned from inventors “as [a] gift of the gods,” but rather became “sustained...deliberate, and therefore, up to a point, predictable.”²

The implications of this evolution are profound. It would suggest that national security strategies should not only include doctrine and force planning, but deeper choices about investment in engineering and basic scientific research. Strategic studies have largely neglected these deeper issues of “technology strategy,” instead relegating these questions to more compartmentalized analyses of procurement and maintenance of the industrial base.³ The current technological environment—characterized by rapid change and widely diffused sources of innovation—requires new analyses that endogenize the emerging

1 This chapter results from research supported by the Naval Postgraduate School under Grant No. N00244-16-1-0054 awarded by the NAVSUP Fleet Logistics Center San Diego (NAVSUP FLC San Diego). The views expressed here do not necessarily reflect the official policies of the Naval Postgraduate School nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

2 Martin van Creveld, *Technology and War: From 2000 BC to the Present, Revised Ed.* (New York: Free Press, 1991), 218.

3 A notable exception is Audra J. Wolfe, *Competing with Soviets: Science, Technology, and the State in the Cold War* (Baltimore: Johns Hopkins University Press, 2012).

technology milieu into strategic planning. We seek to provide such a conceptual framework here—one that will be suited for analyses of strategic latency, as well as the types of policy choices that might be derived in light of it.

To set the stage, we must first look at the evolution of intellectual thinking about technology, policy, and war. It was 19th-century naval competition that drove the genesis of the “invention of invention.” The revolution of sail to steam propulsion, wood to steel hulls, and smooth bore, muzzle-loading to rifled, breach-loading guns radically altered the manner in which major powers interacted with emerging technologies to secure themselves. For the first time in history, nation-states needed to consider developing mature strategies for balancing technological innovation, private industry, and national security.⁴ Given that competition among states in this era began to include long-term technological competition—in peace as well as in war—20th-century analysts began to look closely at such competition. Scholarly works such as Brodie’s *Sea Power in the Machine Age*⁵ and Marder’s *Anatomy of British Sea Power*⁶ examined the wider technological aspects of Victorian naval competition, and thereby set the stage for future analysts to begin to examine the interplay of engineering, policy, and warfighting in the modern era.

The Cold War provided a new era of rapid technological change and fierce inter-state rivalry to motivate further intellectual work on such relationships. A seminal work on this topic remains Samuel Huntington’s *The Common Defense*.⁷ By tackling the process of “strategic programs” in national defense, he set the stage for our understanding of the interrelated nature of inter-state competition, domestic politics, and bureaucratic dynamics within the context of the early Cold War.⁸

A rich literature has built up in the wake of Huntington’s work that has developed a number of more focused topics. One group of researchers has focused on explaining a military’s likelihood of accepting and integrating emerging technologies into their force structure and doctrine. Works such as Posen’s *The Sources of Military Doctrine*, Rosen’s *Winning the Next War*, Kier’s *Imagining War*, Johnson’s *Fast Tanks and Heavy Bombers*, Winton and Mets’ (eds.) *Challenge of Change*, Pierce’s *Warfighting and Disruptive Technologies*, and Mahnken’s *Technology and the American Way of War* examine civil–military, inter-service, intra-service, and organizational culture dynamics to explain when and how militaries will

4 On the Mercantilist intellectual foundations of this line of thinking, see Edward Meade Earle, Adam Smith, Alexander Hamilton, Friedrich List, “The Economic Foundations of Military Power,” in *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, ed. P. Paret (Princeton: Princeton University Press, 1986).

5 Bernard Brodie, *Sea Power in the Machine Age* (Princeton: Princeton University Press, 1941).

6 Arthur Marder, *Anatomy of British Sea Power: A History of British Naval Policy in the Pre-Dreadnought Era, 1880–1905* (London: Frank Cass, 1940).

7 Samuel P. Huntington, *The Common Defense: Strategic Programs in National Politics* (New York: Columbia University Press, 1961).

8 For an intellectual biography of Vannevar Bush, who singularly shaped the trajectory of the relationship between the US military and applied research, see G. Pascal Zachary, *Endless Frontier: Vannevar Bush, Engineer of the American Century* (Cambridge: MIT Press, 1999).

embrace or reject new technologies.^{9,10,11,12,13,14,15} These works are crucial for understanding how uniformed advocates (or opponents) may shape technological change to fit with organizational preferences or doctrinal vision.

Further, works such as Kotz's *Wild Blue Yonder*, Rundquist and Carsey's *Congress and Defense Spending*, Ruttan's *Is War Necessary for Economic Growth?*, and Thorpe's *American Warfare State* seek to unpack the relationship among defense spending, domestic politics, and the private sector.^{16,17,18,19} In these studies, issues such as profit motive, the industrial base, and the lobbying of lawmakers rise to forefront of military technology investment; such works are important as they widen the aperture of understanding the range of actors who influence the R&D and investment choices that are made for strategic technologies. Taken as a whole, these works essentially ask the question: "How will we exploit new technologies?"

In another vein, the question of diffusion of emerging technology between and among states arises. Krause's *Arms and the State* provides a broad empirical survey of technology diffusion through arms production and transfers in the modern era.²⁰ Goldman and Eliason's (eds.) *Diffusion of Military Technology and Ideas* compiles a number of studies that examine the spread of military technology, driven by the 1990s debate on the "Revolution in Military Affairs."²¹ Horowitz's *Diffusion of Military Power* puts forward the argument that the cost per unit of a technological innovation, as well as the degree of organization change required to implement it, will determine the rate of innovation

9 Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca: Cornell University Press, 1986).

10 Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca: Cornell University Press, 1994).

11 Elizabeth Kier, *Imagining War: French and British Military Doctrine Between the Wars* (Princeton: Princeton University Press, 1999).

12 David E. Johnson, *Fast Tanks and Heavy Bombers: Innovation in the US Army, 1917–1945* (Ithaca: Cornell University Press, 1998).

13 *The Challenge of Change: Military Institutions and New Realities, 1918–1941*, ed. Harold R. Winton and David R. Mets (Lincoln: University of Nebraska Press, 2000).

14 Terry C. Pierce, *Warfighting and Disruptive Technologies: Disguising Innovation* (London: Frank Cass, 2004).

15 Thomas G. Mahnken, *Technology and the American Way of War Since 1945* (New York: Columbia University Press, 2008).

16 Nick Kotz, *Wild Blue Yonder: Money, Politics, and the B-1 Bomber* (New York: Pantheon, 1988).

17 Barry S. Rundquist and Thomas M. Carsey, *Congress and Defense Spending: The Distributive Politics of Military Procurement* (Norman: University of Oklahoma Press, 2002).

18 Vernon W. Ruttan, *Is War Necessary for Economic Growth? Military Procurement and Technology Development* (New York: Oxford University Press, 2006).

19 Rebecca U. Thorpe, *The American Warfare State: The Domestic Politics of Military Spending* (Chicago: University of Chicago Press, 2014).

20 Keith Krause, *Arms and the State: Patterns of Military Production and Trade* (New York: Cambridge University Press, 1992).

21 *The Diffusion of Military Technology and Ideas*, ed. Emily O. Goldman and Leslie C. Eliason (Stanford: Stanford University Press, 2003).

diffusion.²² These works largely focus on the system-level dynamics of technology diffusion among states, but pay much less attention to a conception of strategy that would endogenize both technology development and implementation on the one hand, and the likelihood of subsequent diffusion on the other. These works serve as a nice complement to the previous literature in that they essentially ask the question: “How will other states—including our rivals—exploit new technologies?”

Finally, we consider the concept of strategic latency. Gershwin and Gac provide the following definition: “[It] refers to the inherent potential for technologies to bring about significant shifts in the military or economic balance of power. Such potential may remain unexploited or even unrecognized, and thus latent, until a combination of factors coalesce to produce a powerful capability...Note that the ultimate result is a shift in power.”²³ Embedded within this simple definition is a powerful notion: the degree to which there are technologies with poorly understood impact on the strategic landscape presents a serious challenge to planners and analysts. In other words, the already difficult job of turning societal resources into a viable national security apparatus will be significantly compounded if technologies driving the future strategic landscape are occurring outside the awareness of planners.^{24,25} This concept, then, drives the question: “How will novel, private-sector innovations drive strategic technology?”

Given this set of questions, what remains to be explicitly modeled is what an optimal strategy of technology diffusion might look like—simultaneously asking what we might gain from new private-sector technology and considering the likelihood of its diffusion to others. This is becoming an increasingly pressing question in light of the high rates of innovation currently being experienced.²⁶ Blanken and Lepore provide a basic model of this question by developing a formal argument of military technology competition among nations.²⁷ This base model assumes unitary state actors that can choose to introduce any level of military technology that is within their capacity, mimic their rivals’ level of technology, or withdraw from the contest.

22 Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton: Princeton University Press, 2010).

23 Lawrence K. Gershwin and Frank D. Gac, “Foreword,” in *Strategic Latency and World Power: How Technology is Changing Our Concepts of Security*, ed. Z. Davis, R. Lehman, and M. Nacht (Livermore, CA: Center for Global Security Research, 2014), v.

24 On the already difficult task of planning, see Paul K. Davis, “Planning Under Uncertainty Then and Now: Paradigms Lost and Paradigms Emerging,” in *New Challenges for Defense Planning: Rethinking How Much Is Enough*, ed. P. Davis (Santa Monica: RAND, 1994).

25 Also see Richard K. Betts, *Military Readiness: Concepts, Choices, and Consequences* (Washington, D.C.: Brookings, 1995).

26 Matthew Kroenig and Tristan Volpe, “3D Printing the Bomb? The Nuclear Nonproliferation Challenge,” *Washington Quarterly* 38, no. 3 (2015): 7–19.

27 Leo J. Blanken and Jason J. Lepore, “Slowing Down to Keep the Lead in Military Technology,” *Defence and Peace Economics* 22, no. 3 (2011): 317–334.

This work specifies the conditions under which states should push the limits of technology or, conversely, withhold cutting-edge technologies—releasing them only on a disciplined schedule to trump rivals' efforts. The logic of this strategic-technology implementation schedule is to force trailing rivals to pay maximum, unrecoverable costs in research, development, and implementation. This framework, then, provides the basis for modeling the implications of strategic latency in competition between state-controlled industries, but must be modified to reflect the growing impact of private-sector innovation on national security. We will do so below.

The chapter proceeds as follows: first, we explain the base model of technology diffusion and competition among states. This model is highly constrained by assumptions that map to the traditional relationship between state power and strategic technology—one of intimacy. Next, we modify this base model to approximate the emerging private-sector technology innovation environment. In this model, the relationship between the state and locus of technological innovation is problematized. The state may not be able to control, or even understand, technological innovations with strategic repercussions. The results of our analysis are counterintuitive and, in some ways, unwelcome. Given some basic assumptions regarding market dynamics and the uncertainty inherent to strategic latency, we show that being the home of leading private-sector innovation may, in fact, carry large and underappreciated costs.

Base Model: State-centric Innovation

In this section, we present a streamlined two-period example of the dynamic game introduced in Blanken and Lepore.²⁸ The version of the model we present highlights features of technology withholding by the technological leader. This action exploits the trade-off in resources between innovation and imitation a rival nation-state must make. Technology withholding is only present in equilibrium for the case in which the two nation states have asymmetric initial technological capacities. Thus, we only consider this case for the current treatment.

Consider a two-period game with player one and player two making choices regarding investment in military technological capacity (capacity) and the level of technology to implement (level). In the interest of parsimony, we consider a game of complete information in which all players know everything.

The players one and two begin with capacities x_1 and x_2 , respectively. We assume that $x_1 \geq x_2$. The timing of the game goes as follows: given the initial capacities, each state begins the game by simultaneously and independently deciding on the level of technology to implement s_1 and s_2 . The level of technology must be below capacity, formally $s_i \leq x_i$. Based on these levels each state gets an expected payoff from international interactions

²⁸ Ibid.

(this payoff includes both peacetime bargaining and wartime capabilities): $\pi_1(s_1, s_2)$ and $\pi_2(s_2, s_1)$.²⁹ In the second period of the game, the states decide on capacity investments for the future. The states must decide between innovating or imitating the other state. Innovation gives state 1 the capacity next period of $y_1 = \alpha x_1$ and similarly $y_2 = \alpha x_2$, where $\alpha > 1$.

On the other hand, imitation gives state 1: $y_1 = s_2$ and state 2: $y_2 = s_1$. The payoff of the future (period 2) is determined by the capacity of each state. The second period level decisions are omitted since it will be optimal for both states to implement the highest level possible.³⁰ We denote the future payoff of each state by $\Pi_1(y_1, y_2)$ and $\Pi_2(y_2, y_1)$. Each state has a discount factor $\delta, 0 < \delta \leq 1$, that determines the relative value of the utility in the present to the future utility. Thus, the payoff of an arbitrary state i given a fixed set of choices s_1, s_2, y_1 , and y_2 is

$$\pi_i(s_1, s_2) + \delta \Pi_i(y_1, y_2).$$

We assume that π_i is increasing in s_i and decreasing in s_j . Similarly, Π_i is increasing in y_i and decreasing in y_j .

Now we can analyze the equilibrium of this game by way of backward induction. Let us begin with the choice of capacity in the second period. The equilibrium of this subgame is very straightforward; each state will pick the methods that increase capacity the most. That is, state i will pick according to the following rule:

$$\begin{aligned} \text{Innovate if} & \quad \alpha x_i > s_j, \\ \text{Imitate if} & \quad \alpha x_i < s_j. \end{aligned}$$

If $\alpha x_i = s_j$, then the state is indifferent between innovating and imitating. Notice that state 1 will never find it optimal to imitate in period 2, since $\alpha x_1 \geq \alpha x_2 > s_2$.

In period 1, each state decides on the level of technology to implement. For state 2, this decision is very easy; since there is no potential downside from implementing the highest level of technology, because state 1 will never find it optimal to imitate, state 2 will always be best off picking $s_2 = x_2$. The nature of the equilibrium of the game depends on the following decision problem for state 1.

Imitation is only possible for that case that $x_1 > \alpha x_2$. That is, state 1 has a sufficiently large lead in technology. There are two distinct cases to consider:

29 See Blanken and Lepore, "Slowing Down to Keep the Lead in Military Technology." The expected payoff includes both war and peacetime payoffs. For this example, we abstract away from these details and just assume that the function π_i has the important properties that follow from the more detailed construction.

30 The implementation of the maximum technology level is optimal because the end of the game eliminates future concerns of diffusion.

No Imitation:

State 1's best choice is $s_1=x_1$ since payoff is $\pi_1(s_1, x_2) + \delta\Pi_1(ax_1, ax_2)$, which is increasing in s_1 . The maximum payoff of state 1 conditional of state 2 innovating is

$$V_1^{NP}(x_1, x_2) = \pi_1(x_1, x_2) + \delta\Pi_1(ax_1, ax_2).$$

Imitation:

State 1's expected payoff is $\pi_1(s_1, x_2) + \delta\Pi_1(ax_1, s_1)$ where we know that π_1 is increasing in s_1 and Π_1 is decreasing in s_1 (since it is state 2's capacity in period 2). So, state 1 picks its level to maximize its payoff given that its rival imitates. Formally,

$$V_1^P(x_1, x_2) = \max_{s_1 \leq ax_2} \{ \pi_1(s_1, x_2) + \delta\Pi_1(ax_1, s_1) \}$$

Consequently, state 1 is always withholding technology in equilibrium if $V_1^P(x_1, x_2) > V_1^{NP}(x_1, x_2)$ and never withholding if $V_1^P(x^1, x^2) < V_1^{NP}(x_1, x_2)$.

The following comparative static is shown in Blanken and Lepore.³¹ An increase in the technological rate of innovation weakly increases the level of gap between the implemented technology and the technological capacity of the leading state. Therefore, in times of rapid technological progress, withholding cutting-edge technology is more important. This has implications for the current environment, as the rate of technological innovation is generally viewed as extremely rapid.

Strategic Latency Modeled: Private Innovation and State Competition

In this section we examine the case that private actors are generating innovation that is potentially valuable for military states as well as the private market. This setting introduces a non-standard "zero-sum" type competition for the technology between states. In a standard market, actors (firms, states, etc.) compete for an input that gives them a particular expected value if they attain the item and no value if they do not attain it. Consequently, an actor is never incentivized to buy an item for more than its expected value. In contrast, competition between rival states for technology has the added feature that a rival attaining the technology is worse than the status quo. This is because the rival's increased military strength confers increased bargaining power, while the home country's strength has stayed the same.

A consequence of this zero-sum feature is that states compete much harder for technology, resulting in welfare lower than the status quo for both states. This outcome occurs because the state that does not obtain the item has lower welfare due to loss in relative power, while the state that attains the technology gains welfare from the change in relative power, as

31 Blanken and Lepore, "Slowing Down to Keep the Lead in Military Technology."

the price paid to get the technology far outweighs the value the technology provides. We detail an intentionally simplified model of this type of competition with two rival states and a private market for technology in what follows.

Innovation Choice

Consider a single agent who must decide how much of their time, effort and resources to invest in innovation.³² The level of innovation for the agent is described by a , a non-negative real number. The individual has preferences represented by the payoff function:

$$\theta m(a) - c(a)$$

where $m(a)$ is the market value of innovation a . The function m_i is endogenous to the equilibrium of the model and, accordingly, will be specified later. Assume the cost function is of the explicit form $c(x) = a^2/2$.

The optimal choices of the innovator are defined by the first order condition (assuming that m_i is differentiable):³³

$$\frac{\partial m(a^*)}{\partial x} = a^*$$

Next we consider the behavior of the states as buyers in the technology market.

Market for Technology

Consider 3 buyers for the new technology: the private market, the home state military 1, and the rival state military 2. The innovation has a private value va , while the military value is dependent on the relative value to the states. We assume that v is a uniform random variable on the outcomes $[0,4]$. This will be sufficiently varied to make some cases in which innovation is more valuable to industry and other cases such that innovation is more valuable for some military purpose. The value of the innovation for the military purpose is uncertain. Particularly, we assume that the expected value of the invention will only be valuable for a military purpose with probability μ , where $0 < \mu < 1$.

Returning to the model of section 1, we write the expected value of this innovation if obtained by an arbitrary state i is

$$E[\Gamma_i(f(a, x_i), x_j)] = \mu V_i(f(a, x_i), x_j) + (1 - \mu) V_i(x_i, x_j).$$

³² We focus on the case of a single innovator for this treatment, but the results extend to the case of any number of innovators with no significant complementarities in production of technology and for the case technologies have independent values to the states.

³³ Obviously, assuming this very simple form of expected payoff is not without loss of generality. This assumption illuminates certain intricacies that would be of interest in a more extensive treatment, but works to clarify the main point of this treatment.

Note that the expected value depends on the technological capacities of the two states and the nature of the interaction of the technologies determined by f . For example, if the private and government technologies are perfect substitutes then $f(a, x_i) = \max\{a, x_i\}$. We will abstract away from the specification of a particular f at this point, but discuss the implications of input relationships later. For the simplicity required in this brief treatment, we just assume that the expected value of attaining the technology for each state i is:

$$(1) \quad E[\Gamma_i (f(a, x_i), x_j)] = \omega_i + a.$$

Thus, if this were part of a government-owned innovation program, then each state would be willing to pay a (its expected value) for the technology. Since the private market generates this technology, the states must compete for the technology and this drastically changes their willingness-to-pay. The reason for this change is the possibility that the rival state attains the technology instead. The expected value from the other state obtaining the innovation is

$$E[\Gamma_i (x_i, f(a, x_j))] = \mu V_i (x_i, f(a, x_j)) + (1-\mu) V_i (x_i, x_j).$$

Again we make the simplifying assumption:

$$(2) \quad E[\Gamma_i (x_i, f(a, x_j))] = \omega_i - a.$$

We consider technology competition to occur in a highest-bidder-gets-the-prize contest. This is modeled via a second price-sealed bid auction. The home and rival country both have optimal bid functions:

$$b_i(x) = \begin{cases} a, & 2 < v \\ 2a, & 2 \geq v \end{cases}$$

The innovation market value is the second-highest valuation of the three players, which is always:

$$m(a) = 2a$$

Note this function is differentiable as claimed in the previous section.

Open Market Equilibrium

Based on the optimal bid functions we can see that price is always $2a$ if either military acquires the good. Immediately this gives the conclusion that the states are paying excessively for technology. Every good purchased by a state involves investment $a^* = 2$ in all goods. In the expectation one half the time the good is bought by the private market and the other half the time by a country for a military purpose. Expected military benefit minus cost for either state i is:

$$\omega_i - 1.$$

Note that this expectation is calculated based on the fact that the private industry will in expectation acquire the technology fifty percent of the time.

Notice that the status quo of there being no private-market innovation would be better for both countries. In other words, each state ends up paying more than the value of the innovation above the status quo because of the force of inter-state competition. Overall the investment in technology is excessively large based on this deleterious competition. The expected innovation investment is 2. This outcome could be good if there is a very large social value to these innovations not being accounted for by the private valuation. Otherwise, this equilibrium involves inducing a huge amount of innovation and paying an extreme price for it just to keep it away from the rival.

Information and Home Preference in Equilibrium

Now suppose that the innovator has a preference toward the home country given that they understand the danger of selling their item to the rival country. This preference could be induced by an information campaign or governmental engagement effort in the home country.³⁴ We formalize this by altering the agent's preferences such that their payoff function is $M(a)$:

$$M(a)a - a^2/2$$

where $M(a)=p$ if either the private market or home country purchases the innovation at price p , while $M(a)=\beta p$ where $0 < \beta < 1$ if the rival country buys the technology at price p . The parameter β reflects an innovator's preference towards selling potentially dangerous technology to the home country over the rival.

We can now analyze the equilibrium expected outcome of this market. The equilibrium pricing is not as simple as the previous section. Consider the two cases:

$$\textit{Case 1: } 1/2 < \beta < 1$$

With probability $1-\beta/2$ the private-market values the good higher than the rival country and gets the good, while with probability $\beta/2$ we have one of the two following outcomes. The home state attains the good only if $2\beta \geq v$ occurs. The price in this case is $2\beta a$. The innovation level is $a^* = 2\beta$. The expected welfare of the home state is:

$$\omega_1 + \beta(\beta - 2\beta^2).$$

Notice this is less than the status quo of ω_1 for all $1/2 < \beta < 1$.

$$\textit{Case 2: } 0 < \beta < 1/2$$

³⁴ See Snow chapter, this volume.

With probability 3/4 the private market values the good higher than the rival country and gets the good. That is, because only if $v \leq I$ will the home country purchase the technology. Conditional on $v \leq I$, there are two subcases.

First, consider the subcase that $2\beta < v$. The home country will prefer to buy the technology at price va . The remaining one quarter of the goods are sold to the home country at the effort $a^* = v$ and at the price v^2 .

Second, consider the subcase that $2\beta \geq v$ occurs. The price in this case is $2\beta a$. The innovation level is $a^* = 2\beta$. The equilibrium expected payoff to the home country from the technology is

$$\Gamma_1 = \omega_1 + \left(\frac{1}{4}\right)(2\beta(2\beta - 4\beta^2) + (1 - 2\beta)(E[v | 2\beta \leq v \leq I] - E[v^2 | 2\beta \leq v \leq I]))$$

$$\omega_1 + \left(\frac{1}{4}\right)\left(2\beta(2\beta - 4\beta^2) + (1 - 2\beta)\left(\left(\frac{1}{6}\right) + \left(\frac{\beta}{3}\right) - \left(\frac{4\beta^2}{3}\right)\right)\right)$$

For this second case, the information policy leads to welfare greater than the status quo. Note that this payoff is strictly decreasing in β . That is, the greater the preference for the home country, the greater the welfare of the home country. Outlawing Rival Sales

Outlawing Rival Sales

The nature of competition is very different if the rival is unable to buy from the market. This eliminates the foreign country from bidding for the technology and the maximum bid function of the home country becomes

$$b_i(x) = \begin{cases} a, & I < v \\ va, & I \geq v \end{cases}$$

Consequently, in expectation, three quarters of the time the good is sold to private industry and innovation effort is $a^* = I$. The remaining one quarter of the time the good is sold to the military home country at the effort $a^* = v$ and at the price v^2 . Thus, the expected payoff to the home country from the technology is

$$\omega_1 + (1/4)(E[v | v \leq I] - E[v^2 | v \leq I]).$$

Since v is a uniform random variable, $E[v | v \leq I] = I/2$ and $E[v^2 | v \leq I] = I/3$ and we have

$$\omega_1 + \frac{I}{24}$$

Notice this is exactly the limiting case of the previous section as $\beta \rightarrow 0$.

The Impact of Technological Uncertainty

Up to this point, the latent aspect of technology, that is the degree to which its impact on the military balance of power is uncertain, has remained silent in the analysis. This is primarily based on the functional form simplification we made in equations (1) and (2). This specification introduces a very simple symmetry that is not realistic if one state has a technological lead. Consider for example another specification where the new technology is a perfect substitute for current capacity. That is only the maximum of initial capacity and the realization of the private latent technology is the functional capacity. That is, $f(a, x_i) = \max\{a, x_i\}$. Further, suppose that $x_1 > 2/\mu$. In this case the private technology can never increase the technology of the home state (since $a^* \leq 2$ will always hold). The expected payoff of state 1 attaining the technology is

$$(3) \quad E[\Gamma_1(f(a, x_1), x_2)] = \omega_1 \text{ and } E[\Gamma_2(x_2, f(a, x_1))] = \omega_2 .$$

In addition, let us assume that $x_1 < I/\mu$, which (we will show) is a capacity sufficiently small that the investment in the private technology will increase the technological capacity of state 2. Based on this assumption, we write

$$(4) \quad E[\Gamma_1(x_1, f(a, x_2))] = \omega_1 - a \text{ and } E[\Gamma_2(f(a, x_2), x_1)] = \omega_2 + a .$$

More explicitly, the expected payoff of state 1 can be written

$$\begin{aligned} E[\Gamma_1(x_1, f(a, x_2))] &= \mu V_1(x_1, \frac{a}{u}) + (1-\mu) V_1(x_1, x_2) \\ &= \mu(\omega_1 - \frac{a}{u}) + (1-\mu)\omega_1 \end{aligned}$$

It is only with probability μ that the technology has value for state 2. In this case, state 1 does not benefit from the private technology at all, but is willing to pay to keep the technology away from the rival state. Contingent on $v < I$, the optimal choice of investment is $a^* = I$. The equilibrium bids of both states are 1. The equilibrium expected payoff of the home state is

$$\omega_1 - I/4.$$

The rival state has the expected payoff ω_2 . The equilibrium is a situation in which state 1 purchases useless technology just to avoid the small chance this technology is of value to the rival state. Clearly, this is a problematic scenario for the home state in which the state is wasting resources just to play “keep away.” Technological Spillovers

Technological Spillovers

Another issue that our model does not address is the impact of technological spillover if the private market acquires the technology. This scenario puts the home state (as the

technological leader) in an even more precarious position. Consider the case of complete diffusion to both states in the case that a private firm acquires the technology. We continue to assume the payoffs are of the form specified in (3) and (4). Adding diffusion from private purchase only makes matters worse for the home state and better for the rival state. This is because the diffusion is beneficial to the rival state (increasing their capacity with probability μ) and provides no benefit to the home state (since $x_1 > a/\mu$). The equilibrium expected payoff of the home state is

$$\omega_1 - 1,$$

while the expected payoff of the rival state is

$$\omega_2 + 3/4.$$

The payoff is greater than the status quo based on the fact that with probability 3/4, the rival state is getting the technology through diffusion without paying any cost, which has an expected value of 1.

Conclusion

On February 19, 2014, Facebook acquired the WhatsApp messaging application for \$19.3 billion, despite the fact that the previous year WhatsApp had only earned \$20 million...why? Many concluded, “to stop anyone else [from] buying it.”^{35,36} In other words, unsure how the start-up might affect the future global communications market, Facebook paid an enormous cost to forestall the possibility that the technology might prove crucial in a rival’s hands. Is this the future for international security competition? Our model suggests that, in the face of growing strategic latency, this may be a concern.

In fact, an overriding theme of the analysis in this chapter is that the existence of an open private market with technology that has potential value for military usage is inherently detrimental to the home state if it is the technological leader. This market introduces the possibility that a rival state buys technology from the home state’s private market that (with some probability) has military value. In equilibrium, the home state pays a heavy price to essentially keep the technology away from the rival state, in spite of the fact that the home state’s acquisition of the technology could offer no technological benefit beyond the current technological capacity. This is a recipe for wasteful military spending.

These results are sobering. Most commentators assume explicitly or implicitly that a) the United States is the hub of emerging technology innovation and that b) this is a major boon

35 Gordon Kelly, “5 Key Reasons WhatsApp is Worth \$19 Billion—to Facebook,” *Forbes*, February 20, 2009, <https://www.forbes.com/sites/gordonkelly/2014/02/20/5-key-reasons-whatsapp-is-worth-19bn-to-facebook/#13e48b9960d9>

36 Dennis K. Berman, “I Thought Facebook’s WhatsApp Deal Was Crazy. Then I Did Some Math,” *Wall Street Journal*, February 24, 2014.

for U.S. national security. Utilizing reasonable assumptions, we show that serious negative implications can, in fact, result from this state of affairs.

We consider a few abstract policy options that can improve this situation for the home state. First, we consider the case that the home state innovators have a preference for selling to the home military, if they understand the potential value of the technology to the rival state. An effort to inform technology innovators of the potential military value of the technology can mitigate the destructive competition for the home state to some degree. Second, we consider that a policy of prohibition of the rival state purchasing technology with potential military use, if feasible, changes the nature of competition, allowing the home state to benefit from the existence of the private market of latent technology; this path is problematized, however, by the degree to which the impact of technologies is uncertain.¹ Neither of these policy recommendations is easy or entirely attractive. They may, however, form the basis of better-informed lines of effort as the strategic latency landscape continues to evolve.

Finally, in the present analysis we have omitted the value of the technology on the development of new technology. That is, we have not included the possible complementarities of production between various technological developments. It is worth noting that the conclusions of the present model are unlikely to be altered unless the complementarities across technology are sufficiently large. Including this factor would require a much more extensive modeling effort that is inappropriate for this venue and we leave to future research.

¹ If the impact of the innovation were known, then the control of the technology would simply fall within existing export control efforts. For an overview of this broad topic, see Bert Chapman, *Export Controls: A Contemporary History* (Lanham, MD: University Press of America, 2015).

Chapter 10

Terrorist Tech: How Will Emerging Technologies Be Used by Terrorists to Achieve Strategic Effects?

Zachary Davis and Michael Nacht

Terrorist use of weapons of mass destruction (WMD) ranks high among the threats driving public perceptions of danger to the U.S. homeland. What if a group like ISIS were to acquire nuclear, chemical, or biological weapons and use them against the U.S. or its allies? Al Qaida's apparent interest in WMD² and reports of chemical weapons use in Syria³ lend credence to the idea that terrorists could acquire and use strategic assets such as nuclear, chemical, or biological weapons. However, the debate over whether the risk of WMD-T (as it is called in Defense Department terminology) is urgent, nascent, or over-hyped rages on. Explaining why a major attack has not occurred is a major research question. What is more certain is that terrorists are finding new ways to use technology to pursue their violent objectives.

We maintain that a suite of emerging technologies is poised to complement classic WMD as threats to U.S. and international security. Known as Forward Generational Technologies, Radical Leveling Technologies,⁴ emerging and disruptive technologies, or by our term Strategic Latency, the confluence of unprecedented scientific progress and accelerating access to technology through global markets is making it easier for states and groups to acquire powerful technical capabilities. With such availability we note a propensity for innovation among terrorist groups, whether it is rapid adaptation of new technologies like

2 Rolf Mowatt-Larson, "Al Qaeda's Religious Justification of Nuclear Terrorism," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, November 12, 2010, last accessed October 27, 2017, <https://www.belfercenter.org/publication/al-qaedas-religious-justification-nuclear-terrorism>.

3 Jeffrey Lewis, "Syria Is a Chemical Weapons Free-for-All," *Foreign Policy*, November 30, 2015, accessed October 27, 2017, <http://foreignpolicy.com/2015/11/30/syria-is-a-chemical-weapons-free-for-all-happy-holidays/>.

4 Jennifer Snow, *Entering the Matrix: The Challenge of Regulating Radical Leveling Technologies*, NPS Thesis, 2016, last accessed October 27, 2017, <http://calhoun.nps.edu/handle/10945/47874>.

drones, or new applications for old ones, as with Improvised Explosive Devices (IEDs). The question is whether these new technical possibilities represent game changers or fall into the same category as the known WMD threats: nascent but unproven dangers?

Our analysis covers the following four research questions:

- Are terrorists interested in newly emerging technologies?
- What could they do with them?
- How much does it matter?
- What can and should be done about it?

This chapter represents an initial assessment of the intentions and technical capabilities needed for violent extremist organizations (VEOs) to exploit the potential of emerging and disruptive technologies to achieve strategic effects. Such effects may include economic or societal harm, but only if damages are sufficient to cause a significant shift in the balance of power.⁵ By this definition, costly temporary disruptions would not qualify. We then review the implications for national and international security and conclude with some ideas about possible policy options.

Are Terrorists Interested in Advanced Technology?

Terrorist interest in WMD is well established.⁶ We believe sufficient evidence exists to confirm that terrorists are also interested in a variety of emerging technologies. Scholars have documented efforts by ISIS, Al Qaeda, and others to adapt a wide range of technologies to achieve their objectives, including innovative uses of well-known tools such as cell phones, aircraft, and explosives.⁷ Recent innovations include concerted efforts to use cyber operations, mass media, social networking, advanced communications, and creative financing to achieve their goals.

What might inspire terror groups to innovate with technology? If necessity is the mother of invention, desperation also motivates creative ways to maximize available resources. In this regard, terrorists are no different than anyone else looking for asymmetric advantage. As ISIS lost territory in Iraq and Syria it has escalated or inspired civilian attacks on soft targets around the world.⁸ The more terror groups go on the defensive, the more likely they may be to employ technology to maintain visibility, recruitment, funding, and operational

5 Our definition of strategic effect is derived from Ariel Levite, *Intelligence and Strategic Surprise* (New York: Columbia Press, 1987). See also *Strategic Latency and Warning: Private Sector Perspectives on Current Intelligence Changes in Science and Technology* (Livermore: Lawrence Livermore National Laboratory, January 8, 2016).

6 Mowatt-Larson, "Al Qaeda's Religious Justification of Nuclear Terrorism," 2010.

7 For example, Gary Ackerman, "Designing Danger: Complex Engineering by Violent Non-State Actors," *Journal of Strategic Security* 9, no. 1 (2016), last accessed October 27, 2017, <http://scholarcommons.usf.edu/jss/vol9/iss1/>.

8 Peter Bergen, *The United States of Jihad: Investigating America's Homegrown Terrorists* (New York: Crown Publishers, 2016).

effectiveness.⁹ Competition among groups for attention as the world's leading jihadist organization could, for example, lead Al Qaeda to employ technology to demonstrate its superior prowess over other contenders like ISIS.

Research on the psychological motivations of terror groups and individuals provides insight into what drives them to extreme violence, but it is not clear that these same factors also explain the possible allure of mass-effect weapons like WMD and other large-scale asymmetric means.¹⁰ Clearly Al Qaeda sought the drama associated with mass effects, but subsequent attacks have not seen the use of WMD as many expected.¹¹ It is one thing to adapt easily available technological means such as the internet or drones to improve operational effectiveness and quite another to pursue sophisticated and hard-to-come-by materials with which to make and use nuclear, chemical, or biological weapons. Of course, if such weapons were to become available to terrorists, as they did with the loss of government control over chemical weapons in Syria, terrorists may be more inclined to accept the risks and costs associated with WMD.

The risks include the proximate dangers from handling, storing, transporting, and using such weapons as well as the risks of being caught with them. However, it is debatable whether legacy WMD that are lost or stolen from a state arsenal necessarily qualify as advanced technology. In such a case innovation might be directed toward improvised delivery mechanisms for old weapons or materials.

What Technologies Could Be Applied to Make Mass Effect Weapons?

Technology companies, do it yourself (DIY) enthusiasts and governments are not alone in searching for the next product that puts them ahead of their competitors. Several new technologies possess latent potential for terrorists to weaponize, even if they are not seeking mass destruction effects and merely want to improve their operational effectiveness. A list of candidate emerging S&T prospects attractive to non-state actors could include the following:

The Devil's Workshop: Additive and Advanced Manufacturing. In addition to making do-it-yourself (DIY) guns and explosives that are hard to detect, terror groups may be drawn to the revolutionary design potential made possible by 3D printing. Like legitimate businesses, the ability to design and produce weapons, tools, replacement parts, and other items without depending on outside suppliers will appeal to terrorists. We are skeptical, however, about

9 Andrew Watkins, "Losing Territory and Lashing Out: The Islamic State and International Terror," *CTC Sentinel*, March 17, 2016, last accessed October 27, 2017, <https://ctc.usma.edu/posts/losing-territory-and-lashing-out-the-islamic-state-and-international-terror/>

10 "Special Report: The Psychology of Terrorism," *Scientific American* March 25, 2016, last accessed October 27, 2017, <https://www.scientificamerican.com/article/special-report-the-psychology-of-terrorism/>.

11 Rolf Mowatt-Larssen, "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, January 2010, last accessed October 27, 2017, <http://belfercenter.ksg.harvard.edu/files/al-qaeda-wmd-threat.pdf>.

the potential for 3D printing to provide terrorists with shortcuts to making true WMD, for which they must still possess weapons-grade materials.

Not Your Mother’s Easy-Bake Oven: Flow-Process Microreactors. Already in wide use in numerous industries, microreactors enable “just in time” synthesis and production of complex chemicals and pharmaceutical compounds. Instead of buying, storing, managing, and mixing large quantities of toxic and controlled substances, companies can make precise quantities of needed chemicals in situ using these small, disposable production units. The concern is that this technology could provide terrorists with a shortcut to produce modest quantities of controlled chemical or biological agents. Modest quantities are probably sufficient for an effective terrorist attack, but the advantage of this technology over other, well-known methods of making chemical or biological weapons is unclear. Beyond the shock value of any chemical or biological attack, we do not see this technology as a game changer.

Latency Unleashed: Cyberwarfare and Social Media. Terrorist groups and their supporters were early adopters of cyber capabilities. The appeal is obvious: low cost, remote operation, relative security, and the potential for high impact, making cyber tactics a natural tool for terrorists. The internet has many advantages for terrorist networks. Potential applications can be divided into three groups: (1) use of social media for propaganda and recruiting; (2) use of the internet for communications, planning, and financing; and (3) cyberattacks via malware, denial of service or other means to disrupt, hack, or even destroy systems and infrastructure. Of course, the U.S. and others already possess large-scale cyber organizations, so it should come as no surprise that others would seek similar capabilities, especially in light of the extensive vulnerabilities made evident by the cascade of successful attacks on U.S. persons and institutions.¹²

What’s next? The Internet of Things (IoT) will present a rich menu of potential target opportunities to disrupt civil society, from transportation (automobiles, airplanes, drones) medical records and devices, and industrial controls (dams, refineries, electric grids). So far it appears that terrorist cyberattacks have been limited to social media hacks and defacing web sites and have not succeeded in using destructive malware to cause major physical damage.^{13,14} Increasing sophistication, however, suggests it is only a matter of time before terrorist groups acquire these capabilities. Whether they can actually achieve truly strategic effects is debatable.

Arguably the most readily available applications of new technology for terrorists exist in the realm of communications. The latent applications of the internet and social media platforms

12 Cybercom Commander Admiral Rogers, unclassified testimony before the Senate Select Committee on Intelligence, April 2016.

13 Eduard Kovacs, “Cyber terrorist Attacks Unsophisticated but Effective: Former FBI Agent,” *Security Week*, March 14, 2016, last accessed October 27, 2017, <http://www.securityweek.com/cyberterrorist-attacks-unsophisticated-effective-former-fbi-agent>.

14 Joseph Marks, “ISIL aims to launch cyber attacks on U.S.,” *Politico*, December 29, 2015, last accessed October 27, 2017, <http://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179>.

have been vigorously exploited by a wide range of terror groups, including ISIS, Lashkar-e-Taiba (LeT), and Al Qaeda.¹⁵ While the use of websites and social media for recruitment has been an obvious and apparently successful endeavor, other applications include propaganda/misinformation, communications for operational plans, and real-time command and control over operations, as demonstrated in the 2008 Mumbai attacks in which LeT terrorist teams reportedly planned the operation using Google Earth and maintained contact with their headquarters, the media, and with one another throughout the event.^{16,17} Al Qaeda and ISIS have used encrypted, secure messaging¹⁸ and steganography to embed secret messages in public transmissions of information.^{19,20} Several terror groups have developed their own apps to facilitate outreach, training, and operations.²¹ These support functions, however, would not qualify by themselves as having strategic consequences.

If it is true that the Mumbai terrorists received assistance and operational guidance from Pakistan's Inter-Services Intelligence Directorate, such state sponsorship of terrorist operations raises questions about the provision of advanced cyber tools to terrorists. Would Iran provide cyber tools to Hezbollah and other Shiite groups? Who might North Korea arm? The issue of cyber mercenaries also becomes increasingly relevant in light of Russian and Chinese hacker intrusions into U.S. public and private institutions.^{22,23} In contrast to advanced conventional weapons and WMD, cyberterrorists can possess and use the most advanced tools available to anyone.

Necessity is the mother
of invention.

—Unknown

15 Nico Prucha and Ali Fisher, "Tweeting for the Caliphate: Twitter as the New Frontier for Jihadist Propaganda," *CTC Sentinel*, June 25, 2013, last accessed October 27, 2017, <https://ctc.usma.edu/posts/tweeting-for-the-caliphate-twitter-as-the-new-frontier-for-jihadist-propaganda>.

16 RAND Occasional Paper, *The Lessons of Mumbai*, 2009, last accessed October 27, 2017, http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP249.pdf.

17 James Glanz, Sebastian Rotella and David Sanger, "In 2008 Mumbai Attacks, Piles of Spy Data but an Uncompleted Puzzle," *New York Times*, Dec 21, 2014, last accessed October 27, 2017, http://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html?_r=0.

18 Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel*, June 16, 2016, accessed October 27, 2017, <https://ctc.usma.edu/posts/how-terrorists-use-encryption>.

19 Sean Gallagher, "Steganography: How al Qaeda Hid Secret Documents in a Porn Video," *Ars Technica*, May 2, 2012, last accessed October 27, 2017, <http://arstechnica.com/business/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/>.

20 Bogdanoski, Risteski, and Bogdanoski, "Steganography in Support of Global Terrorism," in *Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses*, ed. Mehmet Nesip Ogun (Amsterdam: IOS Press, in cooperation with NATO Emerging Security Challenges Division, 2015).

21 Rita Katz, SITE Intelligence Group, "ISIS's Mobile App Developers are in Crisis Mode," *Motherboard*, June 6, 2016, last accessed October 27, 2017, <http://motherboard.vice.com/read/isis-mobile-app-developers-are-in-crisis-mode>.

22 Susan Hennessey, "What Does the U.S. Government Know About Russia and the DNC Hack," *Lawfare*, July 25, 2016, last accessed October 27, 2017, <https://www.lawfareblog.com/what-does-us-government-know-about-russia-and-dnc-hack>.

23 Danny Yadron, "Report Warns of Chinese Hacking," *The Wall Street Journal*, Oct. 19, 2015, last accessed October 27, 2017, <https://www.wsj.com/articles/report-warns-of-chinese-hacking-1445227440>.

In terms of recruitment, American-born jihadi Anwar al Awlaki's online messages continue to lure new recruits even after his death in a drone strike in 2011.²⁴ The online version of Al Qaeda's magazine *Inspire* offers ideological and operational guidance to those seeking the means or the justification for violence against infidels and the perceived enemies of the caliphate.²⁵ Not to be outdone, ISIS has its own slick online magazine, *Dabiq*, which also provides spiritual and operational succor to its followers.²⁶ Beyond their appeal to potential jihadis, these mediums and others like them provide intellectual ammunition to state and non-state critics of U.S. and allied foreign policies. By influencing public discourse, terrorists can assert a louder voice and claim to have more political status than may actually be the case. Cyberwarfare is a great leveler of capabilities, an asymmetric weapon that empowers the weak and strong alike

Open Skies: Discovering Latent Potential for Drones. The watershed latency event for drone warfare occurred when U.S. officials armed the Predator drone with Hellfire missiles.²⁷ It was only a matter of time before others would also explore their latent potential. ISIS is using drones on the battlefield to provide intelligence, surveillance, and reconnaissance (ISR) for its military operations as well as conducting crude attacks.²⁸ Insurgents have reportedly hacked U.S. and Israeli drones,^{29,30} and drug smugglers are pioneering the use of air and seaborne drones to deliver illicit goods.³¹ U.S. officials have voiced concerns about drone attacks on nuclear facilities, although the actual threat to civilian or military nuclear installations is unclear.³² The use of drones to deliver commercial and military payloads is maturing before our eyes.³³ Not limited to the air, autonomous vehicles are becoming ubiquitous on land and at sea, raising endless possibilities for constructive and malevolent

24 Scott Shane, "The Enduring Influence of Anwar al Awlaki in the Age of the Islamic State," *CTC Sentinel*, July 27, 2016, last accessed October 27, 2017, <https://ctc.usma.edu/posts/the-enduring-influence-of-anwar-al-awlaki-in-the-age-of-the-islamic-state>.

25 The Spring 2016 issue of *Inspire* contains instructions on assassination techniques and bomb making in addition to interviews and spiritual exhortations from famous jihadi terrorists. All 15 issues of *Inspire* can be found at: <https://www.adl.org/search?keys=inspire+magazine>

26 Issues of *Dabiq* available at <http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq>, last accessed October 27, 2017.

27 Richard Whittle, "Hellfire Meets Predator," *Air and Space*, March 2015, last accessed October 27, 2017, <http://www.airspacemag.com/flight-today/hellfire-meets-predator-180953940/?no-ist>.

28 Matthew L. Schehl, "ISIS is expanding the reach and sophistication of its drone fleet," *Marine Times*, April 17, 2016, last accessed October 27, 2017, <http://www.marinecorpstimes.com/story/military/tech/2016/04/17/islamic-state-drones-target-american-coalition-forces/83096864/>.

29 Aliya Sternstein, "How to Hack a Military Drone," *Defense One*, April 29, 2015, last accessed October 27, 2017, <http://www.defenseone.com/technology/2015/04/how-hack-military-drone/111391/>.

30 David Axe, "How Islamic Jihad Hacked Israel's Drones," *Daily Beast*, March 24, 2016, last accessed October 27, 2017, <http://www.thedailybeast.com/articles/2016/03/25/how-islamic-jihad-hacked-israel-s-drones.html>.

31 "Mexican Cartel Strategic Note No. 18: Narcodrones on the Border and Beyond," *Small Wars Journal*, March 28, 2016.

32 Joe Gould, "Defense Bill Has Nuclear Facilities Fighting Drones," *Defense News*, May 7, 2016, last accessed October 27, 2027, <https://www.defensenews.com/congress/2016/05/07/defense-bill-has-nuclear-facilities-fighting-drones/>.

33 James Bamford, "What America Hath Wrought," *Foreign Policy*, May 2016.

innovation. The maritime domain appears particularly rich with latent potential for mischief. The big question for terrorists is: Can they use drones to deliver chemical, biological, or radiological payloads? Relatedly, can drones carry enough WMD material to have truly strategic effects? If not, their effects may be limited and not cross the strategic threshold as we have defined it. While autonomous vehicles represent a major development in state warfare, it is not clear at this point that terror groups possess the command and control systems required to use drone swarms as strategic weapons.

Reach for the High Frontier: Terrorists in Space? While it may seem unlikely that terrorists could launch their own space vehicles or commandeer someone else's satellites, terrorists could someday reach for the high frontier. Satellite imagery and geospatial information has reportedly been used in major terrorist attacks, including the Mumbai attack in 2008, as stated previously.³⁴ If not via their own spacecraft, cyber hacking might enable terrorists to steal data and wreak havoc in the already contested space environment—especially if aided by a capable state sponsor.³⁵ Even if terrorists cannot match Saddam Hussein's supergun that came close to being able to launch crude satellites into orbit,³⁶ they may try to disrupt a major power's dependence on space assets by causing malfunctions, possibly via cyber hacking. Out-of-control satellites could result in collisions that produce space debris that threatens everything in its orbital path. The trend toward privatization and democratization of space raises questions about terrorists buying their own satellites, especially as miniature satellites and launch services become cheap and more readily available.³⁷

Past as Prologue: Why So Few Chemical and Biological Attacks? Despite consistent interest in chemical and biological weapons by various groups over many years, terrorists have yet to launch a full-fledged mass-casualty chemical or biological attack against the West. The doomsday cult Aum Shinrikyo's sarin and anthrax attacks in Japan stand out as the most deliberate and carefully executed WMD plots, followed by the anthrax letters sent to the U.S. Senate and media outlets in 2001.^{38,39} As stated earlier, use of Syria's legacy chemical weapons and materials by various factions in Syria and Iraq represents a distinct category of use characterized by opportunistic acquisition of existing assets. As devastating as those events were for those who have endured them, it is debatable whether they have had truly strategic consequences. The use of those weapons outside the conflict zone would, however, represent a new and troubling development. Effective terrorist use of lost or

34 Anthony L. Kimery, "Mumbai Terrorist's Use of Google Earth Reignites Concerns," *Homeland Security Today*, December 5, 2008, last accessed October 27, 2017, <http://www.hstoday.us/columns/the-kimery-report/blog/mumbai-terrorists-use-of-google-earth-reignites-concerns/642770639e0a4ae59d34a79be3a628fa.html>.

35 Micah Zenko, *Dangerous Space Incidents*, Contingency Planning Memorandum No. 21, Council on Foreign Relations, April 2014.

36 William Park, "The Tragic Tale of Saddam Hussein's Supergun," BBC, March 16, 2016, last accessed October 27, 2017, <http://www.bbc.com/future/story/20160317-the-man-who-tried-to-make-a-super-gun-for-saddam-hussein>.

37 Don Reisinger, "SpaceX Alums Eye Easier Way to Get Mini Satellites Into Orbit," *PC Magazine*, April 27, 2016.

38 Andrea Nehorayoff, Benjamin Ash, David Smith, "Aum Shinrikyo's Nuclear and Chemical Weapons Development Efforts," *Journal of Strategic Security* 9, no. 1 (2016).

39 United States Department of Justice, *Amerithrax Investigative Summary*, February 19, 2010.

stolen nuclear weapons might, however, satisfy our definition of strategic effects, depending on the circumstances.

Researchers have scoured the literature to understand the low incidence of chemical or biological terrorism, especially in light of avowed interest in them and dire warnings of their use.⁴⁰ The congressionally mandated Report of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, titled *World At Risk*, concluded in 2008 that: "...unless the world community acts decisively and with great urgency, it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013. The Commission further believes that terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon."⁴¹ As Wes Spain points out in his chapter in this volume, years of warnings by experts have not lived up to the hype.⁴²

Adding to the debate over why this is so, the ability of hobbyists or do-it-yourself (DIY) biologists to master gene-splicing techniques via the CRISPR method adds new fuel to the fire.⁴³ As the technological barriers continue to drop, does it become more likely that terrorists will make and use biological weapons?⁴⁴ If the motivation exists, is capability a major obstacle? Even if they do acquire and use some type of biological agent, what are the chances that the effects will be truly strategic in nature? Years of speculation about terrorist use of biological weapons raise at least as many questions as answers.

A Distinction with a Difference: Radiological Devices vs Atomic Bombs

Using our definition of strategic effect, spreading radioactive materials in an urban area would not *necessarily* qualify as a weapon of mass destruction, and might not meet the standard of strategic consequence. We do not discount the serious nature of this type of threat and fully endorse efforts to prevent it from happening. In particular, the Obama Administration's four Nuclear Summits focused world attention on the need to secure nuclear materials precisely for this reason. Nor do we downplay the apparent intent of terror

40 For example, the National Consortium for the Study of Terrorism and Responses to Terrorism has compiled extensive research on the motives and capabilities of terrorist groups and individuals to conduct WMD attacks. See their website at <http://www.start.umd.edu>.

41 *World At Risk: Report of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism*, 2008.

42 Wes Spain, "Dogs That Didn't Bark," Chapter 3.

43 Laurie Garrett, "CRISPR: Transformative and Troubling," *Council on Foreign Relations*, April 13, 2016.

44 For a skeptical view see Filippa Lentzos, Catherine Jefferson, Claire Marris, "The myths and realities of synthetic bioweapons," *Bulletin of the Atomic Scientists*, September 2014, last accessed October 27, 2017, <https://thebulletin.org/myths-and-realities-synthetic-bioweapons7626>. For a different perspective see Marc Goodman and Andrew Hessel, "DNA hacking is the biggest opportunity since cyber attacks," *Wired*, May 28, 2013, last accessed October 27, <http://www.wired.co.uk/article/the-bio-crime-prophecy>.

groups to acquire nuclear materials. ISIS was reportedly scoping Belgian nuclear facilities and workers in pursuit of nuclear materials.⁴⁵

Nevertheless, even if terrorists were able to disperse radioactive materials in a city, more casualties would likely result from the explosives used to spread the materials than from radiation, especially if the population took steps to avoid exposure. Without producing nuclear yield, the main effects of a radiological dispersion device (RDD), or dirty bomb, would be public fears about health safety. True, the resulting property and economic damage could be substantial and highly disruptive, but not necessarily strategic in nature. Emergency preparedness and consequence management would be critical, especially communications to affected populations.^{46,47} By contrast, a true nuclear explosive device has the potential to cripple a nation and alter the course of history.

Money Makes the World Go 'Round: New Technology for Terrorist Finance

Our final category addresses revolutionary changes in global economic activity that may offer terrorists new opportunities. Spurred by necessity to be early adapters, terrorist organizations, like legitimate and criminal enterprises, can be expected to find new ways to protect and grow their assets. ISIS's seizure of Iraq's oil fields is an example of terrorists appropriating a nation's strategic assets to fund their operations.⁴⁸ To the extent that oil revenue made possible the growth of ISIS, the effects were strategic. Beyond stealing resources, what other disruptive business models might spill over from the business world to aid terrorists? A recent study highlights how drug cartels mimic the business practices of legitimate global corporations.⁴⁹ Creative financing has long been a hallmark of terrorist finance, largely due to the need to evade law enforcement. Relatedly, terrorist collaboration with criminal cartels is a well-documented phenomenon, and it comes as no surprise they are both well represented among dark web networks.⁵⁰ Hawalas, charities, front companies, money laundering, corruption, and secret bank accounts are standard tools of the trade.

45 Alissa Rubin and Milan Schreuer, "Belgium Fears Nuclear Plants Are Vulnerable," *New York Times*, March 25, 2016, last accessed October 27, 2017, <https://www.nytimes.com/2016/03/26/world/europe/belgium-fears-nuclear-plants-are-vulnerable.html>.

46 *Dirty Bombs: Radiological Dispersal Device Medical Preparedness and Response. Guidance for First Responders and Health Care Workers*, U.S. Government, Department of Homeland Security.

47 Congressional Research Service, *Dirty Bombs: Technical Background, Attack Prevention and Response, Issues for Congress*, by Jonathan Medalia, June 24, 2011.

48 "Inside ISIS Inc: The journey of a barrel of oil," *Financial Times*, updated Feb. 29, 2016, last accessed October 27, 2017, <http://ig.ft.com/sites/2015/isis-oil/>.

49 Tom Wainwright, *Narconomics: How To Run a Drug Cartel* (Public Affairs, 2016).

50 Daniel Moore and Thomas Rid, "Cryptopolitik and the Darknet," *Survival* 58, no.1 (2016).

What innovations in business finance should we expect terrorist to adopt? Crypto or virtual currencies offer certain advantages to those seeing to evade detection.^{51,52} Bitcoin has reportedly been used to facilitate donations from wealthy benefactors who do not want to be held accountable.⁵³ Virtual currency and secure money transfers using block-chain technology could be useful for evading sanctions as well as the transparency associated with major banks. Whether such innovations greatly increase the effectiveness of terror groups or simply make them harder to track will determine the strategic salience of new business models.

Does It Matter?

Even if terrorists are able to exploit these and other emerging technologies, the question remains: does technology make terrorists deadlier? And if they are deadly enough to achieve strategic effects, and demonstrate intent to use innovative technological capabilities against the United States and its allies, what should be done?

We see two potential capabilities in a class by themselves. Possession of a nuclear explosive device capable of producing nuclear yield crosses a threshold that warrants special attention, both in terms of strategic warning and operations to counter the threat. The two most likely pathways for VEOs to acquire nuclear weapons are to buy or steal weapons from a nuclear weapon state or buy or steal nuclear materials—highly enriched uranium or plutonium—from a state-owned stockpile. This situation and the technology involved, however, is not new. Current national and international non- and counter-proliferation mechanisms present formidable obstacles to these types of threat scenarios.

Second, we reserve judgment about the latent potential for VEOs to weaponize emerging biological science. While state actors are apparently moving closer to entering a new era of strategic latency in the biological sciences, as illustrated by James Giordano's chapter about China's neurobiology sector, it is not yet clear that individuals and non-state actors have the capacity to use such innovations in a strategically significant manner. Moreover, we are mindful of Wes Spain's warning about threats that never materialize. For now we are persuaded by Jen Snow's advice about engaging hacker, maker, and DIY biology communities to gain insight into the intentions and capabilities that would enable terrorist bio threats.

51 Joshua Baron et al., *National Security Implications of Virtual Currency: Examining the Potential for Non-state Actor Deployment* (Santa Monica, CA: RAND Corporation, 2015), last accessed October 27, 2017, http://www.rand.org/pubs/research_reports/RR1231.html. Also available in print form.

52 Alan Brill and Connie Keene, "Cryptocurrencies: The Next Generation of Terrorist Finance," *Defense Against Terrorism Review* 6, no. 1 (Spring & Fall 2014).

53 Yaya Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," *The Cipher Brief*, August 24, 2016, last accessed October 27, 2017, https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin.

How then do we assess the threat of terrorists using technological innovations to advance their agendas? In our view, innovation is most likely to occur using existing, easily available, and adaptable technologies, such as drones, albeit in new ways. Some research suggests that terrorists prefer cheap, simple, and known technologies over expensive, complicated, and novel technologies.⁵⁴ Brian Jenkins warns that terrorists are adept at manipulating our fears of WMD terrorism, without even attempting the technical challenge of making and using them.⁵⁵ However, disruptive new business models will certainly help terrorists use technology to be more agile, evasive, influential, wealthy, and deadly. Modern case studies such as the use of IEDs in Iraq and Afghanistan and Al Qaeda's use of civilian aircraft suggest a predilection for known technologies and little appetite for experimental, unproven methods that incur added risks and operational requirements.

So far, terrorists appear more likely to focus their efforts on using new technologies to improve their current operational practices. This preference for incremental improvement appears to extend to the few instances when terrorists were trying to achieve strategic effects. One hybrid possibility is cyber hacking to achieve strategic effects through media manipulation or disrupting industrial systems.

All of these terrorist innovations demand a response. Access to technology is increasingly hard to block. The level of destruction and disruption achieved by terrorists can be elevated through innovative uses of technology, new, old, and in combination. But technology does not alter the fundamental nature of those who would kill innocents and perpetrate terror. The people are more of a threat than the technologies and a far better target for counterterror efforts. Chasing technology is a losing strategy.

54 Bowyer Bell, *The Secret Army: The IRA*, 3rd ed. (New York: Transaction Books, 1997).

55 Brian Jenkins, *Will Terrorists Go Nuclear?* (Amherst, NY: Prometheus Books, 2008).

Chapter 11

The Latent Potential of Privacy Technologies: How Our Future Will Be Shaped by Today's Privacy Decisions

William Welser IV, Rebecca Balebako, Cameron Colquhoun, Osonde Osoba

Modern history is in part the story of how humans have used knowledge and technology to enrich themselves and dominate their rivals. Those with superior technologies have typically prevailed. This potential for science and technology to affect the balance of power between nations is known as “strategic latency.”¹ The concept of strategic latency is described as “technological advances—still underdeveloped—that once fully materialized could fundamentally change the power environment among key international actors.”²

While strategic latency has traditionally focused on geopolitical and military strength, the digitalization of life in the 21st century requires that a nation's power to acquire, store, and use data also be scrutinized for potential strategic latencies. In the past decade, immense quantities of data have been collected, but the human ability to exploit this data to change societies and disrupt power structures is only in its infancy. Technologies that will be developed from 2017 to 2040 will have even more potential to affect privacy, diplomacy, and the wealth of nations, and will thus have even more potential to change the balance of power between nation-states.

At present, the United States enjoys an unrivalled hegemony over data: most of humanity's personal data is under the control of U.S. companies, which benefit from access to it, whether the data is stored in the United States itself or overseas. Since these companies are subject to U.S. law and regulation, their practices may become the de facto international

1 Zachary Davis et al., “Strategic Latency and World Politics: How Technology Is Changing Our Concepts of Security.” (Livermore, CA: Lawrence Livermore National Laboratory, 2014).

2 Ibid.

norms. Thus, the United States has dominated expectations and norms of digital privacy (or lack thereof) for citizens worldwide.

In this chapter, we examine the effect of decisions about privacy, which, accumulated over the course of decades, have the power to fundamentally alter the amount of privacy available to individual citizens, and by extension, the power relationships between individuals and companies³ and between nation-states.⁴ As we have learned to our discomfort in the early 21st century, new technologies that create, collect, store, transmit, and exploit information about individuals can be used or abused to disrupt business, finance, diplomacy, elections, and other aspects of national and global affairs. This is accentuated by the proliferation and diffusion of collection sources, data breaches, and cyberattacks, and the ability to run big-data analytics on what is collected. Limitations on the use and utility of such personal data could be imposed via controls on data ownership, cryptography and encryption, and data anonymization. Decisions today about whether and how to impose such data controls—and enforce them—may have dramatic or unintended effects on society 25 years from now.

Privacy advocates have argued that as societies across the globe become more interconnected and digitized, the availability and quality of future liberties in most countries will be tied to the amount of privacy citizens enjoy, or could choose to enjoy should they wish.⁵ Regardless of its legal framework, privacy is inherently contextual:⁶ what is considered private may depend on the individual, the culture, and the situation; the persons or institutions with whom information will be shared; the perceived value of sharing information; the timing; or the location associated with the information. Therefore, inherent in privacy is the notion of individual choice and discretion.

We recognize that powerful data technologies with deep implications for privacy may in the future be developed outside the United States. However, for the purposes of this paper, we consider how new technologies developed by U.S. companies will affect privacy inside the country, and whether these technologies will enhance or undermine U.S. power with respect to other major international actors.

3 Recent examples include the politically polarized debate in the U.S. Congress over what information telecommunications companies may collect and sell about their customers' online activities, and the regulatory battle over what companies must do to secure their customers' data against unauthorized breaches. See Cecilia Kang, "Congress Moves to Strike Internet Privacy Rules From Obama Era," *New York Times*, March 23, 2017, and "F.C.C., in Potential Sign of the Future, Halts New Data Security Rules," *New York Times*, March 1, 2017.

4 Recent examples include the data breaches of Sony Pictures, allegedly by North Korea; of sensitive personnel files from the U.S. Office of Personnel Management, allegedly by China; and of emails from the Hillary Clinton presidential campaign and the Democratic National Committee, allegedly by Russia. The latter prompted the U.S. government to impose financial sanctions against Russia in December, 2016.

5 Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (Dec. 15, 1890): pp. 193–220.

6 Helen Nissenbaum, "Privacy as Contextual Integrity" (Proc. of IEEE Symposium on Security and Privacy, 2006).

To explore the potential strategic latency of privacy decisions made today, we convened a multidisciplinary group of almost two dozen researchers and experts, including from the disciplines of computer science, public policy, history, and psychology, and held structured brainstorming sessions. We imagined three plausible alternative futures for the United States in 2040. Each scenario derives from earlier decisions that were made to protect or not to protect individual privacy by means of nine specific privacy instruments that will be discussed in detail below. Each future unfolds based on the specific societal goals, values, or priorities that underpin its worldview and hence its decisions about privacy. And for each scenario, we analyze the resulting effects on U.S. national interests, specifically on military and intelligence, the economy, governance, and cultural attractiveness and soft power.

In the first imagined future, the United States has prioritized the pursuit of happiness and health over other societal goals, such as economic growth or national security. In the second scenario, the country has optimized the pursuit of personal convenience and economic growth above other national interests. In the third future, following a spate of terrorist attacks, the United States is focused above all on the pursuit of order and security. Of course, these three scenarios do not represent all possible or plausible futures, nor do they identify the probability that any particular future will come to be. Rather, they are intended to prompt us to reflect on the futures we want and those we wish to avert.

The task of imagining the future—an audacious undertaking at any moment—is particularly difficult today because the Information Age is still in its infancy. Vast information has been gathered over the past decade, yet humans are not yet able to exploit that information at scale and in near-real time. This will change due to advances in computer power, increased sophistication of artificial agents (i.e., autonomous, learning, non-biologic systems), and increased velocity of information. The question is how soon people will be able to exploit these developments to change societies, and to what ends.

Future 1: The Pursuit of Happiness and Health

In 2040, U.S. society prioritizes the individual pursuit of happiness and health, goals now deemed even more important than national-level economic growth. Society prioritizes work-life balance, public health and personal fulfillment, and advanced technologies to help achieve these goals. While some of these technologies may seem invasive, significant advances in cybersecurity and the enactment of laws and regulations to protect privacy have gradually built public trust and willingness to share sensitive data. The American public demands and expects strict enforcement of the country's anti-hacking statutes, anti-fraud regulations, restrictions on data retention and expiration, and other privacy-protecting mechanisms.

In the early decades of the 21st century, intellectual workers and hourly employees alike struggled to juggle work, commuting, family, and lifestyle, but by 2040, technological advances allow individuals increasing amounts of meaningful choice over when they are

available to work, or wish to spend time with family or friends. In 2017, last-minute, on-demand schedules for low-income workers led to erratic schedules, and hourly workers were often only given a few days' notice for their work schedule. By 2040, artificial intelligence (AI)-enabled scheduling systems exist for hourly workers and these systems predict service demand several months ahead. Therefore, part-time and low-wage workers know several months in advance what their schedules will be and are able to arrange childcare, attend school or training, meet commitments to family and friends, and even volunteer in the community. Furthermore, they are able to predict their near-term earnings with accuracy not possible in earlier decades.

Advanced scheduling systems increase business profitability by removing uncertainty about labor supply and demand, as employment scheduling systems data is merged with other data sets that track the availability of childcare, education and training, and public transportation. Workers can enter these constraints into the system in a private manner using cryptographically secured systems that ensure the inputs are anonymous, which prevents this information from affecting their job status. The collected data is then used to create a work schedule using secure techniques that utilize cryptographic protocols, such as secure multi-party computation. Such protocols are now ubiquitous as tools for preserving privacy. Scheduling and similar systems are enabled by the continued maturation of AI algorithms (in this case, specifically machine learning) and are programmed to ensure regulatory compliance.

Family size has been declining for decades. The 20th century fears of a shrinking nuclear family have given way to worries that Americans also have less and less contact with extended family, such as cousins, aunts, and grandparents, simply due to the fact that fewer of them exist. Small and far-flung families are unable to benefit from economies of scale or the mutual support systems that had historically been based on proximity. Instead, they try to offset the lack of physical access with digital methods of maintaining contact with relatives and gaining "social capital." It is now legally acceptable and technologically feasible for family members to babysit or check on elders online through home robots and video streaming. They socialize through virtual reality (VR) forums.

The sharing of intimate details among families and friends is enabled by strict data ownership laws which dictate that employees, parents, and children may allow their images or information to be used for specific purpose, but no one can sell, share, or profit from such information without explicit permission. Children's pictures and videos online have guaranteed expiration dates, allowing minor youthful indiscretions (as well as adorable but embarrassing baby bathtub pictures) to be forgotten. Starting after their 18th birthday, individuals now monitor and review all pictures and videos they are in, much like they used to check their credit reports, and they may delete these media, make corrections, or restrict access.

The practice of medicine is barely recognizable from healthcare at the beginning of the 21st century. Online AI-informed diagnosis is followed by visits to physicians only in cases

of severe illness or algorithm uncertainty. Advanced systems use AI, network analysis tools, location data, and personal health data to predict the spread of diseases and deliver real-time recommendations for mitigation and eradication. Public health officials often preempt predicted outbreaks by deploying vaccines and medicines to the most relevant locations, while also creating pre-outbreak quarantine zones. While the travel restrictions, cancellations, and logistical problems associated with such pop-up quarantine zones are disruptive, society largely accepts them, as everyone wants to avoid the devastating pandemics of prior decades. In some cases, “Patient Zero” is identified before becoming sick and placed in physical isolation, but all infected individuals are allowed private, secure communications so that they can interact virtually with family, friends, and employers.

Health data is widely collected but strictly protected. Illicit access or misuse of health data is a felony. This has enabled the sharing of vast data sets with public health officials, the research community, for-profit companies, and governments, and fuels continuous breakthroughs in the development and delivery of healthcare. The prevalence of cancer, dementia, diabetes, and other chronic diseases and conditions has declined, as research has identified foods, environmental, and genetic factors deemed causal to these chronic diseases and conditions. As a result, agricultural production of foodstuffs deemed unhealthy has decreased, and the food industry has shifted toward production of a much smaller number of expensive “superfoods” that consumers now demand. Farms struggle with soil depletion and small disruptions to climate have large-scale impacts on global food availability. Crop failure is a common occurrence due to temperature shifts and pestilence. Fortunately, AI-enabled 3D printers are in most homes and use the data stream from each individual to formulate and fabricate synthetic nutrition capsules when such disruptions occur.

Impact on National Interests

Although domestic data is well secured and privacy is heavily regulated, foreign powers, criminals, terrorists, business competitors, and ideologically motivated actors continue to try to access the extensive data that has been collected by government, industry, and nonprofits. Espionage and data theft cannot be eliminated, but they have been much reduced. U.S. government and corporate spending on cybersecurity consumes a larger share of GDP, as citizens expect a high level of digital protection. As a result of the 2030 International Convention on Data Security, data may not be used to interfere with personal or national autonomy. Hence there are several areas in which national interests have strengthened, which may improve the overall power balance in the U.S.’s favor. For example, international rivals are no longer able to build data sets about U.S. citizens or companies. And smaller countries or nefarious actors are unable to wage asymmetric cyberattacks on U.S. government and commercial computer systems. However, U.S. intelligence agencies no longer have access to behavioral data on citizens, as secondary uses of data are prevented.

As result of efficient and widespread use of data, per-capita productivity is higher and per capita GDP is increased. Expenditures on healthcare are reduced. Expenditures on food are increased. As people focus on quality of life, consumption shifts from material goods to services and digital or virtual products and technologies. Additive manufacturing allows more goods to be produced domestically, so imports fall. The main items produced for export are information and digital services. Local communities are stronger as workers now have more time to become involved. There is more engagement in neighborhoods and communities. However, the introduction of new laws or regulation becomes very slow, as consensus-building and stakeholder input are required. The United States is culturally attractive, particularly for those seeking free speech, freedom to worship, and the pursuit of happiness.

Future 2: Pursuit of Personal Convenience and Economic Growth

By 2040, the singular focus of the nation state is economic growth and the dominant political philosophy is free-market capitalism. It is widely accepted, in both social and governance circles, that personal convenience—and happiness—can be best achieved through new technologies. Decades of emphasis on economic growth, deregulation, free trade, and privatization have resulted in a hyper-concentration of societal wealth in four major technology companies. For convenience, we refer to them as the “Infogopoly.”

Together, these four companies are responsible for 50% of global GDP. They supply the world with comforts and conveniences that were unimaginable earlier in the century. The Infogopoly and the U.S. government teeter in an uneasy but mutually beneficial relationship, as new technologies have reduced U.S. government costs and deficits, and in return, the Infogopoly enjoys unprecedented access to and control over the lives of citizens. Data security is high as the Infogopoly protects its secrets.

The Infogopoly fueled growth by perfecting a business model that is irresistible to consumers and governments. In the mid-2020s, its leaders realized that their technologies, super-charged by true AI, could vastly improve the efficiency of governance, albeit with a reduction in individual privacy. By 2040, many services that had been once provided by government are now provided more efficiently by the Infogopoly. AI has drastically reduced spending on education, medicine, transportation, and elder care, but has forced government to institute a universal basic income stipend and other entitlement programs to compensate for large-scale job loss.

The Infogopoly holds tremendous political power, as their donations are critical to electoral success. Candidates of all political hues fawn for support. The academic community insists that the Infogopoly is able to steer societal views and mood through its networked technologies and subtle messaging, though politicians largely reject this and believe that they are still the decision-makers.

The United States long ago abandoned the use of widely compromised Social Security numbers, and now uses a “Citizen Identity Profile” that includes tax and banking

information, medical records, passports, licenses, and various virtual avatars. The Infogopoly provides many services for free, tailored to the Citizen Identify Profile, in return for data ownership rights. Starting in the mid-2030s, the Citizen Identity Profiles were assigned at birth and those who do not have one are severely limited in their access to basic services. Privacy advocacy groups still exist, but they focus on physical privacy, having long since abandoned hope for any semblance of data privacy.

In healthcare, the Infogopoly provides artificial or enhanced organs, which, in return for being free, are used to collect and transmit data from inside the patient's body. Those who opt-out of e-organs thus forfeit access to cutting-edge healthcare.

The Infogopoly also provides free local transportation to all citizens, who in return, must use their services because private cars are not permitted in the nation's many megacities. The result is a mini-economic boom, as urban dwellers' transportation costs fall to nearly zero, and the consumer and lifestyle sectors explode as citizens enjoy an unparalleled level of convenience. The systemic intelligence derived from full transportation data capture allows the Infogopoly to dominate retail sales, city planning, service provision, and public decision-making.

Children are deeply influenced by the Infogopoly via the virtual- and mixed-reality interfaces used for schooling and recreation. The content is so rich that children are hooked immediately, although the content developers continue to struggle with incorporating enough physical activity to avoid obesity-driven increases in healthcare costs. While there are some concerns among neuroscientists and behavioral scientists about the effects of the loss of active movement and social development, there is greater concern that children will be isolated if they do not participate in virtual education and recreation. The Infogopoly enjoys total data capture in the VR world. Every pupil dilation, hand gesture, and facial muscle movement is recorded. This and all other available data are combined to characterize every aspect of a child's personality, hone psychological and behavioral predictions, and tailor education and job opportunities.

Electric power is the Infogopoly's biggest expense. Huge amounts of electricity and water are required to power and cool colossal data centers and keep the VR and Internet worlds running. To manage costs, companies delete data that is more than five years old, placing residual markers on citizens' profiles to summarize the past. However, people can pay to keep their experiences and memories alive forever online.

The concentration of power and wealth in a handful of companies and individuals leads to the emergence of "data castes." Affluent citizens can afford to opt out of some services they deem too intrusive and hire lawyers to help them ensure that derogatory information is forgotten. At the lower end of the caste system, those designated as criminals by statute can never delete their history or change their identity. Their movement and behaviors are intimately studied to improve crime detection. This differential surveillance of certain socioeconomic groups and profiling are self-reinforcing systems; as crime-detection

algorithms improve, more and more individuals who commit petty offenses are identified and classified as criminals. Even as data is deleted to reduce electricity costs, it is difficult for children to escape the actions of their parents; long-ago deleted data that was used to profile the parents, such as income, criminal record, ethnicity, education, or zip code, is linked to their children's profiles. Such old information often comes to light after the original has been deleted, and affects decision-makers, but there is no opportunity to reconcile or reverse the decisions.

This future yields unprecedented quality-of-life improvements for the masses, but with permanent class structures, an untouchable elite, and increased corporate control of government policy. In an ironic twist, the United States now mirrors a past its founders had tried to escape: 18th-century Europe.

Impact on National Interests

As the Infogopoly's constituent companies remain based in the United States, the U.S. government retains some limited regulatory power over its activities, although the Infogopoly is politically powerful enough to shape the regulatory environment. It frequently threatens to move operations offshore in order to secure political and regulatory concessions. Infogopoly businesses are global and collect data about people in all corners of the world. This provides the Infogopoly with international clout, placing the preponderance of power in the United States but not in the hands of the government.

Because data is of paramount financial value, the Infogopoly has invested heavily in cybersecurity, which it also sells to the U.S. government and other friendly governments. Except for rare cyberattacks or espionage successes, other nations are unable to access the Infogopoly's data. However, the Infogopoly has weakened the U.S. government and is taxed at a low rate, straining the budget for military and other public services that the four companies do not wish to provide. As a result, the military is weaker and the nation is more vulnerable to physical attack.

Governance is also weakened, as are many democratic norms, as the influence of the Infogopoly spreads through the Executive, Legislative, and Judicial branches. Overseas, the United States is viewed as a rich country with an easy lifestyle. However, it is not admired for its cultural values or viewed as a safe harbor. Its soft power has eroded.

Future 3: Pursuit of Order and Security

“Are you safe?”

“Are you secure?”

“Do you know your neighbor?”

These questions are posted throughout communities on electronic systems in 2040. Citizens face constant reminders that there are sacrifices to be made in exchange for safety, security, and order, which have become the nation's primary concerns. It started in 2021 with a series of attacks by non-state terrorist groups, causing death tolls that dwarfed those of September 11, 2001. These came in rapid succession over the course of a few years. The frequency and unpredictability of the attacks sparked public fear and public outrage, including fury over the perceived incompetence or inability of the government to halt them. This brought the United States to the brink of martial law. To calm the populace and re-establish security, governments from across the globe committed to continuous military activity targeting violent non-state actors and authorized increasingly invasive domestic measures to safeguard their homelands.

The U.S. strategy is to use information dominance to preempt and punish attackers. Legislation is adopted granting broad government access to all data collected by the private sector for national security use. By 2040, private data ownership has largely ceased to exist. The U.S. government has argued that civilian data trails are public goods since they enable the state to accurately estimate citizen risk, and the courts have accepted this interpretation.

The government also commandeers resources and personnel from tech giants to supplement the military and maintain an edge in the information security battle. It conducts extensive research and development into AI systems that comply with the Lethal Autonomous Weapons Convention of 2023 and that are deployed entirely without operators, since the distributed nature of terrorist organizations requires timely, precision strikes with limited collateral damage.

Ubiquitous cameras feed facial recognition and biometric systems and are used to keep track of all persons. While commercial firms collect and store this type of information, the government uses it to develop profiles of citizens and foreign nationals of interest. Algorithm-enabled automated decision-making agents allocate enforcement resources and pre-emptively identify security loopholes. Through GPS traces, social media presence, energy usage and other indicators, information scientists establish guidelines about the information footprint that humans typically generate in their daily lives. Citizens are expected to produce data trails within predetermined volume limits. Attempting to make too much of one's data private, and thereby producing too little observable data, raises suspicion of disgruntlement or concealment. Producing and transmitting too much data raises suspicions of conspiracy or espionage.

Even as the U.S. government has abandoned privacy in its battle against terrorism, it still struggles to control the vast number of fast-moving global online networks that challenge its writ. Intellectual elites, academics, and the public begin to notice a major shift in the organization of human societies, as nations and peoples share power and influence with online sub-tribes that are no longer bound by geography, nationality, or language. These sub-tribes function as global political, economic, cultural, or ideological affinity groups. They

are technologically sophisticated, operate at the accelerated speed of the era (in contrast to slow-moving governments), and manipulate data to produce many unanticipated outcomes.

David Ronfeldt had argued in the late 1990s^{7,8} that societies were evolving from small tribal communities with hierarchical command structures to massive, unstructured, and decentralized networks. He traced his evolution in societal structures to the historical expansion in available lines of communication, starting with trade routes all the way to the internet and social media platforms. This evolution accelerated in the 21st century, leading to a fragmented and balkanized global society characterized by fluid, independent sub-tribes characterized by technology-empowered individuals.

In Future 3, an increasingly authoritarian U.S. government whose legitimacy depends on its ability to halt terrorism struggles to govern a range of sub-tribes and networks whose structures, capabilities, and behaviors are rapidly evolving. Encryption makes this accelerating world even more difficult to understand or control. Dissent—and sometimes sabotage—are waged via secretive, encrypted networks. Hyper-empowered individuals mask their information footprints and their intent with encryption protocols that advance faster than the government's ability to crack them.

Network fragmentation and balkanization reduce the barriers to mobilizing violent or non-violent dissent, and once-harmless fringe dissenters are now organizing throughout the world. These sub-tribes cause many national and supranational effects. In 2040, for example, Asian cyber-actors have created and then popped real estate bubbles in London and Dubai. The government uncovers large financial reserves whose ownership remains anonymous amongst the blockchain-enabled cryptocurrency markets. Is it the source of terrorist funding, or a stash of private wealth?

Cryptography and software engineering are now part of the common curriculum. So a large pool of people have the technical skills to use disruptive technologies, even as advanced technologies can be used to powerful effect by individuals with less and less technical expertise. Meanwhile uncertainty regarding external threats fractures the established order of a society that is already highly divided along socio-economic lines. Inequality of wealth and decades of economic disenfranchisement of the lower classes causes waves of populism, civil unrest, and crime. Wealth disproportionately accumulates in a small number of megacities that are highly globalized, diverse, and technologically advanced. A divide appears and then widens as superior digital services, with more privacy options, are offered in affluent cities, while low-income rural areas that generate less data receive fewer services and options for digital privacy. Wealth inequality, geographic inequality, and cognitive stratification have eroded national cohesion.

7 David Ronfeldt, "Tribes, Institutions, Markets, Networks: A Framework About Societal Evolution," *RAND Corporation*, 1996, <https://www.rand.org/content/dam/rand/pubs/papers/2005/P7967.pdf>.

8 "Three Dark Pieces," *RAND Corporation*, January 1990, <https://www.rand.org/content/dam/rand/pubs/papers/2008/P7607.pdf>.

High-income neighborhoods insist on total security at the expense of civil liberties. City governments, empowered by mass surveillance and powerful AI, seek to stop the surge in crime and now employ predictive policing. Behavioral data from web browsing, police surveillance, drones, and pervasive Internet of Things (IoT) devices are fed into crime-prediction models, which all use facial-recognition to identify individuals. While urbanites have no choice but to be under constant surveillance, the velocity and volume of information is so great that audits and error correction are all but impossible. False positives are commonplace, but since humans have been designed out of most systems, there is little opportunity to interject non-algorithmic judgment or sense-making. This automation bias is left unchecked as citizens are sent to prison based on algorithmic profiles that are assumed true.

Civil liberties, including freedom of speech and freedom of association, are impossible to defend in the absence of data privacy. However, most media outlets reinforce the prevailing public preference for order and security in their news coverage and the public is content that terrorists have not staged any successful attacks of late. Thus there is little public support for reinstating privacy protections or personal liberties.

Impact on National Interests

In this future world, the United States has succeeded in protecting citizens' physical safety inside the country, but its power to persuade and influence other countries, and to govern emerging global sub-tribes, has diminished. AI and unfettered access to individuals' data enhances the ability of the intelligence community to preempt attackers. Military expenditures and recruitment increase, as everyone is motivated to protect the country from physical attacks.

Inequality has gutted the middle class, meaning fewer people are able to purchase discretionary goods. Productivity and per capita GDP decrease, as people are focused on security threats. Low national cohesion leads to weak governance and protection. Focus on security reduces ability to provide other public goods.

While foreign elites seek homes in U.S. urban areas, where surveillance has sharply reduced crime, the United States is no longer viewed as a country of refuge. Soft power has eroded.

Privacy Instruments

The three preceding scenarios extrapolate to the future based on nine “privacy instruments”—tools, technologies, human-computer interfaces, laws, regulations, or business practices—that the expert group deemed likely to be particularly salient in the future. While currently underdeveloped, these instruments have the potential to gird privacy, liberty, and the uninhibited pursuit of happiness, or, by undermining privacy, interfere with individual autonomy, weakening the power of the individual vis-à-vis technology companies and/or the state.

The nine instruments are:

1. **Meaningful choice.** Options that give individuals clear choices about information sharing that they can understand and that are relevant to their needs. Many existing technologies, including apps and websites, provide a choice that is not meaningful. For example, users who do not check a box to indicate that they accept the service and accept the company's terms for privacy and data use are not permitted to use the service. This type of take-it-or-leave-it approach does not offer meaningful choice.
2. **Access control.** Individuals may choose who can access information about them, while system designers, companies, or regulators may control who has access to databases and systems. Many separate technologies, policies, and techniques are used for access control, and users may be unaware of them. For example, the proper use of encryption can ensure that only authorized parties can view information, as can physical controls—permitting data only to be accessed within a specific physical building.
3. **Data ownership.** Assignment of rights and responsibilities over data. Ideally, data ownership would confer specific value to data such that data owners are incentivized to protect their data, but also would have the right to sell or trade that data in a free, open, and transparent market. In a privacy-protective version of data ownership, data subjects may own data about themselves, and they have the right to sell that data on a free market. We currently have a skewed version of this, as users of “free” digital services essentially trade the right to use the service in exchange for their personal data, yet the value of this data is unclear—to users and governments. Data subjects may be unaware of the value of their data and even lack sufficient knowledge of specific transactions, which can lead to privacy violations and/or invasions.
4. **Data expiration.** Data-retention policies to delineate the amount of time data may be stored or made available. While there are benefits of historical records and keeping data to understand trends, there are also risks to liberty and safety from data security threats or invasive data handling. Data retention carries financial and security costs. While the collection of data often carries an associated cost, little analysis has been done to quantify the full social and economic costs associated with storing and archiving all collected data. While some costs are known at current prices, such as the construction and operating costs of large data repositories, other costs are typically not taken into account, such as those incurred from data breaches, the loss of citizens' time when extraneous data is transmitted, or the pollution caused from data storage energy usage.
5. **Data anonymization.** Sanitizing data to prevent the data from individuals in the data set from being identified. This clashes with commercial entities' and service providers' desires to understand their users to improve services, target marketing, or address customers' problems. The standard compromise over the years has been that service providers may collect de-identified data (data scrubbed of

personally identifiable information) on users on their platform. The assumption has been that de-identified data contains valuable informative patterns and trends that cannot be linked to original users in this form. Users have (or have developed) a reasonable expectation of privacy and anonymity as they use many online services. User outrage over egregious breaches serves as limited evidence for this sometimes-informal contract between users and providers. However, researchers have found that standard de-identification or anonymization techniques can no longer guarantee the anonymity of data subjects. State-of-the-art statistical re-identification techniques are powerful and easy to implement. Improvements in available computational resources, the availability of secondary data sources for cross-linking, and progress in algorithm design^{9,10} imply that most users in any data release can be re-identified given enough effort and resources. That effort will decrease in the future as computing resources become more powerful and user data sets proliferate.

6. **Data-driven profiling.** Sorting people into profiles or groups based on data and inferences from that data. It has become standard practice to collect as much behavioral data on users as possible, and the ability to collect such data will increase with the adoption of web-enabled hardware (the Internet of Things). Profiling may be based on AI or simpler formulas that weigh some data points (e.g., zip code or income level). These profiles can be highly specific and commercial firms are leveraging this data to better target ads to complement a user's habits or interests.^{11,12} Brokers sell either personal data or personal profiles constructed from personal data to firms (such as health insurers or financial institutions) that want to improve reach to certain users. However, the profiles themselves may reveal inferences that data subjects considered private, such as income, pregnancy or health status, ethnicity, sexual preference, life events such as marriage or divorce, purchasing history, and more. Furthermore, the data subjects may not even be aware that the profiles are being built, raising concerns about their ability to control information about themselves.
7. **Artificial intelligence and algorithmic decision-making.** AI is defined for the purposes of this analysis as any "non-biologic, autonomous learning system." AI is being used to inform decision-making in financial systems (e.g., for fraud detection, default risk estimation), criminal justice systems (e.g., for recidivism risk estimation, predictive policing), and health systems (e.g., disease-risk

9 Arvind Narayanan and Vitaly Shmatikov, "Robust De-Anonymization of Large Sparse Datasets," *2008 IEEE Symposium on Security and Privacy* (sp 2008): pp. 111–125.

10 "Myths and Fallacies of Personally Identifiable Information." *Communications of the ACM* 53, no. 6 (2010): 24–26.

11 "Data Brokers: A Call for Transparency and Accountability," *Federal Communications Commission*, May 2014 accessed October 27, 2017, <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

12 Charles Duhigg, "How Companies Learn Your Secrets," *New York Times Magazine*, February 16, 2012 accessed October 27, 2017, <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

estimation, radiology). These are largely in the pattern recognition sub-field. The growing magnitude and variety of available data indicates that algorithmic decision-making is likely to be a major (if not dominant) decision-making paradigm for the foreseeable future. However, these systems are opaque and can have unreliable results for sub-populations. Current implementations of AI have poor metacognitive capacity; they are not yet well equipped to recognize when they are unsure of the results. The interplay between this lack of meta-cognitive capacity and the human tendency to give algorithmic decision more credence than they deserve (automation bias), leads to poor automated decisions persisting without criticism.

8. **Cryptography.** Securing communications between the sender and recipient. Cryptography is also important for digital-signature schemes used to verify the provenance of data. Cryptographic schemes rely on enforcing a computational asymmetry between encoding and code-breaking operations. Most popular encryption schemes are based on the hard computational problem of either finding the factors of large integers (e.g., Rivest–Shamir–Adleman (RSA)) or finding discrete logarithms (elliptic curve cryptography (ECC) schemes, which work on points on elliptic curves). Encrypted communications allow individuals to protect themselves from data-hungry actors: advertisers, criminals, nation-states, and data-warehousing firms, amongst others. Recent developments in cryptography are likely to enhance the power of the individual in relation to the corporation or nation-state. However, the advent of quantum computing and quantum information processing poses threats to some of the underlying assumptions of cryptography.¹³
9. **Regulation, law, and policy.** Even the most privacy-conscious technologists cannot code away problems caused by market forces or other externalities. Legislation, regulatory measures, and policies will be required if privacy protection is desired.

Conclusions

These three future scenarios offer both positive and negative aspects of privacy-related protections and security and the implementation of the various privacy instruments. In Future 1, the focus on work-life balance and the development of personalized AI enables an existence that most people in 2017 would describe as net positive. National interests are preserved. Society sees an increase in community service, national cohesion, and overall productivity. Futures 2 and 3 would likely be viewed as a net negative change from 2017, with national cohesion diminished, governance structures undermined, and personal autonomy curtailed.

Some of the privacy instruments that we consider most salient appear in multiple futures. For example, the development of data-expiry technologies yields positive influence

¹³ Michael Nielsen and Isaac Chuang, "Quantum Computation and Quantum Information" (Cambridge Series on Information and the Natural Sciences, 2004).

in Future 1, while the continued use of old data in Future 2 results in the embedding of biases into machine-learning outputs. Some technologies are notable by their absence; for example, there is a lack of *meaningful* choice in Future 2, in which the Infogopoly manipulates choice.

In Future 1, the sophisticated level of privacy-protection instruments diminishes the power of any government to use behavioral data to persuade, influence, or control populations. This has leveled the playing field; the U.S. government and intelligence communities cannot gain advantage due to favored access to Silicon Valley giants. However, other national strengths have grown and can be leveraged in international power negotiations.

In Future 2, the Infogopoly has turned privacy tools into instruments of political power. Claiming to provide meaningful choice, the Infogopoly simply nudges users through persuasive interfaces to share data, and the increasing concept of free services in return for data capture is a bargain most citizens accept without significant debate. Control over personal data is a privilege reserved for only the most senior of the Infogopoly, and the security services of compliant nation-states. Billionaires pay huge sums to see behind the data curtain. By controlling internet protocol and encryption, the Infogopoly limits full insight and knowledge to a mere handful of individuals. Due to the power of the Infogopoly and the lack of privacy, the U.S. begins to suffer a brain drain, as skilled migrants and specialists move to countries where privacy protections are enforced and quality of life is enhanced. Over decades, this undermines U.S. leadership in technology and science, as well as its soft power.

In Future 3, AI, profiling, facial recognition, and cryptography have improved public safety and security, but many privacy-protecting instruments have been outlawed. National cohesion is in doubt. Cities are on the brink of becoming fully autonomous regions, protected by the U.S. military but otherwise independent. Due to the oppressive security policies deployed by the government, the United States has lost in soft power whatever it gained in hard power. It begins to resemble the countries that fail to develop due to overspending on military and underspending on other infrastructure. It has lost strategic power relative to the international community.

These unspooling futures help us explore how instruments that are generally considered to affect individual privacy also have implications for broader national interests and the balance of power. Three overarching issues emerge that deserve further thought. First, other international powers, as well as powerful non-state globalized networks, will evolve in unique and surprising ways, and will react to U.S. decisions about privacy and security in ways that may please or displease American companies or the government.

Second, the lack of robust valuation of personal data in today's dollars, and lack of understanding of the potential monetary value of such data, hinders informed decision-making by consumers and regulators. A person who does not know what his browsing data is worth, what it might be worth in the future, or how and by whom it might be used, cannot

make meaningful choices or trade-offs. Thus, leaving privacy choices to the discretion of consumers could allow service providers most of the power to make privacy decisions that will have strategic latency as well as broad ramifications for U.S. society and democracy.

Finally, using this approach to consider the long-term effects of today's privacy-related decisions reveals inherent tensions between three ongoing trends: the current and likely future reliance on commercial elites to determine privacy norms; the desire of governments to exercise meaningful control over technologies that have strategic latency; and the democratization of technology, whereby individuals gain access to tools that are both more powerful and easier to use. Given these three trends, the ultimate question becomes: "How will privacy fare when these forces collide?"

About the Center for Global Risk and Security

The Center for Global Risk and Security (CGRS) works across the RAND Corporation to develop multi-disciplinary research and policy analysis dealing with systemic risks to global security. The Center draws on RAND's unparalleled expertise to complement and expand RAND research in many fields, including security, economics, health, and technology. A board of distinguished business leaders, philanthropists, and former policymakers advise and support the center's activities, which are increasingly focused on global security trends and the impact of disruptive technologies on risk and security. For more information about the RAND Center for Global Risk and Security, visit www.rand.org/international/cgrs.

RAND Ventures

RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND Ventures is a vehicle for investing in policy solutions. Philanthropic contributions support our ability to take the long view, tackle tough and often-controversial topics, and share our findings in innovative and compelling ways. RAND's research findings and recommendations are based on data and evidence, and therefore do not necessarily reflect the policy preferences or interests of its clients, donors, or supporters.

Chapter 12

An Effects-Based Framework for Evaluating Latent Technology

Daniel Tapia-Jimenez

Given the important role of technology in national security, the consequences of strategic latency are not lost on analysts and researchers. However, the concept poses unique difficulties because uncertainty is inherent in its definition: strategic latency describes “technological advances—*still underdeveloped*—that...fundamentally change the power environment among key international actors” (emphasis added).¹ One way of coping with this uncertainty is to utilize frameworks which can characterize strategic latency in the same terms and concepts that apply to realized or contemporary technologies. Doing so permits us to discern differences between strategically latent and current conventional technologies. This approach also allows researchers and analysts to consider how conventional technologies could be combined with others to give rise to a case of strategic latency.

To this end, this chapter sets out to make two contributions. First, it presents an existing framework that conceptualizes technologies in terms of four distinct changes. Technologies can create changes in capabilities, means or methods of interactions, beliefs, or issue areas. Second, this chapter argues that strategically latent technologies are those that express at least two effects. Technologies that lead to two of these changes are more likely to be strategically latent because they are less likely to have available and reliable countermeasures. Submarine-launched ballistic missiles serve as a clear illustration of this argument. Looking towards the future, this chapter also applies this framework to additive manufacturing (more widely known as “3D printing”) to identify relevant changes and provide initial expectations as to how and whether it represents a strategically latent technology.

¹ Zachary Davis et al., “Strategic Latency and World Power: How Technology is Changing Our Concepts of National Security.” (Livermore, CA: Lawrence Livermore National Laboratory, 2014).

Strategic Latency and the Challenges of Technological Assessment

A technology is defined here as an object which is used to accomplish some technical end according to prescribed uses. This definition excludes social technologies like institutions, but considers technologies like the assembly line since it specifies a distinct configuration of hardware. The term “prescribed uses” is taken to mean that there is a shared expectation around how the technology should be used. It should be noted that how a strategically latent technology is to be used is unknown because its technical aspects are undeveloped. Technologies themselves are also subsets of others. For example, gunpowder is a technology, but so are bullet cartridges and firearms. When we say that a firearm is a technology, it is necessary to recognize that it is made up of component technologies (the firearm itself, a magazine, and individual bullet cartridges).

Thus, strategic latency not only concerns wholly new technologies, but also combinations of existing technologies that are used to create a strategic change when used together. Strategic latency is the development and deployment of a technology that, when fully realized, changes the dynamics of world politics. Given that strategically latent technologies “could fundamentally change the power environment among key international actors,”² such technologies clearly have long-term implications in national security strategy.

Thus, the concept of strategic latency concerns two categories of technologies: technologies that are impactful by themselves (e.g., nuclear weapons), but also those combinations of contemporary technologies that threaten security (e.g., genetic modification in combination with biological warfare). The challenge for analysts is identifying strategically latent technologies and mitigating against or leveraging them, which is more difficult in cases where a single technology is not considered one with obvious national security implications, such as many commercial technologies (e.g., fertilizer).

A historical example of a technology that contributes to strategic latency is the gyroscope. A gyroscope is an object that provides information about the direction of an object relative to a single axis because it maintains its orientation despite rotation along other axes. Combining several gyroscopes together and pairing them with computers can provide locational information and facilitate navigation for ships. Pairing gyroscopes and guidance systems with rockets can turn them into guided missiles and, with subsequent developments in capabilities, these guided missiles could obtain intercontinental strike range. Install a nuclear warhead on an intercontinental ballistic missile (ICBM) and it contributes to a strategic nuclear force that does not depend on other, more vulnerable weapon systems (as would using artillery or bombers). Early ICBMs would be difficult to deploy and use successfully without gyroscopes compared to alternative guidance systems, like radio-guided missiles. Analysts do not consider gyroscopes themselves a threat, but

2 Ibid.

rather their combination with other technologies that could be used to compromise security (hence their export control).³

The contribution of gyroscopes to ICBM guidance systems is a case where a technology can be combined with others to become far more strategically impactful than its individual technical aspects would suggest. This suggests a nonlinear relationship between individual technologies, their components, combination with others, and their consequences. This nonlinear, or latent, relationship is in large part due to whether and how states employ these technologies and how they fit into the scope of interactions between different actors, especially where an interaction or exchange is a surprising one. Indeed, when we consider technological risk, we are predisposed to worry about discontinuities.

To use an analogy, it is often not the fact that nuts and bolts could be used to help compose sturdier tanks, it is the fact that they can be used as impromptu and readily available shrapnel in an improvised explosive device that worries us. While this simple example is not typical of the magnitude of threats we are trying to identify, it is analogous to many of the concerns we have regarding strategic latency: malicious code could render infrastructure useless,⁴ additive manufacturing may increase the ability to create critical parts for nuclear weapons,⁵ and artificial intelligence and drones could violate the rules of engagement.⁶ It is these discontinuities that states intend to identify, exploit, and mitigate against.

Identifying, exploiting, or mitigating such technologies is difficult because the core of innovative activity happens outside of government auspices.⁷ Private firms are at the forefront of developing advanced technologies and their profit-centered motive may lead to the proliferation of a dual-use technology that could force a significant change in national security strategy.⁸ For this reason, it is critical to look beyond what are conventionally thought of as military technologies because focusing on them to the exclusion of the innovation driven by the market could be a crucial misstep. The impacts of military technologies are more easily understood since they will readily (or relatively quickly) be used in security applications, whereas commercial technologies' impacts on national security, let alone international relations, are harder to discern.

3 "Missile Technology Control Regime (M.T.C.R.) Equipment, Software and Technology Annex," October 20, 2016 accessed October 27, 2017, http://mtcr.info/wordpress/wp-content/uploads/2016/10/MTCR-TEM-Technical_Annex_2016-10-20.pdf.

4 P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).

5 Maryne Dijkstra et al., "U.S. National Security for Additive Manufacturing" (capstone project, Yale Jackson Institute for Global Affairs, 2014).

6 Kosal, M. *Science, Technology, and the Future of Warfare*. (West Point, NY, 2016). Retrieved from <http://mwi.usma.edu/science-technology-future-warfare>.

7 Daniel Headrick, *Technology: A World History* (La Vergne, TN: Oxford University Press, 2010).

8 Davis, *Strategic Latency and World Power*, 2014.

In order to better understand how technologies can contribute to strategic latency, this paper advances a framework which aims to guide analysis of potentially disruptive technologies. Given the need to address the latent potential of dual-use technologies, the framework applies regardless of whether a given technology is understood as a commercial or military one. The framework provided here identifies the ways combinations of technologies can affect the strategic environment. It is not meant to supplant the conventional approach, which is to start with the assumption that technology *will* provide some advantage in a competition against other states, but to complement it by identifying a given technology's other, less noted potential impacts.

In so doing it provides a vocabulary to speak about commercial or military technologies in common (non-technical) terms and to help identify important but secondary aspects of technology that could impact national security in subtle, non-linear ways. To illustrate the usefulness of the framework, I argue that technologies which express at least two of the following technological effects—that is, whether they change relative capabilities, means of engagement, methods of interaction, or ideas, or redefine issue areas—should be considered strategically latent technologies.

A Framework of Technological Effects

While we often view technology as a gadget that allows us to accomplish some task, all technologies have at least two defining aspects: their technical characteristics and the social ideas regarding their use. The technical characteristics are the objective features of a given technology; for a missile, this would include a missile's range or its warhead's explosive yield, or payload capacity. The social ideas regarding a technology's use are the implicit or explicit beliefs we hold about the technology and how it should be used. Sputnik, for example, was little more than a metal ball with antennae, but it triggered the space race and opened a new chapter of Cold War competition. Similarly, a rocket can be viewed as a space exploration vehicle, or a delivery system for strategic nuclear weapons, but is not considered an appropriate means for dispersing protesters or disposing of planetary waste.

It is interesting that Elon Musk's new missiles are not considered threats while North Korea's are. Just as individuals have social beliefs about how technologies should be used, states do as well with their social referents being their domestic constituents and the international community. We need to expand our thinking about the possible uses of latent technologies.

Provided this duality between a technology's technical aspects and how it is understood by people, it is virtually impossible to fully appraise a technology's consequences without considering both aspects. Knowing a technology's material form or technical characteristics is critical to understanding its uses and the potential tactical changes it may create. For example, it is important to know if a country has ICBM capabilities and whether their range presents a threat. Hence, technical information is critical for understanding the potential of technologies. Meanwhile, understanding social ideas that

guide technologies' use can provide expectations about how some fit into the ensemble of interactions between states. For instance, the goals and means of cyberwarfare are viewed very differently by the U.S. Navy and Air Force.⁹ Both branches recognize cyberspace as a domain to contest, but their strategies differ tremendously. The Air Force, adhering to Douhet's principles, views the objective as conducting offensive operations in order to disable the enemy. Thus, they are likely to attempt to disrupt or otherwise target the opponent's commercial capacities directly. Conversely, the Navy, in following Mahanian ideas of the seas, is likely to primarily focus on preserving "cyber lanes of communication" in addition to disabling enemy cyber operations.¹⁰

In this way, technologies' social aspects help us understand their potential role and use in a given context. When considering questions of capabilities and intentions, it is clear that technical aspects speak to the former while the social aspects address the latter. However, social aspects address more than intention because they include the context that technologies are situated within: they consider the manner of deployment and appropriateness of use. For example, why is it considered a war crime to use lasers to blind enemy combatants, yet acceptable to kill them with bullets and bombs? Of the technical characteristics and social aspects, the latter aspects are often the object of concern for political analysis because those ideas ultimately determine the use and impact of technologies.

Thus, to understand technologies' role in international relations it is critical to identify a social context, the preferences and intentions of actors involved, and some understanding of the relevant activities into which the technology will be injected. Realistically, this may amount to identifying the social context as an interaction such as the bilateral relationship between the United States and the United Kingdom, and the relevant activities being traded between them as part of their long-running security cooperation.

In another example, the bilateral relationship between the United States and the Soviet Union probably tended to have more security competition and contests for political influence. The context was the Cold War. Having an initial grasp of the social context and relevant actors is critical to properly understanding how technologies will be deployed by actors. We would expect the role of new military technology to be shared and potentially co-developed with allies, as was the case with the Polaris missile system with the United States and United Kingdom, or be a point of tension as was the development of second-strike capabilities between the United States and Soviet Union. The U.S. did not have similar concerns about the development of French missiles and independent deterrent.

Because the impacts of a technology are conditioned by context, this means that the effects of technologies lie in the intersection of their technical aspects and the social milieu. While

9 W. Alexander Vacca, "Military Culture and Cyber Security," *Survival* 53, no. 6 (2011): 159–76.

10 *Ibid.*, p.170.

the technical aspects can give us an indication of a technology's military potential, social ideas will tell us the role that technology will actually play. However, even within a single context there are different types of changes that technologies can create.

The consequences of nuclear weapons in terms of sheer destructive power are important, but in addition to different delivery systems (at first, strategic nuclear weapons were delivered by bomber, then by ICBMs, multiple independently targeted reentry vehicles, or submarine-launched ballistic missiles), there are also different treaties and international organizations (Strategic Arms Reduction Treaty, International Atomic Energy Agency, the Non-Proliferation Treaty), and emergence of specialized knowledge and ideas (deterrence theory, development of detection and verification methods, ethical and moral dilemmas), which to varying degrees shape the way this technology is conditioned to impact national security.

As the definition of technology here implies: there is nothing inherent about a nuclear warhead that produces the emergence of arms control, the International Atomic Energy Agency or the Non-Proliferation Treaty. The consequences, namely the different means of delivering strategic nuclear weapons, the organizations, or emergence of norms, are products of policies and decisions between actors. It is the combination of these consequences that ultimately change the security environment. While the technical characteristics of a nuclear weapon matter, analysts and policymakers are frequently concerned with the uses of a technology and the subsequent demands it places on states to adapt in the long term. While any significant technological change is likely to create changes at the tactical level, those that have implications in the long term demand strategic adaptation, with corresponding investment and effort to implement successfully. Latency, in other words, often must wait until social reactions catch up with technical specifications.

While it is an insurmountable task to catalog all possible social reactions to a technology, there are ways to abstract them into useful categories. The framework advanced here refines and develops an existing one in order to tailor it to the demands of policymakers. It holds that there are four changes that technologies can create for world politics: changes in capability, changes in the means or methods of interactions, changes in ideas, or changes in issue areas.¹¹

Changes in Relative Capability

When technology is initially evaluated for its implications, changes to capabilities are often the most salient consideration. Within this framework, technological changes in capability afford greater abilities to deliver on technical ends. More secure computer code, faster or stealthier jet fighters, more mobile armored vehicles, or accurate imaging technologies help states to pursue their security objectives. These changes are clearly driven by the technical

11 Charles Weiss, "Science, Technology and International Relations," *Technology in Society* 27, no. 3 (2005): 295–313. Although in the original presentation, changes in capability, means or methods of interaction, ideas, or issue areas are considered ordering, interactive, ideational, and substantive effects, respectively.

aspects of a technology in the sense that objects are explicitly designed to be faster, safer, stealthier. Whether states take advantage of their technical potential successfully depends on its deployment and use in strategies. However, whether technologies have such potential follows from their technical aspects. Changes in relative capability are usually expected (because there would be no reason to develop them otherwise).

One caveat with respect to changes in capabilities is that new is not always better, as argued by David Chu in his chapter. More complex and sophisticated technologies may actually present liabilities if rivals possess countermeasures that undermine their utility. Networked combat systems that are susceptible to cyberattacks come to mind.

Changes in Means or Methods of Interactions

A technology that changes the means and methods of interactions are those that change either the tools used in an interaction or the types of actors involved in an interaction, or create a new interaction all together. Such interactions could be anything from diplomatic communication, to surveillance, to the destruction of enemy forces (do states send a bomber, use artillery, or deploy a drone?). Following the development and deployment of a technology, if interactions differ relative to previous ones by including a new actor or component, subtracting one, or enabling interactions between actors that previously did not interact, then a technology is said to change the means or methods of interactions. Whether this effect could be discerned from technical or social aspects depends on the technology, but social media is an example where individuals utilize phones, computers, and networks to communicate with one another. Beyond the internet itself, technologies that rely on telephone networks to connect computers to the internet could lead to changes in the means or methods of interactions, as was the case in the Arab Spring when hackers used phone lines or other non-conventional means to reconnect with the outside world.¹²

Changes in Causal or Normative Beliefs

A technology can induce changes in either causal or normative beliefs. Causal beliefs are taken to be those about the natural world. They include observations about the world, like whether a nuclear test has occurred, or measurements of water levels or surface temperatures. Note that an emphasis on causal beliefs does not presuppose the discovery of a truth, only a belief that some observed event is due to an identifiable cause, e.g., we detect a rise in sea levels because it in fact has occurred; we observe large radar signatures because there are bombers in the air. Normative beliefs are those that concern whether a given action is acceptable by relevant actors.

The nuclear-weapons use taboo, for example, is one such normative belief. Technologies are said to change causal or normative beliefs if, through the development and deployment

12 Yasmine Ryan, "Anonymous and the Arab uprisings," *Al Jazeera*, May 19, 2011 accessed October 27, 2017, <http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html>.

of a technology, they are different than before. In the case of causal beliefs, those about the natural world are most clearly driven by technical aspects. Sensors, satellites, and meters are all designed with the intention of providing information and informing causal beliefs. With respect to normative beliefs, that is almost entirely driven by the role that a given technology would play with respect to societal and political interactions.

Changes in Issue Areas

Finally, technologies can affect the content of international negotiations by either creating complications for previous issues, as was the case with genetically modified organisms and climate change, or creating entirely new ones, as was the case with nuclear proliferation following the creation of nuclear weapons. Such issue reformation typically involves the emergence or challenging of norms. Technologies that lead to these kinds of effects have been the subject of international treaties and arms control negotiations, or affect other negotiations such as energy or trade.

Technological Effects of Strategically Latent Technologies

With respect to strategic latency, relevant technologies will likely change capabilities because the intentions behind their development and use will guide their employment in such a fashion as to leverage their applications for security. This implies that even technologies that are not expected to lead to changes in national capabilities, like most developed for commercial applications, can nonetheless find themselves applied to military applications. Indeed, the U.S. military, through the Defense Advanced Research Projects Agency (DARPA), actively searches for military applications of newer technologies. The internet was a DARPA project, but cyberwar was not the objective.

There are countless scenarios we can imagine where one technological effect (say a change in interactions) would imply changes in capabilities. For example, drones changed interactions in that they represented a new way to monitor, target, and strike terrorists. In this case, the change in interaction, the delivery of a missile onto a target, implies a change in capabilities because it becomes easier to conduct counterterrorism operations.

Although the changes above could be construed as a change in capability, it is still valuable to consider the technological effects separately—even though that is the primary preoccupation when considering strategically latent technologies. Recasting all technological effects as changes in capabilities may make it difficult to incorporate commercial or dual-use technologies that are not explicitly geared towards security applications. Technologies that are developed for civilian use can nonetheless find an innovative application in security. With respect to gyroscopes, although the technology was invented as a curiosity, they provided information about an object's orientation relative to a fixed plane. In the parlance of the framework above, that information changed causal

beliefs and played a vital role in enhancing the navigation for warships and later for ballistic missile guidance.

Gyroscopes today still inform us of our orientation, but the primary concern lies in that they can also guide ICBMs. Technologies being developed today—especially nascent ones—may not lend themselves to an obvious military application but will nonetheless present at least one of the technological effects presented above. Big data analytics is such an example, where military applications were not the original motivation but have gradually become apparent for use in guiding swarms and robots on the battlefield.

Another observation about the framework is that even though the individual effects are distinct, changes occur in the way we view entire issue areas. Technologies that enable new types of interactions, such as telephones or internet-enabled computers, can create new issue areas, where international coordination is necessary to maintain the functionality of a technology. For example, the Internet Engineering Task Force is primarily concerned with maintaining and improving the technical infrastructure of the Internet.¹³ Technologies that dramatically increase destructive capabilities—like nuclear weapons—can spawn entire issue areas, like the “ban the bomb” disarmament movement. Technologies that change or otherwise shape normative beliefs can warrant the creation of new efforts to control or regulate, as is the case with the CRISPR-Cas9 gene-editing method.^{14,15} The creation of issue areas can be considered partly a function of individual technological effects, because in their absence there would be no cause for people and governments to expend effort to address the issues created by them. Entire organizations and bureaucracies are created around the perceived effects of various technologies.

Of course, dramatic increases in a weapon’s destructive capability, precision, or range often inspire countermeasures. In both cases, it is the combinations, or convergence, of technologies to form systems that causes strategic consequences. For instance, the destructive capability of a single bomb is not necessarily game-changing. It is the combination of atomic bombs and delivery systems, airplanes and missiles that changes relations between states. Recall that for the purpose of this essay, I define strategic latency as combining the effects of at least two technologies to create a new security concept that either changes the means or methods of interaction, or changes causal or normative beliefs in addition to changing capabilities.

These effects are products of social interaction between states or groups and subsequently will vary from relationship to relationship. For example, the nuclear weapons program in the United Kingdom is seen by the U.S. as more of an assurance of allied capabilities, in contrast to the nuclear program in North Korea. Nevertheless, if a technology consistently

13 “About the IETF,” *Internet Engineering Task Force*, 2017, <https://www.ietf.org/about/>.

14 James Clapper, *Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence. (Washington, D.C.: Office of the Director of National Intelligence, 2016).

15 Patrick Hsu et al., “Development and Applications of CRISPR-Cas9 for Genome Engineering,” *Cell*, 157, no. 6 (2014): 1262–78.

expresses a specific set of technological effects in similar situations (e.g., in a series of interactions between rivals or allies) then it is relatively safe to say that those effects are in fact broadly present.

The extent to which a technology can express these effects *meaningfully* is important to consider. For example, an improved version of an algorithm that tracks targets under surveillance can represent a change in capabilities, but it may present no functional difference in how a drone or satellite operator conducts surveillance. It's the context that changes. Just because effects of particular technologies exist does not necessarily make them meaningful. Sometimes a cigar is just a cigar. Assessing whether a technology will meaningfully express any one effect relies on knowledge about the social units in question (national, bilateral, multilateral, and so on) as well as technical characteristics at the tactical, operational, or strategic levels.

This framework can only contribute to understanding predictable technologies. That is, the direction of technological development needs to be evident in some way. Accidental discoveries cannot by definition be anticipated, while effort expended on making discoveries or creating innovations can be apparent in some cases. As has been widely accepted in thinking about latent technologies: surprise is inherent. These technologies are not the concern of this framework. States' deliberate attempts to create an advantage via the development or combination of emerging technologies are the focus. Predictable technology is simply taken to mean that analysts can reasonably say what the function of a technology would be or comprehend its likely direction. For example, the end goal of continued development of missiles is relatively clear.

With these caveats and the description of the framework in hand, the next section applies it to two technologies: submarine-launched ballistic missiles and additive manufacturing.

How Technological Effects Inform Understandings of SLBMs and Additive Manufacturing

The usefulness of the framework and the information it draws out is illustrated below with two examples: submarine-launched ballistic missiles (SLBMs) and additive manufacturing (AM). In each case, the framework highlights the impacts and strategic consequences of the technology.

Submarine-Launched Ballistic Missiles and the Fleet Ballistic Missile

The development of a fleet ballistic missile (FBM) and the creation of the SLBM were driven by the desire of the U.S. Navy to play a role in the nuclear weapons mission. The driving force behind this attempt was the Special Project Office (SPO), which experimented with liquid-fueled ballistic missiles launched from the decks of ships before settling on

the idea of submarine-launched missiles over nuclear-equipped cruise missiles.^{16,17,18} The combination of ballistic missile technology and submarines has resulted in what many believe to be the most robust leg of the nuclear triad. Given the reality that submarines are difficult to detect, they enjoy virtual invulnerability and as such are very difficult to counter.

However, developing the SLBM involved technical demands that required sponsorship from the Navy and the SPO in order to create necessary underlying technologies. For example, conventional ballistic missiles were launched from fixed positions, and initially the lack of accuracy could be compensated by the large yield of the nuclear payloads. However, SLBMs would not be launched from fixed positions, but from international waters, where the submarines would be in motion while launching. Higher accuracy in these cases was important because small errors in the calculation of the point of origin would add up to intolerable errors in the actual destination of a weapon. And of course, launching a missile from underwater itself presented a major challenge.

Whereas the weight and size of land-based ballistic missiles were limited by their propulsion, SLBMs faced more stringent size and weight constraints imposed by using submarines as their launch vehicle. They had to be small enough to fit into a submarine and light enough to have a useful range. In order to make launches from submarines feasible and useful, drastic reductions were needed in the weight and size of nuclear warheads and ballistic missiles.^{19,20} These improvements in design coincided with developments in solid fuel, computing, navigation, and inertial sensors which, when combined, made SLBMs a feasible method of delivering nuclear weapons.

Under this framework, SLBMs were a strategically latent technology because they combined several technological systems: missiles and their guidance systems and submarines. First, ballistic missiles enabled countries to deliver warheads to other countries without putting the delivery system itself at risk. This counts as a change in interactions because, prior to ballistic missiles, the act of conducting strategic nuclear strikes would rely on bombers. Fixed missile silos or mobile launchers could be vulnerable to attacks, but they would remain further from the target's defense than bombers would. Meanwhile, submarines themselves have unique capabilities, most relevant of all the ability to remain undetected—and thus unable to be targeted—before striking. Relying on submarines to hold and deliver

16 Graham Spinardi, *From Polaris to Trident: The Development of U.S. Fleet Ballistic Missile Technology* (Cambridge, MA: Cambridge University Press, 1994); MacKenzie, D. *Inventing Accuracy: A Historical Sociology of Nuclear Missile* (Cambridge, MA: The MIT Press, 1990); Strategic Systems Program Office. (1986). *FBM facts/chronology: Polaris, Poseidon, Trident*. Washington, D.C.: Navy Department.

17 Graham Spinardi, *From Polaris to Trident: The Development of U.S. Fleet Ballistic Missile Technology* (Cambridge, MA: Cambridge University Press, 1994).

18 *FBM facts/chronology: Polaris-Poseidon-Trident*. Washington, D.C.: Strategic Systems Program Office, Navy Department. (1986).

19 Ibid.

20 Spinardi, *From Polaris to Trident*, 1994.

nuclear weapons combines the advantages of ballistic missiles with the asymmetrical advantage of nuclear submarines.

The result is that the sea-leg of the U.S. nuclear triad would not be as vulnerable to a first-strike as the air- or land-based legs. As a consequence, the sea-leg could both conduct and survive a first strike, granting the U.S. a second-strike capability with the development and deployment of the Polaris SLBM. While submarines had countermeasures, they were not as vulnerable as bombers were to air defenses. Further, where submarines used to be limited to attacking sea-based targets (e.g., surface ships, other submarines), their newfound ability to strike at land-based targets complicated the defense of cities or other vulnerable areas. As a consequence, the fact that SLBMs further made a second-strike capability feasible forced states to change their national security strategies by making mutually assured destruction a reality. Thus, SLBMs led to two changes: they advanced the destructive capability of states, making first-strike strategies less feasible by ensuring survivable second-strike options, and they changed nuclear deterrence by adding a new domain to the balance of terror.

Additive Manufacturing and Its Implications

Additive Manufacturing (AM), otherwise known as 3D Printing, is a developing manufacturing process that is expected to affect national security and global economic activity. AM enables the production of goods that would otherwise require substantially more investment and time. AM creates products layer-by-layer, building objects from the bottom up. This is contrasted with conventional techniques, which start with raw material and then subtract portions in order to create a desired object (this is referred to as subtractive manufacturing).

Unlike nuclear weapons technologies, AM was developed in the private sector.²¹ Although some initial research was spearheaded by Department of Defense, it was quickly adopted and adapted by the private sector. Although the United States was an early pioneer in this area, the cutting edge in the private sector is currently in foreign countries (e.g., China, Germany).²² Among many, there are two particularly salient national security interests in AM. One important application is the ability it grants to create the components for important repairs closer to the battlefield.²³ This would make it easier to maintain and repair equipment and, because these components are constructed on site, do not require a vulnerable supply chain.²⁴

21 Dijkstra, *U.S. National Security for Additive Manufacturing*, 2014.

22 Anderson, E. (2013). Additive Manufacturing in China: Threats, Opportunities, and Developments (Part I). Accessed from <http://escholarship.org/uc/item/9x38n9b3> on October 27, 2017.

23 Connor McNulty et al., "Toward the Printing World: Additive Manufacturing and Implications for National Security," *Defense Horizons* 71 (2012): 1–16.

24 *Ibid.*

Replacement parts will no longer require large numbers to be held in stock, but AM would allow the individual production of parts where needed. Another important interest lies in AM's ability to improve capabilities by way of permitting designs that are not possible or are impractical using conventional methods. Because AM builds objects from the bottom-up, it opens the door for new designs with particularly special properties, like materials with "negative stiffness."^{25,26}

The property of AM to fashion stronger or more complex objects without being penalized for its complexity is known as "complexity free." This property makes it possible to produce objects that previously required specialized equipment and training with only a build file (essentially a 3D blueprint) and the appropriate material.

AM will be a ready complement to other technologies and will intersect other technological paradigms that are relevant for national security. In particular, build files will be vulnerable to cyberattacks in the sense that schematics may be easily stolen and then the object easily reproduced by another country, or be corrupted in such a way as to sabotage further reproduction of the object.²⁷ AM will have applications in biotechnology, potentially growing tissue from a patient's biological material.²⁸ It is also very possible that there will exist a convergence between nanotechnology and AM, as work on the former relies on a process similar to AM for the construction of nanoscale gears and mechanisms.^{29,30}

Under the framework, additive manufacturing could be considered a strategically latent technology for two reasons. First, additive manufacturing itself expresses two technological effects. Second, additive manufacturing's intersections with other fields (nanotechnology, biotechnology) will make it very likely that it will enable new combinations in ways that represent strategic latency, if not enable it. The first technological effect AM expresses is the improvement of a state's capability to create complex objects with unique properties without the need for specialized production facilities. The second technological effect involves changes in interactions: the process of producing specific goods will likely change following the greater diffusion of additive manufacturing printers.

The resulting change in the production process is likely to be the most impactful aspect of the technology. Because in some cases this technology removes the need for specialized

25 Eric Duoss et al., "Cellular Solids: Three-Dimensional Printing of Elastomeric, Cellular Architectures with Negative Stiffness," *Advanced Functional Materials* 24, no. 31 (2014): 5020.

26 Michael Lucibella, "Manufacturing Revolution May Mean Trouble for National Security," *APS News*, April 2015 accessed October 27, 2017, <https://www.aps.org/publications/apsnews/201504/revolution.cfm>

27 McNulty, C. M., Arnas, N., & Campbell, T., *ibid*.

28 *Ibid*.

29 Olga Ivanova et al., "Additive Manufacturing (AM) and Nanotechnology: Promises and Challenges." *Rapid Prototyping Journal* 19, no. 5 (2013): 353–364.

30 "Application of Nanomaterials to National Security," *Pacific Northwest National Laboratory*, December 2, 2010 accessed October 27, 2017, http://www.pnl.gov/nano/research/pdf/Nano_for_National_Security_Flier_12-02-2010.pdf

producers, it will be a very different activity to purchase an important part or begin to construct something to very particular specifications. This will likely change how individuals, groups, companies, and governments interact with one another unless AM equipment, like conventional manufacturing equipment, remains highly concentrated. However, given that plastic printers are easily available and developments in powder-based printers are improving access and quality, AM technology is expected to be particularly prone to diffuse and thus decentralize production.³¹

The combination of these two effects poses unfamiliar challenges to national security. As it stands, governments know how to regulate the production and movement of goods with highly specialized production sequences. Contemporary export controls restrict their movement and sanction actors accordingly.³² How countries will deal with the decentralization and despecialization of production processes due to AM's "complexity free" trait is still a difficult question, especially as the required build files can travel relatively freely through information and communication networks. Further, the convergence of technologies like nanotechnology and biotechnology with additive manufacturing means it is far more likely that AM will be a component in a strategically latent technology, if not enable and make strategically latent combinations of technologies more likely. Unlike SLBMs where the criterion of two technological changes is met by the combination of two distinct technologies (ICBMs and submarines), AM can be considered strategically latent under this framework solely on its own merits—saying nothing of the likelihood that it combines with other technologies to provide strategic latency.

Conclusion

The framework described above can help researchers and analysts understand how technologies can change long-term strategic environments in ways beyond strict improvements in capability. It draws our attention to technology's social aspects in order to fully appreciate the consequences that follow technology's development and deployment. The four technological effects identified by the framework are relevant for international security in and of itself.

However, strategic latency, as characterized by the framework, is distinguished by the expression of at least two effects. The expression of multiple effects by a technology reflects strategic latency because such a technology would be difficult to counteract. SLBMs and AM represent illustrations of this point. The implications of technologies discussed here are that those that are more readily combined with others or express multiple technological effects are more likely to be strategically latent. With this insight in mind, understanding contemporary technologies through the framework presented can help identify potential developments under which they would become components of strategically latent technologies.

31 Ibid.

32 Boeing was penalized for allowing military-grade gyroscopes to be exported. See "Arms Control Act Violation (QRS-11 Gyrochip)" *Project On Government Oversight*, accessed October 27, 2017, <http://www.contractormisconduct.org/misconduct/913>.

3

The Blue Side: Technology Innovation and National Security Applications



Chapter 13

What Works? Public–private Partnerships for Development of National Security Technology

Frank D. Gac, Timothy P. Grayson, and Joseph M. Keogh¹

Why Do Government Partnerships with the Private Sector Matter to Manage Strategic Latency?

For decades, governments, and particularly the U.S. government, drove the development of advanced technology. The technologies produced by those efforts, including nuclear, space, electronics, and many others, coupled with their associated impact, have helped us recognize and define what we now call strategic latency, namely, “...the inherent potential for technologies to bring about significant shifts in the military or economic balance of power.”^{2,3}

Times have changed. While governments will always drive the creation of some niche capabilities that have no market outside national security, most technology domains are now inspired by the commercial sector (see Figure 1). This is driven partly by the forces of globalization but mostly by the sheer magnitude of investment in the private sector compared with most governments. To get the technology it needs and protect against technology surprise, the U.S. government must engage in partnerships with the private sector. This chapter examines efforts to create such partnerships and evaluates their effectiveness.

¹ The views expressed are those of the authors and do not represent positions or policies of the U.S. Government.

² Zachary Davis et al., “Strategic Latency and World Power: How Technology is Changing Our Concepts of National Security” (Livermore, CA: Lawrence Livermore National Laboratory, 2014).

³ Zachary Davis, Frank Gac and Michael Nacht with the assistance of Joey L. Ching “Strategic Latency and Warning: Private Sector Perspectives on Current Intelligence Challenges in Science and Technology” (Livermore, CA: Lawrence Livermore National Laboratory, 2016).

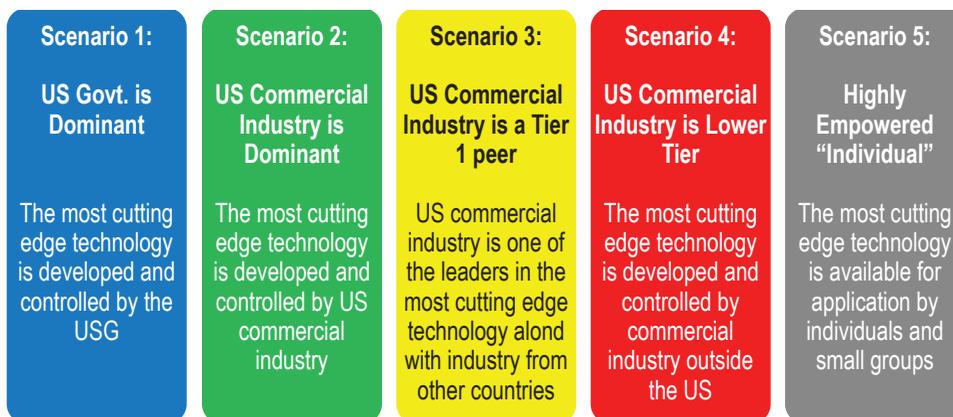


Figure 1: Shifting dominance of technology.

Consider the comparison of national Gross Domestic Products (GDP) to revenues of the Fortune Global 500 (see Table 1). Total GDP of the top 100 countries (or G100) in 2013 was about U.S. \$75 trillion. The combined revenue of the Global 100 was U.S. \$14 trillion, not an insignificant fraction. If it were a sovereign nation, the biggest Global 500 company would be the 29th richest country, ahead of advanced countries such as Austria, United Arab Emirates, Singapore, and Finland.⁴

The scale of this revenue has a dramatic impact on where technology development occurs. While there is not a comprehensive source of data on research spending, consider the following simple model. On the government side, suppose about 30% of a country's GDP is government spending, of which 50% is discretionary, and 10% of that discretionary amount goes to research. On the private sector side, assume 5% of revenue is spent on research and development (R&D), and perhaps as high as 15% for a technology-intensive company. (Admittedly much of that commercial R&D is product-development heavy and not actual technology investment, but it does eventually flow down to technology funding.) Based on this model, the largest single company likely spent about as much money on R&D as somewhere between the eleventh- and the third-largest country. An estimate of total R&D for the G100 countries is about U.S. \$1.1 trillion, and for the Global 100 companies U.S. \$1–2 trillion. At an individual agency and company level, the 2013 budgets for well-known U.S. government R&D organizations were NASA at U.S. \$16 billion,⁵ DOE at U.S.

4 See <http://data.worldbank.org/data-catalog/GDP-ranking-table> for list of GDPs and <http://fortune.com/global500/2013/> for the Global 500 list, last accessed October 27, 2017.

5 "FY 2015 President's Budget Request Summary," NASA, accessed October 27, 2017, http://www.nasa.gov/sites/default/files/files/508_2015_Budget_Estimates.pdf.

\$12 billion,⁶ and DARPA at U.S. \$3 billion.⁷ In comparison, some well-known technology companies are believed to have spent well over U.S. \$10 billion each on R&D⁸ and it may be closer to U.S. \$20 billion.

The scale of private-sector investment drives the importance of public-private partnerships for government understanding and leveraging technical surprise, which is critical for maximizing the benefit and minimizing the threat. With this much investment at stake, the private sector spends significant time and resources on trend analysis, market projection, and avoiding technology surprise in the marketplace. In many cases, private-sector companies are the source of strategic latency for their own business, since being the first mover on a major new market or societal trend can be worth billions in competitive advantage.

At the same time these companies are analyzing markets and global trends so they can target their investments. They do this offensively to find new market opportunities for their own exploitation, and defensively to avoid being surprised by a competitor. The finance sector contributes to this horizon scanning, as they are constantly looking for new investment opportunities and performing due diligence on the competitive position of their portfolio companies. All of this competitive activity creates an estimated \$17 billion market in business market intelligence.⁹

In summary, public-private partnerships are crucial for the government to understand and leverage strategic latency to create and avoid surprise, because the private sector is spending so much of its own effort trying to stay ahead of the pack and is often the first and best indicator of emerging strategic latency.

6 https://www.whitehouse.gov/sites/default/files/microsites/ostp/fy2013rd_summary.pdf, last accessed October 27, 2017.

7 Department of Defense Fiscal Year (FY) 2013 President's Budget Submission, "United States Special Operations Command," February 2012 accessed October 27, 2017, [http://www.darpa.mil/attachments/\(2G4\)%20Global%20Nav%20-%20About%20Us%20-%20Budget%20-%20Budget%20Entries%20-%20FY2013%20\(Approved\).pdf](http://www.darpa.mil/attachments/(2G4)%20Global%20Nav%20-%20About%20Us%20-%20Budget%20-%20Budget%20Entries%20-%20FY2013%20(Approved).pdf).

8 Adam Levy, "5 Tech Companies Spending More on R&D Than Apple Inc.," *The Motley Fool*, Jun 14, 2015 accessed October 27, 2017, <http://www.fool.com/investing/general/2015/06/14/5-tech-companies-spending-more-on-rd-than-apple-in.aspx>.

9 "Gartner Says Worldwide Business Intelligence and Analytics Market to Reach \$16.9 Billion in 2016," *Gartner*, February 3, 2016 accessed October 27, 2017, <http://www.gartner.com/newsroom/id/3198917>.

World GDPs and Fortune Global 100 (2013)			
World GDP		Fortune Global 100	
Rank	Country/Company	GDP/Revenue (U.S. billions)	Est. R&D spending (U.S. billions)
1	United States	16,768.000	251.520
2	China	9,181.000	137.715
3	Japan	4,899.000	73.485
4	Germany	3,730.000	55.950
5	France	2,806.000	42.090
6	United Kingdom	2,678.000	40.170
7	Brazil	2,244.000	33.660
8	Italy	2,149.000	32.235
9	Russia	2,097.000	31.455
10	India	1,938.000	29.070
...			
28	Taiwan	489.000	7.335
1	Royal Dutch Shell (Neth.)	481.70	72
2	Wal-Mart Stores (U.S.)	469.16	70
3	Exxon Mobil (U.S.)	449.89	67
4	Sinopec Group (China)	428.17	64
29	Austria	428.000	6.420
30	Thailand	420.000	6.300
5	China National Petroleum (China)	408.63	61
31	United Arab Emirates	402.000	6.030
6	BP (UK)	388.29	58
32	Colombia	378.000	5.670
...			
36	Malaysia	312.000	4.680
7	State Grid (China)	298.45	45
37	Singapore	296.000	4.440
...			
41	Finland	267.000	4.005
8	Toyota Motor (Japan)	265.70	40
42	Egypt	255.000	3.825
9	Volkswagen (Ger.)	247.61	37
43	Greece	241.000	3.615
10	Total (France)	234.28	35

Table 1: Revenue of the ten largest Fortune Global 500 companies as related to 2013 Gross Domestic Products (GDPs). Each country or company is ranked within its category. R&D spending is estimated based upon a simplistic model of a certain percentage of GDP or revenue, respectively.¹⁰

¹⁰ Derived from <http://data.worldbank.org/data-catalog/GDP-ranking-table> for list of GDPs and <http://fortune.com/global500/2013/> for the Global 500 list.

Taxonomy of Government Public-private Sector Partnerships

Given the importance of working with the private sector, there is value in recognizing the many forms that public-private partnerships may take. Understanding what the government's objectives are for these partnerships is a good first step. They can be diverse, but often include the following goals. (See Figure 2.)



Figure 2: Plot showing spectrum of type of partnerships.

Active influence. At one extreme is the government's desire to drive the creation of strategic surprise that can be used to its own advantage. There are various types of partnerships that enable the government to take an active role in driving the technology agenda. As will be discussed, these partnerships can range from variations on more traditional government procurement relationships, to innovative approaches aimed at influencing development that relies on private investments to fund R&D but provides the government access to the outcome as a commercial product. At the very least, the government wants assured access to game-changing technology that is likely to have strategic effects.

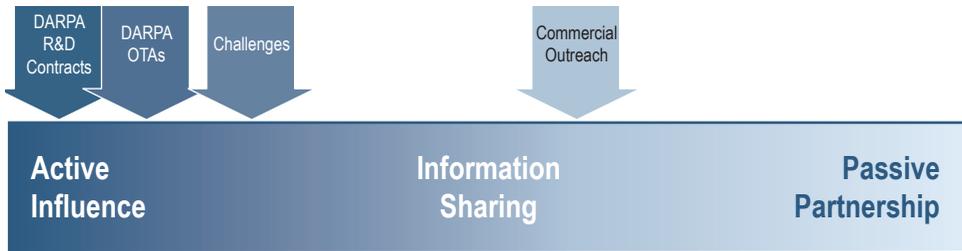
Information Sharing. Other partnerships do not rely on an exchange of funding or products. Instead, these partnerships are established to give the government access to information about important science and technology developments, and provide insights into the private-sector innovation ecosystem. In some cases this may be privileged information, but frequently just involves easy and recurring access to publicly available information that adds value to private-sector insights. This form of partnership is largely targeted at leveraging the investments the private sector makes in their own horizon-scanning activities. In parallel, the private sector benefits from greater insights into the mission needs of the government.

Passive Partnership. This type of partnership is much more speculative and is often only virtual. However, it represents tremendous opportunities for the government to leverage the scale of private-sector business intelligence and technology investment, albeit with some risk. As discussed above, companies and hyper-wealthy individuals are becoming increasingly active in collecting business-pertinent information and maintaining security and stability. When government interests align with private-sector motivations, small actions on the part of the government, such as an expression of interest by simply attending a public conference, can have a significant multiplier effect without any kind of formal relationship.

Examples of Public-private Partnerships to Leverage and Mitigate Strategic Latency

There are many, many examples of public-private partnerships (PPPs). We have chosen the following limited set of U.S. government partnerships in national-security technology development to illustrate the spectrum.

Defense Advanced Research Projects Agency (DARPA)



DARPA's creation was motivated by strategic latency. It was chartered in 1958 in response to the launch of the Sputnik satellite. The Eisenhower administration and the nation were shocked to discover the Soviet Union had beaten the U.S. into space, and established DARPA as a part of its response. DARPA's charter is to "maintain U.S. technological superiority over, and to prevent technological surprise by, its potential adversaries."¹¹

DARPA's FY15 budget was \$2.9 billion, most of which went into funding contracted research projects.¹² Funded activities range from very basic research to development of prototypes of major weapon systems, and they span almost every domain of science and technology. DARPA maintains no in-house research capabilities and relies on a wide range of companies, universities, and other institutions to carry out its work. In addition to traditional defense contractors, DARPA also funds many researchers in academia and in small startups, and there are frequent initiatives to attract non-traditional, private-sector performers.

A potential impediment to DARPA's focus on innovation is the Federal Acquisition Regulations (FAR). Under FAR, companies must abide by a many-volumes list of regulations and reporting requirements, including imposing significant restrictions on topics ranging

¹¹ "DARPA: Bridging The Gap, Powered By Ideas," *Defense Technical Information Center*, 2005.

¹² "Department of Defense Fiscal Year (FY) 2016 President's Budget Submission," *United States Special Operations Command*, February 2015, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2016/budget_justification/pdfs/03_RDT_and_E/RDTE_MasterJustificationBook_United_States_Special_Operations_Command_PB_2016.pdf.

from how the rates it charges customers are defined to executive compensation.¹³ Many of these restrictions come with additional reporting and auditing requirements. Complying with the FAR is a major barrier to non-traditional companies and institutions working with the government. Initial setup of FAR compliance can be burdensome and costly. It is a major distraction for companies whose primary business is commercial, and who are not planning to work closely with the government. More importantly many of the provisions can be detrimental to the company's baseline commercial business practices, driving companies not dedicated to government contracts as a primary business away from working with the government. Consequently, DARPA utilizes an array of creative funding mechanisms to encourage innovation among its partners. These include the following:

Other Transaction Authority (OTA). OTA is a government contracting mechanism to provide a more flexible way for the government to do business with non-traditional performers or pursue more innovative contractual relationships with traditional defense companies.¹⁴ OTA allows the government to enter into a more commercial-like contract with a company or other institution. The authority is targeted at making it easier for non-traditional companies to work with the government, or for traditional contractors to partner with the government in a way that provides cost-sharing.

While OTA was established in 1958 for NASA,¹⁵ DARPA was the first DOD agency to receive the authority and has historically been one of the bigger issuers of these types of contracts.

Prizes and challenges. Prizes and challenges are tools that help to incentivize private-sector cooperation and involvement. Government agencies have been given the authority to award cash prizes in recognition of breakthrough achievements in research and development and application of commercial technology relevant to U.S. government priorities.¹⁶ This authority applies across government agencies, and its use was encouraged by the Obama Administration¹⁷ to incentivize nontraditional companies, institutions, and even individuals to partner with the government.

Not only do these challenges reach nontraditional partners, but they do it in a manner that generates tremendous cost leverage. Unlike a traditional contract or grant, through which the government funds an institution to do work and produce a result, in a challenge

13 For an overview of the FAR and references to additional information, see "Contracting," *U.S. Small Business Administration*, accessed October 27, 2017, <https://www.sba.gov/contracting/contracting-officials/federal-acquisition-regulations-far>.

14 OTA is defined in law in 10 U.S.C. 2371 and Section 845 of the National Defense Authorization Act (NDAA). While the authority was created as a temporary provision with periodic renewal required, at the time of this writing, the draft NDAA of 2016 would make OTA permanent.

15 Elaine Halchin, "Other Transaction (OT) Authority (RL34760)," *CRS Report for Congress*, July 15, 2001, <https://fas.org/sgp/crs/misc/RL34760.pdf>.

16 U.S. Code Title 42, Chapter 149, Subchapter X, § 16396 – Prizes for achievement in grand challenges of science and technology.

17 https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-11.pdf, last accessed October 27, 2017.

the government specifies a goal and rules or guidelines within which to reach it. Other than infrastructure and staff to conduct challenge events, the government makes no up-front expenditures to develop solutions. All funding to develop solutions comes from private sources. Teams create their ideas on their own with no direction or oversight by the government. Then in accordance with the rules of the challenge, the participants compete to see who can meet or exceed the goals.

While not the only agency to take advantage of “challenge and prize” authority, DARPA has been a major sponsor of challenges. In 2004 the “DARPA Grand Challenge”¹⁸ gained public attention when the agency challenged teams to develop a driverless car that could traverse a mostly off-road 150-mile course from Barstow, CA to Primm, NV. Fifteen teams competed, but none completed the course, with the farthest vehicle making it just over 7 miles. However, this initial failure stimulated this community to keep working on the problem, and in 2005 the second driverless-car Grand Challenge became a breakthrough success. Of 23 vehicles that competed, five completed the course, the winner going over 130 miles in less than seven hours. The winner took home a \$2 million prize and perhaps more importantly, a place in history.¹⁹

Subsequently, DARPA has conducted a follow-on 2007 Urban Challenge²⁰ in which the self-driving cars had to complete a 60-mile urban course in less than six hours. DARPA challenges have moved beyond self-driving cars. The 2015 DARPA Robotics Challenge²¹ involved mostly humanoid robots that had to complete a series of eight tasks in a degraded, dangerous environment motivated by the Fukushima nuclear reactor disaster. Other DARPA challenges include the Network Challenge²² in 2009 that challenged teams to use social networking to find hidden red balloons scattered across the country. In 2015 the Chikungunya Challenge²³ required teams to find ways to predict the spread of a virus through the Western Hemisphere. In 2016 the agency held its Cyber Grand Challenge,²⁴ in which computers competed against each other as “hackers” in a computer-network Capture the Flag tournament in an event co-located with the DEF CON²⁵ hacker-community conference.

18 Marsha Walton, “Robots fail to complete Grand Challenge.” *Cable News Network LP, LLLP*, May 6, 2004, <http://www.cnn.com/2004/TECH/ptech/03/14/darpa.race/index.html>.

19 <http://archive.darpa.mil/grandchallenge05/>

20 <http://archive.darpa.mil/grandchallenge/>, last accessed October 27, 2017

21 <http://archive.darpa.mil/roboticschallenge/>

22 “DARPA Network Challenge Program Report,” February 16, 2010, last accessed October 27, 2017, <http://www.eecs.harvard.edu/cs286r/courses/fall10/papers/ProjectReport.pdf>.

23 “CHIKV Challenge Announces Winners, Progress toward Forecasting the Spread of Infectious Diseases,” DARPA, May 26, 2015 accessed October 27, 2017, <http://www.darpa.mil/news-events/2015-05-27>.

24 <http://archive.darpa.mil/cybergrandchallenge/>

25 “Homepage,” *DEF CON Communications, Inc.*, accessed October 27, 2017, <https://www.defcon.org/>.

DARPA's challenges have spurred untold development spending in challenge areas. There is a strong case to be made that the Grand Challenge spawned the entire self-driving car industry. The leader and some of the members of the winning Stanford team moved to Google to form the core of its self-driving car development unit.²⁶ Many of the sensors used by Grand Challenge cars have been commercialized and are appearing in currently available car models as part of driving-assist features.²⁷ More than anything else, the challenges have stimulated imagination and interest, and removed perceptual barriers that "it can't be done" with relatively small government investment.

Other commercial outreach. DARPA continues to search for new ways to reach out to the commercial technology ecosystem and nontraditional partners. This is largely motivated by the trends described at the beginning of this chapter, that the commercial sector is driving the lion's share of innovation and the pace of innovation is benefitting from globalization. In a strategic framework laid out in 2013, shortly after becoming DARPA Director, Dr. Arati Prabhakar stated, "This globalization has important implications for national security... The globalization of all aspects of technology...is an inevitable and in many ways even a healthy fact of modern life. Our challenge is to create an edge for U.S. national security purposes in this environment."²⁸ Clearly the agency has recognized the changing landscape of globalization. The challenge remains to continue the mission of achieving and avoiding technological surprise, now at the pace of commercial development.

To address this situation, DARPA is reaching out to non-traditional communities. As part of this outreach, in 2015 DARPA held its first major conference since 2007, entitled "Wait, What?"²⁹ Unlike its legacy DARPATech conferences, which focused on telling traditional industry what the agency had accomplished and was interested in for the future, "Wait, What?" brought together an eclectic mix of academics and technologists from across many disciplines and sectors. Presenters spoke more about advances happening outside the government, while exhibits and other interactive opportunities for attendees highlighted DARPA technologies and the importance of its national security mission. The goal was twofold: introduce government attendees to the many innovative people and ideas outside the traditional DOD ecosystem, while motivating the nontraditional attendees to take a greater interest in solving the problems of national security.³⁰

26 "On the Road," *Waymo*, <https://waymo.com/ontheroad/>.

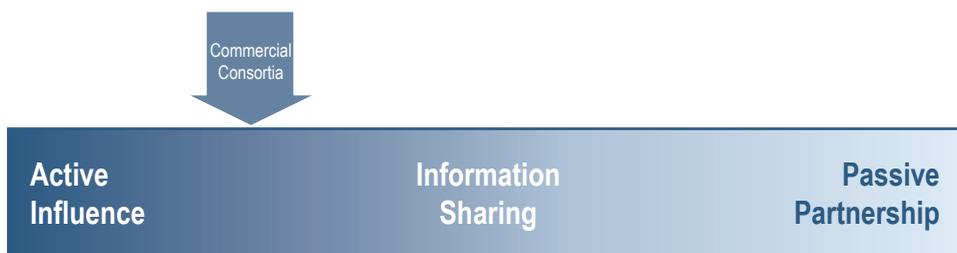
27 While many sensors inspired by the grand challenges have reached commercial markets, one of the most notable is the family of Velodyne LIDAR sensors. See Ray Renteria, "DARPA Urban Challenge Yields its first Commercial-Grade Innovation," *Robot Central*, October 12, 2007 accessed October 27, 2017, "<http://www.robotcentral.com/2007/10/12/darpa-urban-challenge-yields-its-first-commercial-grade-innovation/>."

28 "Driving Technological Surprise: DARPA's Mission in a Changing World," *DARPA*, April 4, 2013, <http://www.defenseinnovationmarketplace.mil/resources/DARPAstrategicPlan.pdf>

29 "Wait What? A Future Technology Forum," *Strategic Analysis, Inc.*, accessed October 27, 2017, <http://archive.darpa.mil/WaitWhat/>.

30 *Ibid.*, <http://archive.darpa.mil/WaitWhat/#about>.

Commercial Consortia



Driven by the broader DOD’s interest in access to non-traditional technology providers and flexible contracting mechanisms like OTAs, several public–private consortia efforts have sprung up. The consortia establish a highly flexible contract vehicle with a very broad scope to provide rapid funding access to members. Most of the early consortia are based upon themes around cybersecurity or open-systems architecture technology.

An example of one of the larger consortia contracts is the Consortium for Command, Control, and Communications in Cyberspace (C5).³¹ It was initiated in 2014 by a small group of individuals with deep experience with both the DOD and multiple small businesses and universities. The Army was looking for ways to accelerate development and acquisition of technology for the warfighter, especially in the rapidly evolving cyber domain. Army Contracting Command at Picatinny Arsenal had become the single largest sponsor of OTAs. Picatinny worked with the founders to establish the consortium and generate the OTA contract vehicle.³²

A C5 contract must involve some type of problem related to offensive or defensive cyberwarfare. Topic areas include system security, control systems, automation systems, hardware and software performance analysis, software and hardware sustainment, and emerging software and hardware technology. Any government sponsor with requirements fitting this scope can issue a “Request for Whitepapers” (RFW). These RFWs communicate challenges for the C5 collective membership to try to solve.³³ Membership in the consortium is open to any U.S. business, university, or other entity that is not a traditional DOD contractor and meets a few other selection criteria. If a member has an innovative solution to the challenge, it can very quickly get funding from the requirement sponsor via the C5 OTA.

31 “Homepage,” *Consortium for Command, Control and Communications in Cyberspace*, accessed October 27, 2017, <http://c5technologies.org/>.

32 *Ibid.*, <http://c5technologies.org/ota>

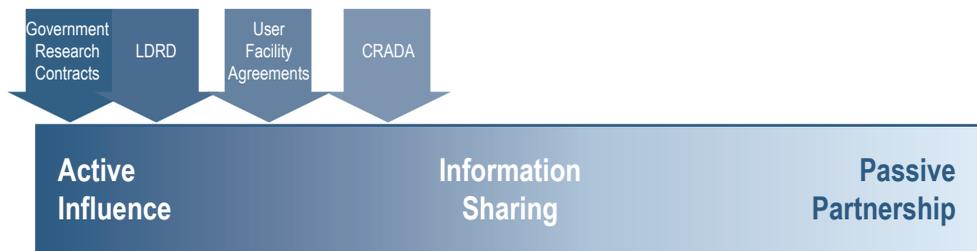
33 “Consortium for Command, Control, Communications and Computer Technologies (C5) OTA Overview,” ASAALT Industry Day, November 2015.

The C5 consortium has been involved in partnering and leveraging other private consortia. In 2011 a volunteer consortium called PlugFest was formed.³⁴ They put forward the “Haiti Storm” emergency-response challenge problem and conducted a live three-day hack-a-thon at the Armed Forces Communications and Electronics Association (AFCEA) C4ISR Symposium. While there was no promise of funding, PlugFest participants worked together to develop new software and communications applications that could aid in emergency relief operations, such as those conducted after the 2010 Haiti earthquake. Participants worked together to produce solutions solely for the satisfaction of developing a solution to a critical global security challenge, and the bragging rights of receiving an award for a particular effective solution. Since then, PlugFest continues as an all-volunteer non-profit consortium, but has motivated several parts of the DOD to sponsor their own PlugFest events.^{35,36}

The concepts of the all-volunteer consortium and the contract-centered C5 consortium came together in 2015 with the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)) Cyber Challenge.³⁷ The Army put together a problem statement for new approaches for automated cyber-risk monitoring. While they were ultimately soliciting new ideas to fund development through the C5 OTA contract, they used the PlugFest consortium to get the word out about this RFW to its non-traditional members and used a PlugFest event to refine its requirements and evaluate interesting potential concepts.

Department of Energy National Laboratories

The Department of Energy (DOE) National Laboratories offer another model for U.S. government access to cutting-edge commercial developments, and vice versa. The National



34 “From the Organization that started Government PlugFests...,” *plugfestplus.org*, accessed October 27, 2017, <http://www.plugfestplus.org/plugfest-plus-history>.

35 One of the largest of these other government PlugFests is organized by the Defense Intelligence Information Enterprise. See <http://di2eplugfest.org/>.

36 See also industry groups, such as AFCEA. See <http://www.afcea.org/events/west/15/plugfest.asp>, last accessed October 27, 2017.

37 “News,” *Consortium for Command, Control and Communications in Cyberspace*, accessed October 27, 2017, <http://c5technologies.org/news>.

Laboratories system finds its origin in the scientific endeavors of WWII, particularly the Manhattan Project.³⁸ There are 16 DOE National Laboratories, which operate as government-owned, contractor-operated entities (GOCO). Each National Laboratory has an integral connection to the private sector and/or academia. The underpinning mission of each National Laboratory is reflective of the following sponsoring offices within the DOE, as follows:³⁹

- Office of Science
- National Nuclear Security Administration (a semi-autonomous agency within the DOE)
- Office of Fossil Energy
- Office of Energy Efficiency and Renewable Energy
- Office of Nuclear Energy, Science and Technology
- Office of Environmental Management

The research and development efforts of the National Laboratories fall into four basic funding categories.

Government Research Contracts. The lion's share of each laboratory's support comes from the respective primary mission office, resulting in a rich infrastructure of technical talent, capabilities, and facilities focused on specific national defense and energy security needs. However, each laboratory also competes for other government-sponsored research, sometimes teaming with the private sector and academia. This results in a further expansion of the breadth and depth of the research infrastructure.

Laboratory Directed Research and Development (LDRD). In 1992, Congress authorized the National Laboratories to initiate the Laboratory Directed Research and Development program.⁴⁰ Funded with approximately six percent of a Laboratory's budget, it represents a prestigious source of research and development funding awarded through a rigorous and highly competitive internal review process. As the sole source of discretionary funding, LDRD resources are invested in high-risk, high-payoff activities that build technical capabilities and develop strategic initiatives to meet future mission needs. Consequently, many of the DOE's most exciting innovations can be traced to LDRD investment. In many laboratories, the technical output of LDRD researchers, measured in patent disclosures, peer-reviewed publications, and publications cited by other authors, typically accounts for one quarter of the laboratory's total. Thus, LDRD is often the catalyst for the most promising private sector engagements.

38 Peter Westwick, *The National Labs: Science in an American System, 1947–1974* (Cambridge, MA: Harvard University Press, 2003).

39 "National Laboratories," *U.S. Department of Energy*, <http://energy.gov/about-national-labs>.

40 "Laboratory Directed Research & Development," *Los Alamos National Laboratory*, 2017 accessed October 27, 2017, <http://www.lanl.gov/science-innovation/science-programs/ldr/index.php>.

User Facility Agreements. Throughout the National Laboratory system, the DOE has also created an extensive suite of user facilities to provide researchers with the most advanced tools of modern science.⁴¹ The facilities encompass accelerators, colliders, supercomputers, light sources, and neutron sources, as well as unique capabilities for studying the nanoworld, the environment, and the atmosphere. The facilities are open to all interested potential users, without regard to nationality or institutional affiliation. The allocation of the facility's resources is determined by merit review of the proposed work, and research is executed via user facility agreements.

User fees are not charged for non-proprietary work if the user intends to publish the research results in the open literature. Full cost recovery is required for proprietary work and the facilities do not compete with an available private-sector capability. The user facilities support formal user organizations to represent the users and facilitate the sharing of information, forming collaborations, and organizing research efforts among users. Thus, the National Laboratories are able to partner with the private sector on fundamental science, and the private sector can even invest in proprietary research or collaborate in what is often pre-competitive research.

Cooperative Research and Development Agreements (CRADAs). CRADAs were created in 1986, and at the time focused on commercializing federal lab-developed technology.⁴² The goal was to provide non-government entities (private for-profit companies, universities, and other nonprofits) a means of partnering with the labs and making use of technology and unique facilities for dual-use purposes. The catalyst for the creation of the CRADA mechanism was the changing mission of the nuclear defense laboratories as demands for nuclear weapons research were fading. Since then, CRADAs have evolved to become full two-way partnerships between government and the private sector, and are available across all parts of government.⁴³

Like contracts, they are legally binding agreements between the government and the private entity, but that is where the similarities end. The government does not provide any funding under a CRADA, so federal contracting regulations do not apply. What it does provide is a vehicle to make government information and property available to the private partner. This could mean licenses to research conducted by the lab or access to unique equipment such as a supercomputing facility or synchrotron. It could also involve sharing otherwise unavailable government information useful for the private partner's research, such as intelligence data, and even sponsor security clearances.

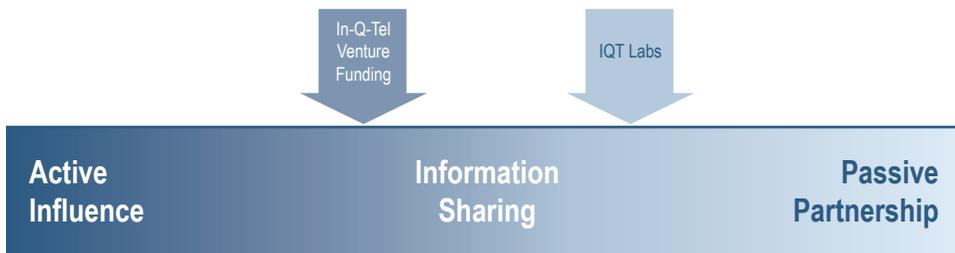
41 "User Facilities," *U.S. Department of Energy Office of Science*, January 5, 2017 accessed October 27, 2017, <http://science.energy.gov/user-facilities/>.

42 Federal Technology Transfer Act of 1986, P.L. 99-502 (1986).

43 See for example how Sandia National Laboratory is managing its CRADA partnerships at http://www.sandia.gov/working_with_sandia/agreements/crada/index.html, last accessed October 27, 2017.

In turn, the private entity performs research of relevance to the government using its own funds (or those of some other third-party source). The private entity can even fund the government under a CRADA, such as paying a user fee to access the specialty facility. The private entity owns the intellectual property rights to any products or information resulting from the CRADA research, but the government partner gets unlimited use of the intellectual property at no cost.⁴⁴

In-Q-Tel



The late 1990s brought great change to the Central Intelligence Agency (CIA) and especially to its Directorate of Science and Technology (DST). The end of the Cold War brought about significant budget reductions and questions about the Agency’s mission. At the same time, the World Wide Web had recently brought the internet into public awareness and was about to spawn the “Dot-Com” boom of commercial information technology development. These combined trends led to a realization that perhaps the private sector could be leveraged to address some of the intelligence community’s (IC) technology needs. Thus In-Q-Tel was created.

In-Q-Tel was chartered by the CIA in 1999 as a private, independent, non-profit corporation.⁴⁵ It was nominally a venture capital (VC) company dedicated to investing in start-up businesses with technology that can benefit the IC, but it has evolved to be much more. While it has been very successful as a VC investor and in providing new technology opportunities to the CIA, its greater value has perhaps been the opportunity for information exchange. Even in its purest role as a VC firm, In-Q-Tel provides the government unprecedented access to other VC investors, as well as major business leaders in the entrepreneurial community. In addition, In-Q-Tel has recently created new functions

⁴⁴ For example, see “CRADA Cooperative Research and Development Agreements,” *Sandia National Laboratories*, 2016 accessed October 27, 2017, http://www.sandia.gov/working_with_sandia/agreements/crada/_assets/documents/External%20CRADA%20Brochure%202016.pdf.

⁴⁵ Rick Yannuzzi, “In-Q-Tel: A New Partnership Between the CIA and the Private Sector.” *Central Intelligence Agency*, 2007, <https://www.cia.gov/library/publications/intelligence-history/in-q-tel>.

beyond its VC investment role that will be discussed below, and these provide even greater opportunities for information exchange.⁴⁶

While chartered by the government and receiving government funding, In-Q-Tel is not a government organization. It is staffed by non-government employees and can make all of its investment and business-operations decisions independently of the government and traditional government personnel and acquisition regulations. It evaluates investments based upon traditional VC criteria associated with business viability and potential return on investment, and only pursues companies driven by commercial success. Unlike traditional VC firms, In-Q-Tel also evaluates investments based upon potential value of a portfolio company's technology to the IC. Currently that value is categorized in four "Practice Areas": Advanced Analytics, Field Deployable Tech, Infrastructure and Security, and Mobility.⁴⁷

To aid in identifying value to the IC, there is a counterpart organization within the CIA called the In-Q-Tel Interface Center (QIC). QIC is staffed by cleared CIA government employees. They have access to operational elements of the CIA and other agencies and aggregate their classified operational needs into unclassified problem sets. Not only does this provide criteria by which to assess IC value of potential investments, it also helps communicate the IC's most pressing problems to portfolio companies and the broader technology community. Recently In-Q-Tel has been broadening its partnerships beyond the CIA. It is now truly a multi-agency resource, and in the process of working with In-Q-Tel, these agencies often start their own dialogs and collaboration across the traditional government "silos."⁴⁸

While In-Q-Tel typically invests a smaller fraction in a company than a conventional VC firm would, it draws a disproportionate degree of interest and co-investment from other companies in the VC community. This is because of the level of due diligence In-Q-Tel can conduct compared with a traditional VC firm.⁴⁹ Its appropriated budget line for internal operations supports a much larger staff with more technical depth, so that if In-Q-Tel decides to invest in a company, it draws a significantly greater co-investment. Its challenge problems also potentially become objectives for other nontraditional companies motivated to work on national security issues. All of this communication potential is capped off by an annual In-Q-Tel CEO summit that brings together business leaders from across the technology sector with government national security leaders.

As In-Q-Tel's mission and approach have evolved, it has taken a more aggressive role both in incubating specific solutions to IC problems and in expanding outreach and information-sharing opportunities. This has occurred through the creation of IQT Labs.⁵⁰ The labs create

46 "Homepage," *In-Q-Tel, Inc.*, last accessed October 27, 2017, <https://www.iqt.org/labs/>.

47 *In-Q-Tel, Inc.*, 2017, <https://www.iqt.org/technology-focus/>.

48 See the "Partners" tab at <https://www.iqt.org/about-iqt/>, last accessed October 27, 2017.

49 *In-Q-Tel, Inc.*, 2017, <https://www.iqt.org/about-iqt/>.

50 *In-Q-Tel, Inc.*, 2017, <https://www.iqt.org/labs/>.

opportunities for in-house In-Q-Tel technical staff and government researchers to partner with nontraditional institutions and researchers. Work performed in the labs is intended to transition both into the government and back into the private sector. Lab staff accumulate insights on global technology trends garnered from these research projects and publish them in openly distributed quarterly journals.⁵¹

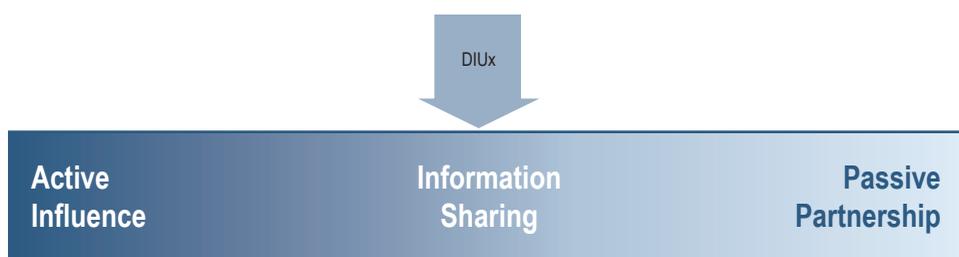
At the time of this writing there were four IQT Lab initiatives:⁵²

- **BiologyNext** is focused on how life sciences impact national security. Particular trends they are investigating at the time of this writing include novel materials, sensors, laboratory automation, big data analytics, and genome editing.
- **CosmiQ Works** is focused on new trends in commercial space technology. Their current key investigation areas are satellite data analytics, communications and payloads for small satellites, mission management, and content delivery. They have a very novel partnership approach to initiating projects that solicits project ideas, participation, and co-funding from the private sector.
- **Cyber Reboot** is based upon the premise that despite the very large amount of public- and private-sector resources being spent on cybersecurity, the number of successful cyberattacks is increasing. Their research focuses on cybersecurity doctrine, awareness, and attribution to be able to impose cost on attackers.
- **Lab41** is conducting research in big data analytics while itself being an experiment in collaboration. It is located in Silicon Valley and has a unique 5-step process to conducting its projects. While criteria for a good problem are defined by government customers, problem recommendations can come from anywhere, including private-sector partners. Once a problem is identified, they do research to find the leading experts in related areas. They reach out to these experts and build a solution team and plan. A diverse team can then be formed to develop solutions to the challenge problem. All resulting software is treated as open source and published on GitHub. Results of the research are advertised around relevant communities via publications, sponsored events, and other presentations.

51 Each focus area publishes its quarterly journals on their web site. See <https://www.iqt.org/technology-focus/>, and look for specific topics under the respective focus area.

52 *In-Q-Tel, Inc.*, 2017, <https://www.iqt.org/labs/>.

Defense Innovation Unit Experimental (DIUx)



DIUx was chartered in 2015 as a personal initiative of Secretary of Defense Ashton Carter, with the objective of tapping more private-sector innovation to solve the DOD's most pressing challenges. Based upon the premise that innovators cluster in geographic regions such as Silicon Valley, DIUx established a DOD presence in the heart of the advanced technology industry, with new hubs opening in Boston and Austin.⁵³ The initial objective was communication and information sharing, building relationships, communicating DOD challenges, and scouting for possible new game-changing technology. However, that may be changing. A major reorganization after its first year, which is described further below, appears to place more emphasis on funding startups than information sharing.

While DIUx is still a relatively new organization, it is dynamic and is adapting to its environment. In May 2016 DIUx underwent a "reset" in terms of a leadership change and shifted its business model.⁵⁴ (This self-awareness and ability to restructure so quickly is by itself very non-traditional for DOD.) The reset was initiated to improve responsiveness and the focus on innovation. In about three months after the reset, DIUx had completed one acquisition cycle called a Commercial Solution Opening (CSO), and was getting a second CSO in place. The goal is to have one CSO per month. Their fundamental objective is to accelerate commercial technology into the hands of the warfighter by funding projects that can adapt privately funded technology into products more suited for military applications and subsequent traditional acquisition.⁵⁵

A CSO is executed in several steps. It begins by posting a list of DOD problems that DIUx staff have collected from DOD warfighters and other DOD organizations. Problems are written very generically to provide significant latitude for innovative solutions. Interested companies can respond via the website with simple statements of capabilities they think might be relevant to one of the problems. Then a very non-traditional step occurs. The

53 Terri Moon Cronk, "Pentagon, DIUx Officials Discuss DoD, Industry Innovation," *DoD News*, <http://www.defense.gov/News/Article/Article/612750>.

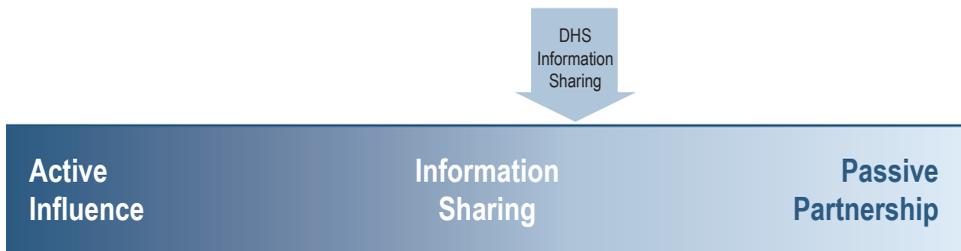
54 Ash Carter, "Remarks Announcing DIUx 2.0," (speech. Mountain View, California, May 11, 2016), accessed October 27, 2017, <http://www.defense.gov/News/Speeches/Speech-View/Article/757539/remarks-announcing-diu-x-20>.

55 Col. Steven J. Butow. Interview by author. July 14, 2016.

company is invited for an in-person meeting to discuss its idea with a DIUx employee in an open dialog to shape a potential project. The company gets to understand the DOD problem in more depth, and DIUx can learn more about the company’s commercial interests. Based on the discussion, the company may be asked to submit a proposal, but the nature of what exactly is requested by the government is mutually shaped by the dialog. If the proposal is then selected for funding, a flexible contract is issued under OTA.⁵⁶

One remaining significant challenge is getting technology funded by DIUx back into traditional DOD acquisition pathways. Part of this will be facilitated by the two-way communication and awareness DIUx attempts to provide, but it is also attempting to leverage a key provision of OTA to encourage traditional DOD organizations to join the partnership. Any commercial prototypes funded by an OTA can then be acquired subsequently via a sole-source contract. This in principle removes a major barrier to traditional DOD organizations’ adoption of DIUx-sponsored technology.⁵⁷ It is too early to tell if the DIUx model for technology acquisition will find broad acceptance and be sustainable, especially in light of political and budget changes that may reduce incentives for innovative approaches.

Department of Homeland Security (DHS) Information Sharing



Perhaps the greatest current threat to the United States and the well-being of society (shy of nuclear weapons) is protection of the nation’s critical infrastructure.⁵⁸ The responsibility for protecting this critical information falls on the Department of Homeland Security (DHS). DHS faces a different challenge compared with the defense mission of the military, in that the infrastructure it is protecting is almost all owned and operated by the private sector. As a result, DHS has little direct means of implementing any critical infrastructure protection

⁵⁶ Ibid.

⁵⁷ National Defense Authorization Act of 2016, Section 815, U.S. Congress and several interpretation white papers. See for example http://www.transform.af.mil/Portals/18/documents/OSA/OTA_Brief_Ver%206Apr2016.pdf, last accessed October 27, 2017.

⁵⁸ “Critical Infrastructure” sectors include Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors and Material, Sector-Specific Agencies, Transportation, and Water and Wastewater. See <https://www.dhs.gov/critical-infrastructure-sectors>, accessed October 27, 2017.

(CIP) solutions it develops, be they integration of new technologies or adoption of new practices. In extreme cases they can seek regulatory action, but for most situations, DHS must take a much more collaborative approach that is accepted by the private sector.

At the core of this collaborative approach is a strong dedication to information sharing. DHS strives to create opportunities for a multi-lateral flow of information from private-sector companies to the government, the government to companies, and between companies. The sharing goals are broad, ranging from near-real time dissemination of attack indications and warning, to general threat and vulnerability analysis, to new tools and best practices.⁵⁹

This type of public-private information sharing is extremely sensitive and requires the utmost care to protect all stakeholders' equities. From the government's perspective, much of its information may involve classified data derived from sensitive and fragile sources and methods. The industry partners arguably have as much or even more at stake. First, there is the basic proprietary nature of their information. How they discover and define threats and vulnerabilities may disclose quite a bit about highly proprietary aspects of their business, ranging from infrastructure design to business practices. If the government were to divulge proprietary data of this nature to competitors, it could result in grave financial losses to the industry partner. Even public statements about threats or vulnerabilities can affect market value.

Perhaps an even greater risk relates to liability. As soon as a company acknowledges a vulnerability, it is potentially culpable for damages that result. If acknowledgement of vulnerabilities, or worse, actual damages, became public, it could be financially catastrophic to a company, due to invalidated insurance claims, potential lawsuits, and basic damage to brand identity. As such, a company accepts significant risk by sharing information with the government. DHS, backed up by new laws and executive orders, strives to respect these risks by taking the utmost care to manage and protect industry data.⁶⁰

To carry out its information-sharing objectives, DHS has established a range of information-sharing programs. In each case DHS is providing a forum to collect and aggregate information provided by both government and industry and provides the finished products back out to all stakeholders.

- **Cyber Information Sharing and Collaboration Program (CISCP).**⁶¹ At the heart of DHS information sharing is the CISCP. It is the central information hub for all information about threats and mitigations. Their products range from warnings of immediate

59 "Information Sharing," *Department of Homeland Security*, accessed October 27, 2017, <https://www.dhs.gov/topic/cybersecurity-information-sharing>.

60 Established under the Critical Infrastructure Information Act of 2002 and the amendment in Final Rule 6 C.F.R. Part 29. See <https://www.dhs.gov/pcii-program>, accessed October 27, 2017.

61 "Cyber Information Sharing and Collaboration Program (CISCP)," *Department of Homeland Security*, accessed October 27, 2017, <https://www.dhs.gov/ciscp>.

threats to more general analysis. Indicator Bulletins and Priority Alerts provide warning to immediate threats, and update threat and vulnerability definitions in formats readable by both humans and machines, the latter to facilitate automated monitoring. Analysis reports and recommended practices provide more general analyses of threats and vulnerabilities, and best practices for securing against them, respectively.

- **National Cybersecurity and Communications Integration Center (NCCIC).**⁶² The NCCIC is the nerve center for information sharing, where the government's and industry's immediate threat data are aggregated and alerts disseminated. They provide real-time situation awareness and warning of threats and incidents while they happen, as well as recommended mitigation.
- **Protected Critical Infrastructure Information Program (PCII).**⁶³ As acknowledgement of the sensitivity of shared information, DHS has established the PCII program. When an industry partner declares an element of information PCII, it is protected from Freedom of Information Act (FOIA) disclosures, as well as certain types of civil and regulatory litigation. It complements the other information-sharing programs by removing the disincentives to sharing.
- **Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs).**^{64,65} ISACs and ISAOs are private, nonprofit organizations focused on providing the information-sharing environment for CIP. In some ways they are similar to In-Q-Tel, in that they are private-sector organizations existing for the express purpose of being a bridge between government and private industry. ISACs are sector-specific and are formed by their constituent owner-operators. Each sector's ISAC is slightly different and tailored to that sector, but their roles range from more general information sharing, like the CISCP, to more real-time situation awareness, like the NCCIC. ISAOs are the newest information-sharing construct, developed in response to the President's 2015 Executive Order 13691. In contrast to ISACs, they are not sector-specific, but instead can be thought of as providing information-sharing infrastructure and enablers. They provide a forum for private-sector members to receive security clearances that will give them more access to sensitive government data. They ensure members a conduit to the NCCIC. In addition, to promote wider use of the rest of DHS' CIP tools and data, they are developing a series of information-sharing data standards. Not only will this facilitate better machine-to-machine passing of data and automated execution, it will also ensure better human-to-human

62 Ibid., <https://www.dhs.gov/national-cybersecurity-and-communications-integration-center>.

63 Ibid., <https://www.dhs.gov/pcii-program>.

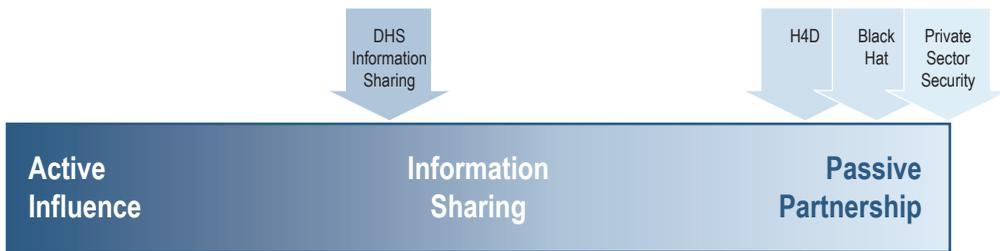
64 Exec. Order No. 13691, 3 C.F.R. 80 FR 9349 (2015). <https://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf>.

65 "Information Sharing and Analysis Organizations (ISAOs)," Department of Homeland Security, accessed October 27, 2017, <https://www.dhs.gov/isao>.

communication, helping to prevent misunderstandings resulting from different lexicons.

One may note that most of these DHS information-sharing programs are much more tactical in nature than operating at the level of a strategic challenge. However, they are important in that they provide a model for engagement, information sharing, and the infrastructure to pass and disseminate this information securely. For our purposes, and taking into account the foreign hacking of public and private U.S. entities, like the Russian hacking of the Democratic National Committee, the DHS information-sharing efforts provide insights into the cyber aspects of strategic latency.

Passive Partnership



Passive Partnerships are characterized by having no or very limited direct involvement by the U.S. government. They rely on private institutions and individuals taking actions on their own accord to make the world a safer place. This could be as innocuous as a private entity hosting a public conference on a topic of interest to the U.S. government. It could also involve development of security-relevant technology without government requirements or funding, but could extend to private-sector entities conducting their own intelligence and security operations, traditionally thought of as the purview of nation-states. Business intelligence is a multi-billion-dollar business that companies depend on to remain competitive. It typically focuses on country and regional security conditions, political trends, and market conditions.

Private-sector security endeavors can be very effective. They can leverage the tremendous monetary and human-capital resources available to the private sector, and they operate with agility outside the constraints of the system. As long as someone sees enough value to allocate capital, they can move forward on a project. Furthermore, companies can focus on specific issues that impact them directly, whereas the government has the responsibility to cover scores of issues spanning the entire globe. Private intelligence services, whether they are in-house or contracted by companies, have much to offer the U.S. government.

In the following we explore four examples of passive partnerships: a non-traditional product development company, a private academic initiative trying to make the traditional security enterprise better, truly independent private-sector security operations, and a public conference on computer security. We want to know how the government can leverage these types of organizations and endeavors. Are there opportunities to benefit from the work being performed by these organizations, perhaps even shaping their actions in ways that help the government, without any direct government funding and no or only limited communication?

Palantir. A well-known Silicon Valley company, Palantir is a thought-provoking example of how a very small In-Q-Tel investment contributed to the success of an entity that can now be described as a passive partnership, namely where the government can still benefit but with no additional direct involvement. Palantir was founded in 2004 on the belief that a non-traditional approach to intelligence analysis could solve critical national-security problems while making a good profit. A group of researchers who had worked together at PayPal realized that there were new technologies emerging that could enable very agile analysis of a wide range of heterogeneous data to solve daunting intelligence problems. They later branched out to apply the same types of tools to different but related problems in financial analysis.

Backed by the significant resources of co-founder Peter Thiel and a small investment by In-Q-Tel, Palantir was able to create tools to analyze a diverse mix of structured and unstructured data. They focused as much on the platform, the analyst experience, and the ability to collaborate as they did on the actual analysis algorithms themselves. Rather than waiting for the next government Request for Proposals, they self-funded their development work, motivated by their three guiding principles: “The best idea wins,” “Nothing is permanent,” and “Keep focused on the mission.” Once they completed initially usable products, they then sold them back to the government as finished products for intelligence analysts to use in combination with other sources of information.

While the bulk of the investment was private money, the very small In-Q-Tel investment was critical to their success, as it provided the opportunity for the U.S. government to shape the mission focus. In-Q-Tel was able to provide Palantir with relevant problems to guide their development work. Thus, they were able to design products with the speed and agility enabled by private funding, but with the relevance of a traditional government acquisition. They also had the insight that the same types of analysis needs faced by the IC could also be relevant in other sectors. In the years since their original software was sold to the government, they have made a major push into the financial sector and other markets with similar large-data information-analysis needs. The profit they make in these other markets adds to the company’s bottom line and in turn helps to finance additional development of national security products.

Hacking for Defense (H4D). H4D, subtitled “Solving National Security Issues with the Lean Launchpad,” started as a class run out of Stanford University that challenged students to

solve national security challenges using the start-up world's best innovation practices.⁶⁶ H4D is the brainchild of Steve Blank, a serial entrepreneur who also had significant IC experience. Motivated by concern that the government acquisition process and culture cannot keep pace with dynamic global threats, he partnered with retired Army Colonel Peter Newell (who as his last active duty assignment led the Army's Rapid Equipping Force) to create the H4D class as a platform to leverage bright minds to solve security challenges while developing new business ideas.

H4D projects begin with self-forming, voluntary teams composed of both Stanford students and outside volunteers. They are given security and intelligence-challenge problems identified by other volunteers and partners with a national security background, and are then set loose to develop solutions in the form of a product or service that has the potential to become a new business. Throughout the duration of the term, the teams refine their ideas with feedback from course leadership and mentors. As the course progresses, they collectively determine if the idea is an actionable business, and if so, identify tangible steps to get it started.⁶⁷

H4D is the ultimate hybrid of a passive-active partnership. It was started and run by a group of national security professionals with prior government or military experience. It also gets some level of non-material support from National Defense University and the Department of Energy. At the same time, it was founded by an individual's own initiative and is completely independent of government control. It attempts to address national security issues but ultimately with the goal of creating for-profit business opportunities.

Private Sector Security Services. As discussed in the opening section of this chapter, many major global corporations are beginning to look like nation-states when it comes to security and intelligence. Some have capabilities approaching those of a small- to medium-size nation-state, and are distributed around the globe in areas of potential risk and opportunity. In addition to the threat posed by regional instability, companies face counterintelligence threats from economic/industrial espionage and possibly even sabotage.

Multinationals have several advantages over the government when it comes to finding solutions to these challenges. First is their independence. Within the legal limits of business, they can develop any solution that might address their risks without the need for any type of approval or policy review. Perhaps more important, they can focus solely on their own interests. The U.S. government national security apparatus must pay attention to any potential threat to national interests anywhere in the world, and must allocate tremendous resources and effort against the most serious threats. Companies, on the other hand, can focus exclusively on locations that affect their immediate business interests, and they are free to ignore the rest of the world. This enables them to concentrate their resources on

66 "Hacking for Defense: Solving National Security Issues with the Lean Launchpad," *Stanford University*, accessed October 27, 2017, <http://hacking4defense.stanford.edu/>.

67 Pete Newell. Interview by author. July 13, 2016.

what matters most. They often have greater opportunity to collect information and conduct security operations, especially when their business operations are located in areas of greatest salience.

Private security operations span a wide range of topics. Two major priorities are traditional physical security services and cybersecurity. Offices, production plants, and other capital resources must be physically protected from industrial espionage, disruption, and sabotage by a variety of perpetrators, including activists, protestors and political opponents. If the facilities are located in unstable regions of the world, physical security risks may come from warring factions, necessitating security measures with almost military-like capabilities. Physical security measures include perimeter security, access control, surveillance, and security forces ranging from guards to mercenary forces. Certain firms specialize in these aspects of private security, often hiring retired Special Forces experts.⁶⁸ Cybersecurity of course involves protection of a company's computers, networks, and other information systems.

In between these two classes of security are emerging threats associated with hybrid or technical-physical security. The scope of these threats can be very broad, but in general, involve threats to a company's interests that are technical in nature, going after a company's information and automation services. However, the attack occurs through various types of physical access rather than software over a network. Examples of hybrid threats include risks from publicly available clandestine audio and video surveillance systems, software-defined radiofrequency (RF) surveillance, hardware embeds in computers and other electronic equipment, and a wide variety of supply-chain attacks. Across all of these is the risk posed by the insider threat, who can steal information directly or enable one of these other hybrid attacks.

Corporations are responding to these threats by taking matters into their own hands. Depending on the laws of the countries in which they operate, they may not have much legal recourse in response to different types of attacks. If they are able to pursue litigation, it is likely they would not be able to recover damages incurred by liability or repair brand impact from acknowledging the problem. In some jurisdictions, there may be legal (or at least not illegal) options for companies to employ active defenses, in which they go on the offense to deter or counter the threat actors. These measures may be performed entirely in-house by sophisticated security departments or outsourced to specialized security firms, likely staffed by former government intelligence and military professionals. In either case, there is a wide array of highly capable enabling technologies openly available on the commercial market to support security operations.

As an example, consider the operations of Royal Dutch Shell, one of the world's largest oil companies, in Nigeria. Shell is estimated to have about 100 staff for its Eja oil field,

68 "30 Most Powerful Private Security Companies in the World," *Security Degree Hub*, accessed October 27, 2017, <http://www.securitydegreehub.com/30-most-powerful-private-security-companies-in-the-world/>.

valued at over a billion U.S. dollars and producing approximately 300,000 barrels of oil per day.⁶⁹ As this region of Nigeria has become threatened by militant groups, its oil production has been impacted. While the U.S. government is certainly interested in any global unrest, it cannot afford to dedicate significant federal resources to Nigeria, compared with other global priorities. Shell, on the other hand, is not only highly motivated to have good intelligence about the Niger Delta, it also has point of presence that provides good intelligence-collection opportunities. Shell has a very sophisticated corporate security department to conduct these security and intelligence operations, and is reported to contract out additional support to high-end private security firms.

Black Hat. Black Hat is a computer security conference that was founded in 1997 by Jeff Moss, who also founded the DEF CON hacker conferences.⁷⁰ It started as an annual conference in Las Vegas, Nevada and now also takes place regularly in Barcelona, Amsterdam, and Abu Dhabi.

Black Hat brings together a variety of people interested in information security, ranging from non-technical individuals, executives, hackers, and industry-leading security professionals. The conference is composed of two major sections, the Black Hat Briefings and Black Hat Trainings. Training is offered by various computer security vendors and individual security professionals. The conference has hosted the National Security Agency's information-assurance manager course and various courses by Cisco Systems, Offensive Security, and others.

The Briefings are composed of tracks covering various topics, including: reverse engineering, identity and privacy, and hacking. The briefings also contain keynote speeches from leading voices in the information security field, including Robert Lentz, Chief Security Officer, United States Department of Defense; Amit Yoran, former Director of the National Cyber Security Division of the Department of Homeland Security; and General Keith B. Alexander, former Director of the National Security Agency and former commander of the United States Cyber Command.

The U.S. government benefits from the venue offered by Black Hat to convey its message and even provide training. In addition, U.S. government participants are able to view and even play with the latest technology developed by the private sector.

Our point in this section is that these private security operations, academic security operations, and computer security conferences are inherently suited to serve as passive partnerships, or force multipliers for U.S. government to understand and counter hostile uses of technology against the U.S. There are other models, such as the Self-Regulating Communities advocated by Jennifer Snow elsewhere in this volume. In terms of U.S. efforts

69 Sarah Kent, "Shell Evacuates Non-Essential Staff From Nigeria Field," *Wall Street Journal*, May 9, 2016 accessed October 27, 2017, <http://www.wsj.com/articles/shell-evacuates-non-essential-staff-from-nigeria-field-1462805125>.

70 https://en.wikipedia.org/wiki/Black_Hat_Briefings, last accessed October 27, 2017.

to prevent strategic surprise, we advocate a comprehensive approach that makes use of these hybrid entities.

PPP Outcome—What Works?

Across the initiatives and opportunities discussed previously, there have been some successful public–private partnerships. We highlight some important lessons learned from these partnerships below.

Private-sector interest and attention. Efforts of the government to stimulate private-sector interest and attention are clearly making an impact. Despite some of the recent distrust of the government after situations like the Snowden revelations, private-sector companies still care about national security. Whether it is out of a sense of duty and patriotism or simply self-serving profit motives, the private sector wants to work on security and intelligence problems. Grand Challenges, conferences, and stand-up of government organizations like DIUx have received strong, positive media attention. In addition, although the government can be a difficult customer, no profit-driven business can ignore the size of the government marketplace into which to sell products.

Value of information sharing and access. While the general public is still nervous about government information sharing and potential impingement on privacy, businesses are generally supportive of the government’s information-sharing programs. In fact, programs such as DHS’ ISACs and ISAOs are not only accepted, but welcomed. There are two key characteristics that make for a valued information-sharing program: two-way communications and indemnification. Private-sector companies want to make sure they can benefit from the exchange to protect their own systems. The indemnification that comes with the information sharing even helps protect them from other liability concerns, making it less risky for them to take unilateral security action.

Leverage private capital. Organizations like In-Q-Tel have shown the leverage that small investments by the government can have on private capital. Private investment values the depth of due diligence and technical expertise the government is able to bring. When the government signals a problem is important through its investment actions, it sends a demand signal to industry that this is potentially a marketable company or capability. And despite the government reputation for being plodding and risk-averse, in many cases it actually has the ability to take greater technical risks. The DARPA Grand Challenge is a good example of this. The Grand Challenge provided an existence proof that self-driving cars could traverse long, complex courses. Once this barrier of doubt was removed, an outpouring of private investment in self-driving cars occurred.

The value of mission focus. Enterprising private-sector companies draw great value from understanding customer problems, so they can develop products with a mission focus. For example, consumer companies may spend millions of dollars on market research. The various PPPs described here provide mechanisms for providing that kind of market-

demand information at no cost to the private company. Given this information in the form of an understanding of mission need, but free from a formal requirements process, an enterprising company can use its own innovative process to develop solutions that it can sell back to the government as catalog products. The company wins with a well-defined market, and the government wins with access to new capability.

Incubation of small businesses. The government has been effective at attracting innovation through small businesses. Many small companies would rather attempt to win government funding for their initial product development than dilute their ownership with private capital. This trend has been bolstered by flexible contracting vehicles and consortia such as C5 that make the government contracting process easier. More importantly, it allows the small businesses to retain their intellectual property.

PPP Outcomes—What Has Not Worked?

Despite some of the successes of PPPs, many challenges remain. Numerous programs that have achieved modest successes are still considered to be ineffective, not because of any fault of their execution, but often from the government's inability to capitalize on the successes. This is particularly the case in cutting-edge areas of research where strategic latency occurs. Here are some of the challenges.

Private sector interest only on their own terms. For all the reasons highlighted previously for private-sector interest in working with the government, companies only want to do so on their own terms. Ideally this involves an upside opportunity for them, but, at the very least, must not add risk to their business. Two of their biggest concerns tend to be around protection of intellectual property and impact to their core business by being slowed down by government. Intellectual property is a company's equivalent to top-secret compartmented information, but the government often does not treat it as carefully as it does classified information. And the biggest potential risk to a company's core business operations comes from speed. A fast-moving private sector company may potentially go through a product cycle or more in the time it takes the government to let a contract. Any delays introduced in a company's ability to execute can severely impact profits and revenues.

Government uptake barriers. Despite having significant ability to leverage companies toward developing technology of interest to the government, the government has consistently shown itself to be unable to capitalize on these successes by getting the technology back into the government. Some of the challenge comes from government contracting and policy restrictions. Despite a product already existing, if it has not come through a traditional contracting process or is a true commodity item, there is not a viable contracting mechanism that meets the terms of both parties. This may be exacerbated by cultural barriers, through which government contracting officers might be reluctant to enter into contracts that do not comply with the FAR and have a crisply defined performance specification. Even when a commercial product is acquired, it may not be compatible

for integration into legacy government systems. This may be due to security-certification challenges or simply because the legacy system is very constrained and it would require exorbitant cost and time to perform integration.

Mismatch between R&D, acquisition, and operations. Aggressive, mission-driven private-sector companies tend to develop a beta product⁷¹ that they get into users' hands and then continue refinement iteratively with direct feedback from the user. This is counter to the way government programs function. As capability developers, they typically do not have the opportunity to engage directly with users. Even if they did, users usually do not have any acquisition funds or contracting mechanisms. Government acquisition organizations are very linear and expect a product to be fully defined up front (even before development begins, let alone after release) and do not support iterative development or user interaction. Government R&D organizations may have both acquisition capability and flexibility, but they have a mission that focuses on initial technology development, not operational usage. Thus many of the commercial products coming into government for continued iterative development are too mature for R&D organizations.

Cost of commercial items. When the government does figure out ways to acquire commercial products, it often balks at the cost structure. Even if the bottom-line cost is affordable, commercial products typically come with higher profit margins and licensing fees. Since the acquiring organization in the government is not the organization that would have paid for R&D in a traditional government acquisition, they do not see the net-cost savings to the government by having the private sector pay for the up-front development cost. They just see a product that is more expensive than what they are accustomed to buying.

Making “skunk works” activities relevant. There have been limited cases in which a government organization is created as a protected, isolated unit to develop innovative solutions unburdened by regular process. These can be very effective at creating stand-alone products, but keeping them relevant and getting them integrated into practice has proven as challenging as if it were a private-sector organization. There is a constant tension between being too close to legacy operations that innovation gets stifled, or too far and relevance is lost. In addition, security considerations often make it infeasible to replicate a “skunk works.”

Speed and culture. Even in government organizations like DARPA that have a reputation for innovation and have fought for flexible contracting mechanisms, they are not always put to full use by the U.S. government because of cultural barriers. Most program managers and other personnel in the contract chain think in terms of a traditional process of announcing a competitive solicitation that has a response period and then results in source selection and contract negotiation, even if it is intended to be a flexible contract, such as an OTA. Even in a streamlined organization, this process can take months and require the generation of a

71 Beta Product: A limited release with the goal of engaging the user in the testing the product.

few hundred pages of proposal material for the developer. Private-sector companies that feel they are doing the government a favor by agreeing to partner are not willing to subject themselves to this process. It is too much of a disruption to their core business.

Motivating more private sector responsibility. The passive partnerships described in this chapter are a significantly underutilized opportunity for the government. This is driven at least in part by private sector companies' reluctance to invest in security. Every dollar of security investment is a dollar taken away from profit. Instead they view their threats in the context of risk management. Even when a threat is very real, if the liability for it can be avoided, they will avoid paying the cost for security. If the government embraced this model as a form of security leverage, there is much that it could do to stimulate more private-sector security investment and partnership. Specific ideas are discussed in the next section, but in general it involves communicating the true latent liability in a manner that is in the best interests of the company to take action.

Risk of blowback. A final cautionary note is that if the government would ever get very serious about PPPs, particularly passive partnership, there is a very real risk of "blowback." As discussed above, passive partnership opportunities exist because powerful companies' interests align with the government's and the common good. But what is the future if these institutions grow too powerful and their interests diverge? There is a serious risk of a rogue corporation or even individual acquiring so much power that the government is helpless to prevent it from imposing its will. Is this the makings of science fiction and the "Iron Man" movie series, or is it the ultimate strategic latency?

Recommendations

The main objective of this chapter has been to inform the reader about opportunities that exist for PPP based on historical experience and current initiatives. To conclude the chapter, it may be helpful to consider some ideas to strengthen both the opportunities for PPPs and the ability to leverage them to warn about and perhaps even shape occurrences of strategic latency. These recommendations are speculative and are by no means intended as a comprehensive list, but rather as a starting point to encourage the reader to consider other innovative ideas.

Develop truly innovative means of funded interaction pilot projects. The government needs an organization that can truly be a dynamic bridge in a PPP. The full description of such an organization may be worthy of its own chapter in a future book on strategic latency, but for now there are a few key characteristics such an entity would need to exhibit. It needs to be highly independent of traditional government organizations and have its own authorities, including special staffing and contracting. It must be able to develop new capabilities without requirements oversight, working with whoever is best for the problem at hand, even if it is a nontraditional institution.

At the same time that it enjoys this independence, it must stay tightly coupled to its home organization. The most critical coupling is with the operators. This interaction will help ensure new capabilities are relevant and provide the venue for iterative development. They should also maintain interactions with counterpart traditional government acquisition and R&D organizations. While this is likely to create competition and friction, it is nevertheless important, since these traditional organizations may be necessary to make modifications to legacy government systems to enable integration. Also, an ideal outcome would be for the traditional organizations to begin inheriting some of the innovative practices of the “skunk works” organization.

Open-systems technology. Most of the technical challenges surrounding good leverage of PPPs comes from the difficulty of integrating new capabilities into legacy systems. This challenge could be substantially mitigated by greater adoption of open-systems technologies. A full discussion of open-systems technologies is beyond the scope of this chapter, but at the time of this writing there were numerous government initiatives underway, like SOFWERX in Tampa, to develop new tools to speed integration and open portals to the private sector.⁷² These range from more traditional projects to identify important system interfaces and relevant standards to some radical new tools being developed to translate interfaces dynamically without the need for common standards. Adoption of tools and best practices such as these would greatly reduce the time and expense of integrating new commercial technology into government systems. They could even be engineered in such a way as to support multi-level security protocols, and thus mitigate some of the security barriers to commercial adoption as well.

Government initiatives to encourage more private sector security. Very limited, no-to-low-cost actions by the government could drive significant leverage in private-sector security investment. This could help create a strong market for private-sector security and facilitate very strong passive partnerships with the government. Much of this activity should focus on risk modeling. Many of the more serious hybrid threats fall into the category of “black swan” events: the likelihood is vanishingly small, but the impact is catastrophic. (This is also a fundamental characteristic of strategic latency.)

Actuarial analysis is notoriously bad at quantifying these types of risks because of the dearth of empirical data. The government could support teams of risk experts, economists, intelligence analysts, and technologists to develop new models for assessing and quantifying the latent liability associated with these threats. Once a liability is quantified in some manner, it can be monetized. This in turn provides a basis to estimate a true market for private-sector security, which in turn can drive proportionate private investment.

Means of aggregating private-sector security. To get the most out of passive partnerships, the government needs a strong mechanism for aggregating, abstracting, and disseminating

72 <http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=2068>, last accessed October 27, 2017.

information from partners and back out to government users. Doing so provides the best leverage of passive partnership information, motivates private-sector partners to participate (since they will be able to receive more government information for their trouble), and minimizes the risk of blowback, since this model provides the opportunity for greater government insight and control. It must be done using technology that allows for “double-blind” search and fusion that protects classified government information, as well as the privacy and intellectual property of the private-sector partners. Some of the open-systems technology described above, combined with new data-fusion technology could provide the technical means. Organizationally it would need to be conducted by a very independent organization, possibly like the “skunk works”-like organization described above, or even a third-party private-sector company used as a conduit.

In this chapter we have begun exploring the influence that government–private sector partnerships can have in strategic latency and innovation. The first step entailed developing a taxonomy for defining a spectrum of partnerships. We then mapped real-life examples onto this spectrum and discussed key aspects of those partnership examples. The conclusion is that in today’s environment the private sector is an essential ingredient for cutting-edge innovation, and under the right circumstances the U.S. government and the private sector can gain much from each other.

Although there are common themes for success that have emerged, like overlapping interest, mission focus, and creative investing/funding, no two situations are alike. Thus, the challenge ahead for the U.S. government is to strive for creativity, agility, and flexibility in its approach. In turn, the private sector needs to maintain an open mind for interacting with the U.S. government to protect our country from the ever-increasing list of potential, i.e., strategically latent, and real threats to our national security.

Chapter 14

Moving at the Speed of S&T: Calibrating the Role of National Laboratories to Support National Security

Lisa Owens Davis

Introduction

In a world of increasing access to information, education, and technology on a global scale, the U.S. needs wise, strategic investments to maintain science and technology (S&T) leadership and national security advantage. Recent government studies and experts' groups have examined the state of research and development activities in the United States in relationship to its scientific and security edge. For example, the congressionally mandated "R&D Commission"¹ raised the concern that government funding for innovative research and development (R&D) is lagging behind our adversaries and the perception that our institutions, including the national laboratories, are not keeping up. It recommended the U.S. government broaden its R&D base and encourage new participants, "especially small innovative firms." In that spirit several federal government agencies are undertaking outreach efforts in Silicon Valley and other tech hubs in the United States. Efforts such as the Defense Innovation Unit Experimental (DIUx) and the Department of Homeland Security (DHS) seek to tap into not only new technology but also the innovative spirit of the private technology (tech) sector.²

However, bridging the gap between the large institutions and bureaucratic practices of the federal government and the fast-paced, risk-taking innovative firms in the private sector

1 The R&D Commission is the short title of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community, and was established by Congress in 2002 to examine the state of R&D in the Intelligence Community.

2 The DOD stood up the Defense Innovation Unit Experimental (DIUx) at Moffett Field in Mountain View, California to serve as a catalyst for new relationships and collaborative national security opportunities. DHS followed suit.

poses many challenges. In this context, we examine the role of the NNSA laboratories, which have undergone multiple reviews in recent years to evaluate their role and effectiveness. The national laboratories reinforce the nation's R&D base with their evolving role in the Post-Cold War era, and might be well suited to play a strategic role working across scientific sectors in public-private partnerships for the advancement of security interests. Assessing various review-panel reports provides a clear picture of NNSA labs' assets in the service of S&T development. In addition, we provide two case studies of projects at Lawrence Livermore National Laboratory (LLNL) and Los Alamos National Laboratory (LANL) respectively to illustrate lab roles in public-private partnerships and the trajectory of core lab capabilities to broad S&T applications. We explore whether a more intentional lab role in such partnerships might enhance national security S&T innovation efforts.

Setting the Stage: Public-private Partnerships Are Not New, and They Can Work Well

Public-private partnerships in the interest of national security have existed for years with traditional defense contractors, mostly large companies. Little scholarly literature exists describing best practices in public-private partnerships; what does exist indicates several benefits and challenges. Critical infrastructure at the national, state, and local levels is often a combination of public and private ventures to manage and operate services such as energy, utilities, and water; security of this infrastructure is vital at all three levels. According to one article analyzing Department of Homeland Security (DHS) partnerships, public-private partnerships that address clear objectives and leverage the strengths of both sectors "can enhance public protection in ways not possible for government or businesses acting independently." The authors cite benefits in the areas of resource and staff enrichment, technology innovation, and trust-enhancing communication.³⁴

A Brookings Institution report similarly addressed advantages and challenges in public-private partnerships for infrastructure, advocating a strong legal framework and clear budget lines for partnerships. The projects should be based strictly on public imperatives and an understanding of private sector needs, aligning interests on both sides. To be successful, Brookings found that projects should be smart politically and applicable to clear, measurable public objectives. Once in place, these projects benefit from empowered

3 One example suggests a model for engagement with the private sector with a view to developing innovative technologies. In the SECURE program (System Efficacy through Commercialization, Utilization, Relevance and Evaluation), DHS specifies clear design specification and requirements against which companies can devote their own R&D efforts. And in theory, the companies are at an advantage to sell the government the technologies they design at a competitive price.

4 Nathan Busch and Austen Givens, "Public-Private Partnerships in Homeland Security: Opportunities and Challenges." *Homeland Security Affairs* 8, Article 18 (October 2012): <https://www.hsaj.org/articles/233>.

teams, transparent processes, clear evaluation, and monitoring procedures and regular engagement with stakeholders.⁵

These recommendations make sense applied to present national security-oriented partnerships with smaller technology. As detailed in Chapter 6, DOD, the intelligence community (IC), DHS, and other federal agencies are pursuing such partnerships with smaller companies and start-ups. In our estimation, the purpose for this outreach is to understand (1) cutting-edge S&T by interacting with innovators in the industry, (2) how those advances could assist our adversaries, (3) how those advances might give the U.S. government (USG) an advantage against adversaries, and (4) how the U.S. might counteract the edge that the new technology is giving adversaries.

Challenges: Do We Really Have a Match? Can Government Achieve Innovative Solutions from Outreach to the Technology Sector?

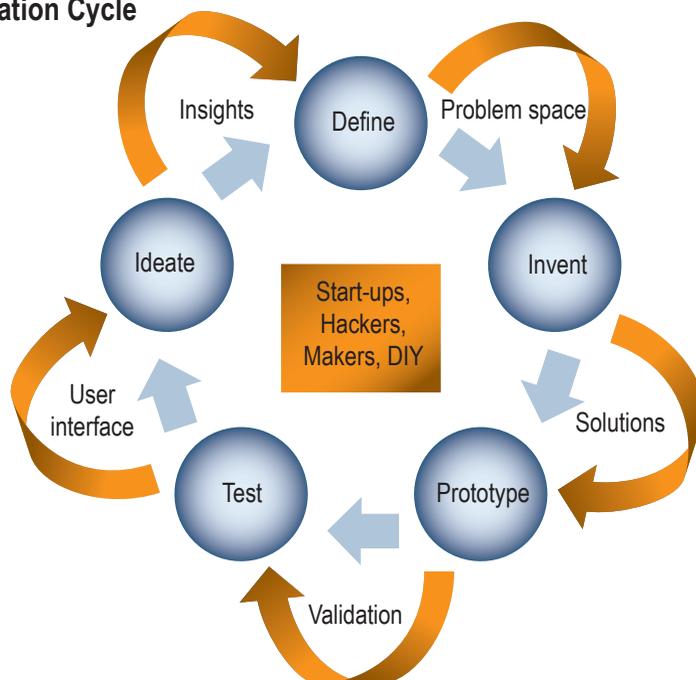
Many challenges faced in more general public-private partnerships are evident in any cross-sector relationship. Competing priorities and motives drive distinct procedures, practices, and behaviors. According to the above-mentioned *Homeland Security Affairs* article, challenges are often found among governance and responsibility, management and accountability, legal and ethical challenges, the need for transparency, politics, budget and long-term planning, and incentivizing private sector participation.⁶ More specific in federal government outreach to the tech sector, challenges may also include tolerance of risk, pace of work, and conflicts of interest and security or secrecy issues. Culture clash is inevitable when fast-moving, profit-driven industry and creative start-up cultures in Silicon Valley encounter the slow-moving, red tape-entangled large institutions of the government.

In striving for innovation, conflicts between government and private-sector cultures may be more evident. Innovation is fostered in an atmosphere of open, creative trial and error with little concern about failures (see figure below). Among the “hacker” or Do-It-Yourself (DIY) community, the key is to do whatever it takes to get results as efficiently and effectively as possible, including workarounds and possibly breaking the rules. Among start-ups, success often comes from failure.

5 Patrick Sabol and Robert Puentes, “Private Capital, Public Good: Drivers of Successful Infrastructure Public-Private Partnerships,” *Brookings*, (December 2014): <https://www.brookings.edu/research/private-capital-public-good-drivers-of-successful-infrastructure-public-private-partnerships/>.

6 Busch and Givens, *Public-Private Partnerships*, 2012, <https://www.hsaj.org/articles/233>

Innovation Cycle



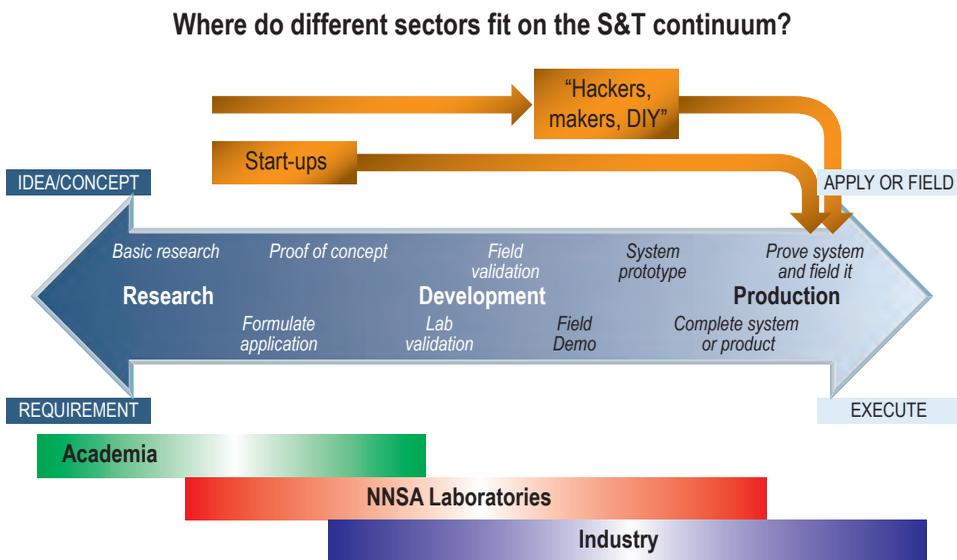
In the government, only so much failure or risk is acceptable, and stability may win out over freewheeling innovation. For national security missions, there are real consequences for applications of new technologies—they have to work and if there is an urgent need, there is no time or funding available for multiple failures. So in some circumstances the government may have to go with the safest solution instead of the most innovative solution. In addition, taxpayer dollars fund government R&D and S&T efforts. Executive-branch bureaucrats and congressional representatives can only tolerate so much risk with the taxpayer dollar.

Incentive to partner is another hurdle to overcome between government and the private sector. Not only is it unclear whether US government outreach efforts have clearly defined goals or funding mechanisms, it is also unclear whether industry is motivated to partner. The private sector must make decisions based on the viability, profit, and general good of the business, not necessarily the public good. Many government projects may have only small-scale profitability or transferability, and could contain perceived risks to a company's market viability or reputation. Many businesses simply cannot afford to jump through all the procedural hoops required to do work for the government. This challenge is very difficult to overcome. Moreover, a generalized distrust of government may make it difficult to persuade companies to partner. The R&D Commission noted that:⁷

⁷ "Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community, Unclassified Version," *U.S. Senate Select Committee on Intelligence*, accessed July 5, 2016, https://www.intelligence.senate.gov/sites/default/files/commission_report.pdf.

...Such [small] firms currently are often discouraged or precluded from contributing by the time and cost imposed by the IC's security and procurement requirements, not to mention the onerous restrictions placed on them as subcontractors of some of the larger contracting organizations. A tiered approach that allows more direct contracting with small firms for important R&D areas should be examined, with the goal of applying it broadly across the IC R&D enterprise.

Another challenge in the national security arena is secrecy. Classification rules and security requirements may restrict government agencies from sharing full technical requirements with a private-sector partner or limit knowledge of the technology's end use. Information compartmentalization is another challenge in this context. For example, DHS officials cite problems related to classification as one of their greatest challenges in working with the tech sector. As it scouts cybersecurity solutions in Silicon Valley, it is faced with difficulty accessing classified information or classified systems to explicitly address the cybersecurity problems it aims to solve.⁸



⁸ As DHS scouts and recruits talent for cybersecurity work, "... that endeavor could be complicated by the fact that, according to Barron-DiCamillo, NPPD components such as US CERT do not have facilities in Silicon Valley where employees can access classified networks. In other words, if US CERT wants to hire a cyber-forensics expert based in the Valley, custom arrangements must be hashed out to give the new employee access to any classified information their new job might require."

Could the NNSA National Labs⁹ Help Bridge the Gap Between the Two Cultures?

The NNSA Laboratories, like federal government agencies, are large institutions from another age and beholden to the bureaucracy of their parent agency, the National Nuclear Security Agency (NNSA). The Labs' nuclear weapon missions of the Cold War era are slowly turning over to address national security challenges more broadly. And like some industry and Silicon Valley companies, the NNSA Labs are driven toward new scientific achievement. Its scientists are motivated to publish, discover, and innovate. Indeed, the National Labs, by the nature of their history and scientific mission, are natural innovators for the government. The nuclear weapon program required and continues to require novel designs and engineering feats. LLNL and LANL were set up to compete against one another to ensure the highest quality of weapon designs. The weapons labs developed cutting-edge technology to support the nuclear weapon mission—high-performance computing (HPC), modeling and simulation, energetics, novel materials, and sophisticated diagnostics, to name a few. And the labs maintain internal R&D programs to foster new science, engage the best and the brightest doctoral and post-doctoral scientists, and advance national security missions. Where do the labs fit as the federal government hunts for new ways to have innovative S&T applied to national security missions?

The 1990s shift from a primarily nuclear weapons mission (and reliance on the infrastructure and assets that the Cold War era created at the labs) toward complicated and relatively unclear new national security missions of the present has left the labs to navigate a relatively unclear pathway. Various commissions have addressed the issue of how to direct the labs in the new and evolving security environment. This mission shift requires concerted strategic focus, clear federal government prioritization of major challenges, and effective management. The mandate is for the laboratories to leverage the investments that the government has made for decades in the nuclear weapon program, including infrastructure, experts, and capabilities, to address new national security challenges. (See Stimson Task Force report for more.)¹⁰

9 For clarity, focus, and simplicity, we address only the NNSA Labs in this article, even though much of our observations and research applies to the broader complex of DOE laboratories as well.

10 Frances Townsend, *Leveraging Science for Security: A Strategy for the Nuclear Weapons Laboratories in the 21st Century* (Washington D.C: Henry L. Stimson Center, 2009).

Exploring the findings and recommendations of the various commissions provides insights into the utility and roles of the NNSA labs.^{11,12,13,14,15,16} The majority of these studies focus on governance and management issues and indicate the labs are not being utilized to their fullest extent. In general, the commissions recommend better leadership and less micromanagement from their parent organization as well as improved internal lab management to ensure appropriate accountability and connection to the strategic mission. Aside from making management recommendations, these commission reports also highlight the value of the laboratories, calling them a vital part of U.S. ability to maintain an S&T edge in national security. These commission reports underscored specific lab assets including:

- **Nuclear deterrent responsibility and expertise.** Every year the Secretary of Energy must certify the reliability of the stockpile to serve U.S. national security requirements. In the absence of nuclear testing, the NNSA Labs undertake research and development, scientific experimentation, and testing to support this certification. Activities include high-performance computer modeling and simulations, engineering audits, and laboratory and flight-testing of warhead components. Maintaining the U.S. nuclear deterrent is conducted under NNSA's Stockpile Stewardship Program, which seeks to ensure nuclear weapons remain safe, secure, and reliable.¹⁷
- **Rare technical expertise and focus that provide S&T advantage.** This S&T advantage is a result of decades of investment in the capabilities and facilities in support of the nation's nuclear deterrent. Routinely the labs spin-off capabilities with broader applications; for example, through understanding nuclear weapons and diagnostics, the labs develop nuclear detection and verification systems. And moving farther from the core nuclear weapons mission, labs undertake big science projects such as the Human Genome Project based on expertise growing

11 Norman Augustine, et al., "A New Foundation for the Nuclear Enterprise: Report of the Congressional Advisory Panel on the Governance of the Nuclear Security Enterprise," *Nuclear Security Working Group*, December 12, 2014, <http://nuclearsecurityworkinggroup.org/congressional-advisory-panel-report-a-new-foundation-for-the-nuclear-enterprise/>.

12 "Final Report-Commission to Review the Effectiveness of the National Energy Laboratories," *Department of Energy*, October 2015, <https://energy.gov/labcommission/downloads/final-report-commission-review-effectiveness-national-energy-laboratories>.

13 Matthew Stepp, et al., "Turning the Page: Reimagining the National Labs in the 21st Century Innovation Economy" *Center for American Progress*, June 20, 2013, <https://www.americanprogress.org/issues/green/reports/2013/06/20/67454/turning-the-page-reimagining-the-national-labs-in-the-21st-century-innovation-economy/>.

14 Townsend, *Leveraging Science for Security*, 2009.

15 *Aligning the Governance Structure of the NNSA Laboratories to meet 21st Century National Security Challenges* (Washington D.C: The National Academies Press, 2015).

16 Elizabeth Turpen, "2009 Stimson Task Force Report: Leveraging Science for Security," (presentation to congressional commission on the DOE laboratories, September 2014).

17 "Defense Programs," *National Nuclear Security Administration*, accessed July 27, 2016, <https://nnsa.energy.gov/about/ourprograms/defenseprograms>.

out of health physics responsibilities and capabilities in supercomputing.¹⁸ Moreover, the National Labs reinvest in state-of-the-art scientific development through Lab-directed R&D (LDRD). Lab scientists seek new discoveries drawing from lab core competencies and seek revolutionary improvements to applications as diverse as nuclear detection, bioengineering, electronics, energetics, computations and simulation/modeling, and materials. The labs' scientific missions and peer-reviewed work establish connections with academia and industry through science-based projects, professional societies, and technology-transfer arrangements.

- **Historic connection and deep understanding of the U.S. national security mission space and its goals and procedures (relative to industry or academia).** The labs have been fulfilling national security requirements through the nuclear weapon program for decades. Core capability spin-offs also address nonproliferation, counterterrorism and homeland security. The labs have experience with and insights into mission requirements and ultimate national security applications for sponsors at NNSA, DOE, DHS, and DOD, to name a few. This experience gives the labs insight into the logistics of U.S. national security programs, security and classification rules, and the connections between technology and policy development.
- **Performance of work ranging from R&D to applied technology that would not typically be done in industry or academia.** The NNSA Labs serve the national interest by pursuing work that might be too small or unprofitable for industry to invest in, too applied and pragmatic for academia to address, or too sensitive to send to the private sector at all.
- **User facilities.** These are important facilities of unique size, capacity, and capability that provide for peer-reviewed R&D by scientists in academia, government, and industry in areas as diverse as lasers, computing energetics, magnetics, and biology. Through user facility agreements, the NNSA labs allow these partners to conduct research to characterize, study, fabricate, calibrate, test, and evaluate new materials, systems, products, and processes. In this way, the NNSA Labs stay integrated in the scientific community. These user facilities have multiple capabilities and may be used as test beds. Please see Appendix A at chapter end for a list of user facilities.
- **Scientific community members.** NNSA Lab scientists and engineers are fully integrated in the S&T community, in particular through user-facilities interactions, but also through peer-reviewed publications, professional societies, and cooperative projects. This involvement allows them to maintain strategic relationships, understand state-of-the-art science, and communicate effectively

18 Kenneth Berns et al., eds. "The Human Genome Center, Lawrence Livermore National Laboratory," in *Resource Sharing in Biomedical Research*, Chapter 7, National Academy of Sciences, 1996. Accessed July 16, 2016, <http://www.ncbi.nlm.nih.gov/books/NBK209077/>.

with scientists and engineers outside of the government or lab system. In cooperative projects, lab personnel often perform an integrator role because of their broad experience and reach.

The overall sense of the labs through these commission reports is of a national asset that needs to be leveraged and that the challenge is not in the many facets of potential contribution, but how to organize and manage the labs and NNSA to better direct such assets. The following two examples effectively illustrate partnership success and the value of NNSA Lab assets.

Case Studies Illustrating Partnerships with the Labs

BLU-129 Case Study^{19,20}

The BLU-129/B is an excellent example of how a government–National Lab–industry partnership can work well, using a national lab for its unique expertise and as a liaison and integrator. The military had an immediate need in the field for munitions that were highly accurate but that minimized collateral damage. The partnership that produced the BLU-129/B to fulfill that need provided fast, high-quality results. The project was executed under the rubric of a joint DOE–DOD program, but the relationships LLNL built with the Air Force sponsor and the manufacturer were most important to the seamless transition from government requirements to design/development and finally manufacture by industry.

Outstanding Results

The BLU-129/B project was considered a success by the government sponsor, LLNL, and its industry partner. Leveraging a rapid innovation cycle using LLNL modeling and simulation expertise on its high-performance computers to develop a design within two months, the first BLU-129/B prototype emerged within seven months of the start date. It was fielded in 17 months. LLNL performed 95% of the final design through modeling and simulation. That capability coupled with LLNL materials expertise enabled a high-quality product that optimized development of stronger, lighter materials and peak performance.

More specifically, the models analyzed material compositions and characterized explosive properties in such a way that researchers could validate the predictability and reliability of the munitions' inner explosive and outer case. The LLNL team combined computer modeling and experimental analysis to evaluate carbon-fiber type, winding patterns, tow tension, epoxy mix ratio, and curing cycle to determine the most effective attributes to meet a sponsor's requirements for light weight, low collateral damage, and precision. Researchers

19 Caryn Meissner, "Advanced Engineering Delivers More Exact Weapons," *Science and Technology Review*, March 2013: pp.4–9

20 Bruce Goodwin, Associate Director at Large. Interview by author. August 17, 2016.

studied different material compositions that would eliminate ejected fragments and improve blast impulse at close range.

HPC resources were used to model a new type of explosive charge called “multiphase blast explosive” (MBX). The greater impulse of energy produced by MBX, which also decreases with distance from the munition, eliminated the need for metal casing to ensure penetration. The LLNL team evaluated carbon-fiber composite for the outer casing, modeling and experimenting to have the best qualities for the munition. Carbon-fiber composite is lighter, strong enough to withstand penetration into concrete, and produces no lethal fragments upon detonation. Its characteristics can also be controlled by the fiber-winding pattern.

With industry partners involved with LLNL from the beginning, the BLU-129/B transitioned seamlessly from development to production. The project was economically smart as well. Developed at government entities, the design of BLU-129/B is government-owned, which allows production to go out for bid to other manufacturers as needed. Competition helps the government get a good price.

Why Successful?

Unquestioned national need. Our analysis of the project highlights several reasons the project was so effective. First and probably most important was the fact that the military had clear requirements and a priority need. A highly prioritized wartime need can focus the most sluggish bureaucracies to work together toward optimized solutions. The casualties experienced in Afghanistan drove the military to seek innovative and highly effective solutions.

Relationships/rubric. There was no need to create complicated new agreements to enable execution of work by a national lab for the Air Force. Contracts could be drawn up under the Joint DOD/DOE Munitions Development Program, which has been in place since 1985 for the creation of advanced technologies for the warfighter. Existing bureaucratic constructs are useful for cutting through red tape, providing funding mechanisms, agreed priorities, and shared requirements. In addition, such agreements foster anticipation and predictability that can reduce risk, maintaining a baseline level of readiness. Perhaps more important, as noted above, however, were the personal relationships forged among the Air Force, Air Force Research Laboratory (AFRL), NNSA, LLNL and the manufacturer. LLNL, the Air Force, and the manufacturer (which worked with LLNL throughout the development and assembly process) were fully integrated, creating seamless, streamlined transitions from design to deployment and all points in between. Nothing gets done quickly and effectively without trust and confidence in your partners. Trust can only be built from strong personal relationships, mutual respect, and repeat successful performance.

Leveraging long-time S&T investments—tech ready to go (prêt-à-porter). The technology needed for the BLU-129/B was at a high enough technology readiness level (TRL), due to historic investments in LLNL’s weapon program, to enable quick turnaround. It leveraged

LLNL's computational codes, computing and manufacturing infrastructure, and physics and engineering expertise, all developed and supported by investment in LLNL's nuclear weapon program.

Lab Role

The role that LLNL played in this project leveraged its strengths. LLNL is strong in the designer role, using simulation, modeling, and HPC to refine and innovate. It took on the challenge of developing a lightweight, strong, and highly accurate munition by building a multidisciplinary team of physicists, computational experts, engineers, chemists, and materials and explosives experts. LLNL used its familiarity with government sponsors and their technical requirements for national security to expedite and distill the Air Force requirements for the BLU-129/B. It also acted as a liaison and integrator between government requirements and manufacturer, and in that role, it was an honest broker. LLNL navigated sensitive information as well as commercially available expertise and ensured a successful transition to industry by having the manufacturing partner involved in the design and development process.

Case Study #2 (from Los Alamos National Laboratory)²¹ LIBS—A National Laboratory Sweet Spot

Being able to analyze the elemental composition of soil, a piece of metal, or a rock on another planet without having to physically remove a sample and ship it off to a lab might seem like something out of an episode of *Star Trek*, but that's exactly the technology that Los Alamos National Laboratory has developed and is being commercialized for industry use, national security, and scientific pursuits.

Laser-Induced Breakdown Spectroscopy (LIBS) is a technology that analyzes the elemental composition of a solid, fluid, or gas by pulsing a laser beam at the sample, creating a short-lived, high-temperature plasma. A spectrometer then analyzes the light emitted by this plasma and accurately identifies the elements comprising the sample. This technology illustrates the sweet spot that a National Laboratory can play in bridging basic research, government missions, applied technology development, and industrial commercialization.

The origins of LIBS began in the early 1960s with the invention of the laser. The Los Alamos National Laboratory was involved in early basic research, due to its analytical chemistry mission in support of nuclear defense, and coined the name LIBS in 1980. Subsequent to that time, multiple missions have driven further research and applied technology development with the government and industry. For example, LIBS was applied to nuclear defense and nonproliferation activities to facilitate verification at a distance. Later it was

²¹ Prepared by Frank D. Gac (retired / Guest Scientist), Laura A. Mullane, James E. Barefield, and Roger C. Wiens, Los Alamos National Laboratory, LA-UR-16-26650.

applied to the oil industry to detect pipe corrosion and finally LIBS was adapted to planetary science applications.

On Other Worlds—Understanding Our Past and Envisaging Our Future

On Mars, sitting atop NASA's Curiosity rover, is ChemCam, a LIBS instrument developed at Los Alamos that can, with a few laser pulses, analyze the chemical composition of Martian rocks and quickly send valuable data about the planet's surface back to Earth. In the four years since landing on Mars, ChemCam has analyzed roughly 1,500 rock and soil samples with more than 350,000 total laser shots at about 10,000 points in all. This data has helped to reveal ancient Mars to be much wetter, and the atmosphere much more oxygen-rich, than previously believed.

The success of ChemCam resulted in NASA contracting with Los Alamos and its partner at the French space agency to create SuperCam, a LIBS instrument that will sit atop the Mars 2020 rover. SuperCam will add another spectrum to its laser that provides the molecular makeup of a target, therefore allowing geologists to determine mineralogy and search for organic materials—thereby providing even more valuable information to scientists back on Earth.



The photo above is a “selfie” of ChemCam; note the inverted image of the Mars surface reflected off ChemCam's primary mirror (photo courtesy of NASA/JPL-Caltech/MSSS).

The Lab Role

In all of these successes, the laboratory drew upon its extensive research in analytical chemistry, advanced computing, and materials science, coupled with a longstanding history of fabricating hardware for extreme environments, such as space, and partnered with industry and other countries to deliver cutting-edge technology. This is an example of developing technology for its core nuclear mission and then working through partnerships to apply it to diverse commercial and scientific fields. This is the sweet spot of a National Laboratory.

Using the NNSA Labs to Help Address the Challenges of Strategic Latency

The NNSA Laboratories are science-driven and perform national security missions on behalf of the government. The case studies illustrate the broad reach of NNSA lab products as well as their ability to operate simultaneously in the technology culture of industry and the security culture of government. Involving the labs in public-private partnerships as intermediaries could overcome some of the challenges noted above.

Insertion of the labs could help pull the processes for government requirement-development and acquisitions in sync with the swift innovation cycles of start-ups. Often the National Labs perform a risk-reduction role early in the realization of a need and can design solutions and develop approaches to a level that a company could take over and work more efficiently. Once the lab can provide proof of concept and produce a prototype that is accepted by the government sponsor, it can pass the technology along to industry for production. If there were a cycle of innovation that allowed a more integrated, ongoing partnership between the labs and start-ups, the labs could take nascent concepts from a start-up partner and develop them into a prototype and test them for application to the security mission. The prototype could then go back to the start-up or to another industrial partner for refining and production.

Conversely, a start-up could take existing technology developed at the labs and innovate around that technology for novel approaches or new applications. For example, DataTribe, an emerging investment entity, has indicated that highly sophisticated cybersecurity technology already exists in government and at the National Labs.²² They intend to license and create start-ups around that technology to improve upon what already exists. Integration of National Labs into their development activities could improve the effectiveness and applicability of their products. Overall, earlier engagement among government, industry, and the labs could facilitate translation of needs and syncing of cycles. The BLU-129/B case study illustrated a successful example of integrated and early partnering leading to rapid solutions. The key may be to find productive peg points for the interaction of each player in the partnership. In addition, contractual relationships established under ongoing partnerships or umbrella agreements might also facilitate or reduce company navigation through the government acquisition process.

As another example of public-private challenge, the sensitivity of program requirements or classification of technology applications can hinder interactions with industry. For example, DHS officials are concerned that its Silicon Valley office does not have access to classified facilities in which to conduct cybersecurity solutions with potential start-up or private-sector

²² Heather Somerville, "Investment firm to fuse startup culture with U.S. intelligence complex," *Reuters*, July 26, 2016 accessed October 27, 2017, <https://www.reuters.com/article/us-cyber-startups/investment-firm-to-fuse-startup-culture-with-u-s-intelligence-complex-idUSKCN1061JT>.

expert partners.²³ A government-industry partnership might benefit from using NNSA Lab classified facilities and security-cleared staff to complete projects. In terms of access to classified information, perhaps a private company develops the technology and approach with surrogate unclassified information, in consultation with lab scientists that may understand the bigger classified picture. And once there is a prototype, the lab personnel could test the approach or tools on a classified system.

NNSA Lab personnel may also be effective translators or intermediaries to overcome any private sector unfamiliarity with or skepticism toward government. Getting to innovation means working with creative technical experts and scientists in Silicon Valley. NNSA Lab scientists may well understand the same language, and relate to the culture and technical drive of Silicon Valley while bridging the gap with their corresponding deep knowledge of the national security space as well as government contracts and regulations. Moreover, the NNSA Labs may offer unique incentive to private-sector partners for collaboration through use of unique user facilities and access to expertise and capabilities. As noted above, lab scientists have robust collaboration and peer-reviewed R&D with academia and industry through their user facilities.

Conclusion

Partnerships among government, national laboratories, and industry for enhancing U.S. national security make good sense theoretically, but the difficulty comes with *how* to do so and *for which* S&T missions. The National Labs and NNSA struggle with effective processes to allow broader access to the labs to perform “work for others” (WFO)²⁴ in a manner that is efficient and expedient. The key seems to lie in the more strategic engagements that NNSA may or may not directly facilitate. In addition, the more the WFO community can articulate its priorities and have a dialogue with the labs about their S&T expertise and insights, the easier it will be to get the right work done by the right parties on the right problem. Add in industry partners, and the need for communication and openness only grows. The key appears to be in forming a structure and process that facilitates strategic agility: increasing the potential to move to the right experts at the right time, a relationship that fosters creativity. Recommendations for productively including the NNSA Labs in public-private partnerships include:

- Merge culture and innovation cycles through technology hubs. Create hubs of specific technology areas at the NNSA National Labs, taking their greatest assets and making them the center of development for that S&T area. The hubs would enable partnership with academia and the private sector.
- Overcome security hurdles through the establishment of NNSA Lab test beds and use

23 Sean Lyngass, “DHS sets up shop in Silicon Valley,” *FCW: The Business of Federal Technology*, March 8, 2016 accessed May 27, 2016, <https://fcw.com/articles/2016/03/08/dhs-silicon-valley-outreach.aspx>.

24 Work for Others (WFO) refers to any work at NNSA National Labs sponsored by a government agency other than DOE or NNSA .

of their classified facilities. Establish a clear lab role to take on classified work in established public–private partnerships. Partner early then take data, approaches, etc. and apply them in classified systems, or test them out in a classified atmosphere at the labs.

- Enhance clarity for public–private partnerships as well as NNSA Labs involvement through focused strategic planning for national security needs within and among NNSA, DOD, IC, and DHS. Such planning could foster clear budget lines and facilitate development of requirements and technical solutions.
- Provide agility through generalized yet focused interagency agreements such as the Joint DOD/DOE Munitions Development Program. Such agreements provide a broad mandate and in some cases budgetary support to allow work on particular technology areas or security applications.

Inclusion of the NNSA Labs may not solve all of the challenges inherent in public–private partnerships, but where their S&T investments might provide advantage in achieving innovation for national security applications, it would be foolish not to try.

APPENDIX: NNSA Laboratories' User Facilities

LANL's largest user facilities²⁵

- Los Alamos Neutron Science Center (LANSCE)
- National High Magnetic Field Laboratory (NHMFL)
- Center for Integrated Nanotechnology (CINT)
- 30 other LANL facilities are available to outside users, including scientists and engineers from industry, universities, and government agencies.

LLNL user facilities²⁶

- Center for Accelerator Mass Spectrometry
- Biomedical Accelerator Mass Spectrometry
- Center for Micro- and Nanotechnologies
- High Explosives Applications Facility
- Joint Genome Institute
- Jupiter Laser Facility
- National Atmospheric Release Advisory Center
- National Ignition Facility
- Program for Climate Model Diagnosis and Intercomparison
- Site 300
- Terascale Simulation Facility

Sandia National Laboratory's facilities²⁷

- Advanced Power Sources Laboratory
- Combustion Research Facility
- Design, Evaluation, and Test Technology Facility
- Distributed Energy Technology Laboratory
- Engineering Sciences Experimental Facilities
- Explosive Components Facility
- Explosive Technology Group

²⁵ User Facilities," Los Alamos National Laboratory, accessed September 2017, <http://www.lanl.gov/collaboration/user-facilities/>.

²⁶ Lawrence Livermore National Laboratory, User Facilities, accessed December 2017, <https://www.llnl.gov/research/user-facilities>,

²⁷ "Technology Deployment Centers," *National Technology and Engineering Solutions of Sandia, LLC*, accessed September 2016, http://www.sandia.gov/research/facilities/technology_deployment_centers/.

- Geomechanics Laboratory
- Ion Beam Laboratory
- Materials Science and Engineering Center
- Mechanical Test and Evaluation Facility
- Microsystems and Engineering Sciences Applications (MESA)
- National Solar Thermal Test Facility
- Nuclear Energy Safety Technologies (NEST)
- Nuclear Facilities Resource Center (NUFAC)
- Photovoltaic Laboratories
- Pulsed-Power and Systems Validation Facility
- Primary Standards Laboratory
- Radiation Detection Materials Characterization Laboratory
- Shock Thermodynamic Applied Research Facility (STAR)
- Weapon and Force Protection Center

Chapter 15

Picking Winners and Losers: How the Government Can Learn to Successfully Assess Technology Potential and Turn It into a Battlefield Advantage

Toby Redshaw

Every day the media reports breaking technology stories, stories that describe how the private sector is identifying new technologies, insightfully projecting their potential and turning those tech investments into corporate profits. It seems easy, right? Then why has it been so difficult for the government? What hidden calculus prevents entities like the Defense Innovation Unit Experimental (DIUx) from interfacing and achieving the same kinds of successes for the Department of Defense? Why can't the government figure out how to be more like Silicon Valley?

Let me be clear, there are a lot of shiny, happy technology success stories that truly have great merit springing up from places like New York City, Boston, Chicago, Austin, and Silicon Valley. For simplicity, we'll focus just on Silicon Valley, the jewel in the crown of the U.S. technology revolution. Silicon Valley has the expertise the government needs, not just for the battlefield but for future science, medicine, policy and more. As such, the communities and people of Silicon Valley are best positioned to help inform the government on how to leverage technology advantageously and where to make smart changes both in processes as well as policy. But this does not mean that the government should strive to become just like Silicon Valley. There are several reasons why.

Silicon Valley is not a great model for efficient technology breakthroughs, orchestration of optimization or pragmatic technology adoption. It is more like a giant Darwinian game of roulette encircled by some incredibly helpful ecosystems designed to optimize the returns to a small percentage of players using other people's venture capital. It is financial privateers, dreamers, visionaries, and hordes of specialized, top-of-their-game craftsmen inside a highly functional tribal system with fantastic high-context communications. The government

is none of these things, nor should it be. In fact, the portion of Silicon Valley that applies to the government is very small. It is the portion that is extremely innovative and agile, two characteristics that the government must embrace if it intends to be successful in the era of emerging disruptive technologies.

There is no magic pill, no quick fix or rapid refocusing effort that can help government to leapfrog forward in this area fast enough to fend off the inherent threats or recover from the dearth of strategic latency experience. It is not as easy as mixing some Silicon Valley essence into the cauldron to produce an instant solution. The U.S. government is at nearly the last pivotal opportunity to course-correct. If done now, in the right way, we will be set on a fantastic path to lead and succeed in the next few decades against an accelerating tsunami of military, economic, and techno-social threats.

Understanding Silicon Valley from a Single Perspective

Silicon Valley is Charles Darwin on steroids. This incredible technology ecosystem merges money, materials, and battalions of talent with high-context communications and mission clarity and makes it look easy. There are around 100,000 new startups annually in the U.S. In the initial phases, a startup consists of a few humans, an idea and maybe a PowerPoint or two. Some even skip the PowerPoint part. 50% are angel- or friends/family-funded. About 4% make it to what would be called a real first funding round. This massive Darwinian sausage factory is not designed to filter for the best or most innovative tech. It is designed to filter out those that can't land funding and to provide their financiers a higher percentage chance of a lucrative exit. Those are two very different things. While a dose of Darwin may be a good thing for government on occasion, the process should be pragmatic progress and innovation, not technology roulette, because roulette is a less than zero-sum game.

Government must be about execution. In the S&T world this means just over-the-horizon must be about maintaining broadly applicable agility. In the real world, the applied world, this is ecosystem excellence—not creation, construction talent or investment guru-ism. This is about real culturally anchored, broad, insightful, innovation leadership and mission clarity. At the core, the truly inspiring mission might actually be governments, military, and security not investing in technology roulette. This means talent supply-chain management and motivation are equally as important, but we will come back to that.

Setting the Stage for Constructive Change

Many Americans believe that we are the technological world leaders, that our military and cyber forces are undisputedly superior, that America is a technology savvy, millennial-imbued economic powerhouse. So why should we worry at all about being leapfrogged in science and technology?

There are three simple reasons. The world is entering an era of unprecedented acceleration in scientific and technological advancement. While Weapons of Mass Destruction still hold

the dominant position for security concerns, this era will be characterized by Weapons of Mass Impact, which will create massive social and economic impacts that while much less bellicose still have the potential to be incredibly harmful. Finally, the barriers dividing disgruntled persons from bad actors are crumbling. Small, almost undetectable increases in pressure can trigger the movement from harmless to malicious. When coupled with the above, this is cause for alarm. Innovation and agility can help to mitigate this threat.

When considering the case for innovation, a look back over the past twenty years can go a long way towards developing a more accurate view to the future. There are a few things that stand out when one does this type of analysis that are both surprising and instructive to the way forward.

Green Men from Mars

No matter where you look, science, geo-politics, sports, weather, information technology, cyber, or even the energy sector, each area is full of what I refer to as “Green Men from Mars” events. What I mean by this term is if a year or two before a significant event I had asked prominent insiders whether that would be more probable than the arrival of green men from Mars, in most cases the men from Mars option would have been chosen as more likely. The rapidity with which the human genome was mapped as well as the drop in cost thanks to technological convergence are two examples. Chinese commercial cloning, CRISPR genetic modification, the growth of mobile, and the amount of data in the deep web are other great examples of this type of trend. The changing nature of threat vectors due to down-skilling of technological applications, the hundred-fold increase in capability and scale in the commercial dark web, and the catalog of extreme weather events are all clearly members of this category. Germany versus Brazil in the World Cup and Leicester FC in the UK, the Cubbies win and even 2016’s Rugby World Cup final are not-to-be-believed-by-sane-people scenarios. These are all more than the unusual long-shot events. In fact, most would have been deemed pure lunacy if predicted just shortly prior to their occurrence. Mohamed Bouazizi being the ignition switch for any event at all, let alone the trigger for the Arab Spring is another interesting example. And yet these events are happening broadly and consistently.

Pattern Matching Is Just the Beginning

The huge growth and acceleration we have seen in the information technology space with social media, mobile technologies, areas like artificial intelligence, big data, and cyber, while impressive, are the patterns not of a technology that has peaked but of a technology that is just getting started. These technology factors are force multipliers, impacting society, science, culture, business, security, intelligence, and future war. They are not and will not be applied evenly. A perfect example of this can be found when considering the amount of data, the amount of IP-enabled nodes, and the unit cost of computer throughput for the next decade. These factors could scale 500 to 1000 times in the next ten years, potentially

even faster and more steeply if technological convergence comes into play, which clearly makes today's technology the very edge of the beginning on a hockey-stick curve.

The Rate of Change

The simple truth about current threats and opportunities is that the rate of change is exponentially increasing across all areas of human existence while the scale of change is ever rocketing upward. Take the simple conversion of the hacking population, which began with 80% independent hackers and 20% somewhat organized professional criminals to the equation facing governments today where roughly 80% of hackers are now parts of organized criminal and sometimes state-sponsored or affiliated organizations with a level of sophistication that was previously only possible if one was a nation-state. To make matters worse, many of these entities have become even more interconnected, collaborating where it is mutually beneficial to do so and significantly increasing the complexity of the threat environment. Add to that the evolution of non-linear asymmetric marketplaces on the dark web, which has created a massive, sophisticated, supply-chain savvy, illicit commercial behemoth. What impacts will this have on legitimate commercial markets? The unit cost for technological horsepower continues to fall, dropping by 1000%, while the skillsets required for entry have been lowered tremendously.

What does this all mean? One thing is for certain: those that effectively embrace innovation at an organizational and cultural level will fare far better than those that do not. Indeed, if this is the beginning of the next set of accelerating changes with massive outlier impact, then driving innovation pragmatically across an organization would seem to be an imperative. This is easily said, but how does that work in a practical, real-world way?

Why a Culture of Innovation Is Key

The recent establishment of government innovation and tech-team outposts in Silicon Valley is independently insufficient to establish a culture of innovation within the Beltway. Innovation coaches and smart-lab ecosystems validating experiments can be force multipliers, but that can only occur within a broader effort where innovation is central to the mission or at least a well understood and supported effort. Most attempts to cultivate innovation in this fashion fail, especially in the corporate world, simply because of misalignment of mission with the mothership. Eventually, higher headquarters will kill off the unit, usually blaming lackluster local leadership. I was lucky enough to see Admiral Stavridis give an interesting presentation where he pointed out that recognizing Sisyphus was important, because after the initial attention from the "brass" fades, many of these outposts continually push one rock or another up the next hill with no variation in the end result. In today's rapid, fast-paced, and dynamic world, being innovative and truly agile may be the only sustainable competitive advantage. Broad innovation is cost effective and anchors agility and continuous improvement while siloed pockets of innovation can be good but are usually cost-additive.

Culture Eats Strategy for Breakfast

This is only true when strategy fails to understand that structure must be matched to mission. A new mission without appropriately modifying the structure (including the cultural aspects) is almost always doomed to fail. Businesses are bad at this. As the world and threats change around them, they typically recognize it and issue a call to arms. The problem is that when they have acknowledged these changes, they proceed to take to the battlefield with the very same army and strategy they used to win the last war, and then are astonished when they fail. Kodak is a classic example, but this problem is bigger than that. In 1935 the lifespan in the S&P 500 was 90 years. Today it is 18 years and rapidly shrinking. “Kodaking” a company is easier.

Combining smart strategy and cultural change requires as much pragmatism as innovation. Does your company have a culture that can innovate? There is, of course, a fog of uncertainty surrounding the term “culture.” I often hear that corporate culture is the insurmountable obstacle to innovation. Before I detail some accelerators that can help to drive a culture of innovation, it’s important to clear up some frequent misconceptions.

The culture of a nation-state or ethnographic segment is not the same thing as the culture of an organization, company, government agency, or institution. The culture of France, for example, is a complex thing and changes at a generational pace. It includes cuisine and the arts, theater, dance and literature. The culture of Motorola or the Department of Agriculture doesn’t have any of those things and in fact is a much simpler thing.

The culture of Motorola in the early 2000s was completely internally focused on the achievement of broad but marginal improvements. It was very much in love with engineering and IP filing for the sake of IP filings, not necessarily monetization. It was a family-oriented culture with literally generations working at the firm. It was in many ways a family business with the great attributes of family, a lot of which do not mesh well with fierce commercial competition. After decades of great pioneering success, the world changed. The firm began to fail. The board brought in a new CEO from Silicon Valley and together we radically changed the company culture in just 18 months by doing six simple things:

1. Clearly communicated a comprehensive new mission that was externally focused, fast-paced, innovative, and customer-centric.
2. Set out expectations for behaviors which would be rewarded or punished.
3. Continually “sold” the rationale behind why we were changing and over-communicated.
4. Made sure rewards and punishments were indeed publicly metered out to support the new direction.

5. Matched structure to mission and talent to task. When the game changes from soccer to rugby, not all team members get to move forward, despite prior excellent performance.
6. Eliminated active objectors and passive resisters who would only simulate support. One third of the top 120 executives changed inside 12 months for this reason alone.

With radical culture change came radical changes in performance too. In just 18 months we released the breakthrough RAZR phone that became the bestselling phone of all time. Unfortunately, a few years later Apple made a thing known as the iPhone and Motorola made some very bad leadership-talent decisions and chose to back hardware over software in our biggest business unit (Mobile Devices). No amount of motivation or positive innovation culture will save an organization from a bad strategy married to poor talent decisions for key posts, while facing emerging world-class competition.

In order for an organization to thrive in the midst of an innovation-heavy environment, a well-defined, well-communicated mission backed up by a clear system of rewards and punishments is key. Behaviors are driven by this system and to achieve the desired culture to sustain such a climate, the organization must get both the reward part and the punishment part right. What typically happens though is that the reward part, the easy part, is done correctly but the organization will fail miserably on the punishment side and then wonder why they still have cultural obstacles. The sum of the behaviors in an organization is the culture.

This is another important lesson from Silicon Valley that is useful to government entities seeking to establish an innovation culture. Be specific. Make certain that there is no lack of clarity on what the mission is because the attributes of that culture are all tightly aligned to mission. Silicon Valley does this very well. They have matched talent to task and created a fantastic talent supply chain that stretches from Stanford to Bangalore to Siberia to Waterloo (the Canadian one).

Again, to be clear, we don't want the exact same culture as Silicon Valley, but we do want a more agile and innovative one capable of handling the impending science and technology behind strategic latency threats. It also would be incorrect to assume that a peanut-butter spread approach is appropriate. We need a few starting points and some pragmatic target within governments where it makes the most sense, and unwavering leadership and decade-long stick-with-it-ness to see it through. Professor Jim Cash (Harvard Business School for 27 years) said that "sometimes to do good change management you need to change management." Innovation is born from this.

The term *innovation* is derived from two Latin words stuck together that basically mean "to make new stuff." If the mission for everyone from the top down is permissioned and expected to be innovative, then this can become part of the fabric or culture of that

organization. In Silicon Valley this is as common as oxygen. It is the default factory setting behind the tech culture.

The other mistake that is frequently made by organizations seeking to innovate is that success is driven by inventing big breakthroughs. This isn't the case. Successful innovators build their success around both big and small innovations. Things like room-temperature superconductivity or cost-effective fusion or a 10x throughput improvement for photovoltaic cells are huge, disruptive breakthroughs that I expect to see in the next 5–10 years. This however is not the domain of a culture of innovation for most organizations.

Almost all organizations have an untapped wealth of innovation that can be found in just eliminating daily the negative stuff confronting the rank and file. The person working on passport processing at the consul in Managua may have a process idea that is innovative and high impact for the whole organization. There is often an obvious-to-the-front-line-person opportunity for improvement that can provide a better, more efficient and effective solution to the status quo of doing things the way it's always been done. But without a culture of innovation, the masses of small, incremental continuous improvements lie dormant and amongst those, the ideas that have broader potential rarely surface. Idea platforms and innovation/suggestion processes are all well and good, but they should live inside an innovation culture where everyone knows this is a permissioned part of their individual mission, supported by the underpinning institutional agility and the continuous improvement that goes with it. In general, civil service throughout many time periods and geographies has historically been the opposite. The implementation of a culture of innovation means creating an ecosystem of support for an organization to live and grow in.

We have talked about clarity around roles, responsibilities, and the underlying command-and-control system aimed at managing incentives (and disincentives). We will talk a bit more about how to help drive a collaborative, cooperative, and teaming approach at scale. Common tools and processes help. Organizations desiring to become more innovative must consciously create connectivity across the horizons mentioned above. This means helping innovative ideas move from ideation to test, then taking them live (production) and ensuring correct scaling. Good ideas and changes often succeed out of the gate and then die from lack of attention, as scaling and maintaining change is difficult. It also requires innovators to have a near-term horizon and a long-term view in order to foster the desired cultural changes and keep the program on track as it grows out of its infancy. There are many stories about the initial excitement of going big on innovation that are then followed by nothing as the leadership attention waned, the novelty of the program passed and the hard work of scaling and maintaining ensued.

Change Management and Silicon Valley (But Just the Good Bits)

Having said all that, keeping up with the changing environment does not necessarily mean an organization should change at the same pace. Let me say that again: keeping up with

the changing environment does not necessarily mean we should change at the same pace. It does mean that we absolutely must be adaptable, agile, great at managing change, and very effective at the necessary but mundane underlying program management. These are required to be innovative at scale over time. It also means we must be deeply externally aware, see far over the horizon, and manage new potential challenges, opportunities, and threat profiles as far in advance as possible. Being innovative, effectively agile change masters is the prescription, but it doesn't happen overnight. This is a longer journey with incremental continuous progress. We eat the elephant one chunk at a time, not in one giant gulp.

Before we talk about change-management mastery I want to first dispel a key misconception about Silicon Valley being the model we should follow. I have been a venture capitalist (VC), a startup employee living out of a suitcase, a startup executive chairman, and served on over a dozen boards and advisory boards including first movers in key areas and a current "unicorn."

Silicon Valley has an excellent ecosystem for starting tech-intensive companies and a stack of experienced start-up tech talent inside a well-connected if not well-orchestrated network. It has an abundance of venture capital. It has amazing PR output mechanisms that trumpet wins (Google, Facebook, Uber, Airbnb, DocuSign etc.) while relatively ignoring or under-reporting failures. The VC world is also very good at killing off and "pivoting" failing ideas. A relatively unknown but great example of a successful pivot is Groupon. This firm was actually in shut-down mode and tried one last mini-pivot which turned it all around and it grew to \$14 billion in market cap. Yes, it later stumbled and yes, it's in Chicago, not Silicon Valley, but the point remains. The clear majority of VCs over the past twenty years have failed to provide competitive financial returns. The number of startup failures massively outweighs the number of winners.

The can-do, embrace innovation, full-tilt approach of Silicon Valley has much to admire (and copy), but it is not a model for how a large company, a ministry, a city or a nation wins with broad innovation. You want the biology of your entire organization to be innovative. You want broad majority success and innovation. And the only place you want the financial funding/portfolio betting side around ideas ensconced in business plans to be innovative is those areas in which you want to incubate and grow Silicon Valley-type outputs. Even then, the smarter approach may be to adopt models that cherry-pick the good bits from California innovators and marry those to broader company/entity scale models. This 2.0 version of Silicon Valley for government might feel more like Apple meets DARPA meets social incubator than the gold rush days of Silicon Valley a decade or so ago, but the end result will be a better fit for the kind of innovation needed.

The takeaways from Silicon Valley are really five things:

- Ecosystem approaches matter
- Agility, especially in killing off things that aren't working and then pivoting matters

- Attracting talent and managing the talent supply chain is crucial
- Rewarding innovation gets you a lot more innovation
- Innovation must be part of your company culture

Innovation at Scale Requires Change Management

I have spoken on creating a culture of innovation at many companies and organizations like Special Operations Command at MacDill AFB (under Admiral McRaven). I cannot talk about creating a culture of innovation without also teaching how change-management models work best. It sounds obvious that driving a culture of innovation is change intensive, yet I almost never see a decent understanding of change-management models or the ability to determine which one is most effective for specific situations. This education piece is important. Ensuring that all employees know which model the company wants to use and why is key and promotes buy-in. The opposite, not clearly articulating the “why,” invites problems, obviously. There are only four change management models and one of them is three times better than the next best.

Accelerators—Tactical Items That Have Real Impact

For an organization trying to go big on pragmatic innovation and agility, here are a few factors that are important accelerators and force multipliers they should know about.

1. **Knowledge Management/Collaboration Platforms.** This really matters. Leveraging the cumulative IQ of an organization is a clear winning strategy. There are platforms specifically designed to do this. IBM, Microsoft, Opentext, and Jive all sell them. I have implemented this as part of a change-management plan at three global 100 firms over the past fifteen years. These tools improve decision-cycle time and the quality of decisions, eliminate rework, motivate employees, help recruit people under 28, and expose expertise to broad audiences fast. The analysis branch of a leading intelligence agency runs on one of these platforms. Here is a link to a business case example: <http://bit.ly/1EQq8oM>.
2. **Agility and Program Management.** Having skilled and empowered program managers who can make honest calls on programs (especially negative ones) and do that special mixture of science and art that makes top-flight program management is vital. Of 504 large technology shops surveyed in the U.S., only 7% are ranked as excellent by their business leaders. The only thing they all have in common is that they are great at program management. Over-budget, underdeveloped, and late programs most often can be traced back to program-management skill gaps backed up by poor leadership.
3. **Journey Talent.** This is a simple and often neglected item. On any new journey, it is tremendously helpful to have a few people down in the trenches, plus a couple in the leadership ranks that have been on that same journey before. These are

accelerators and force multipliers.

4. **HLI and PowerPoint.** This works well if PowerPoint is a common artifact in your culture. I think PowerPoint is the lingua franca of government and many branches of the military around the world. I'm not sure that is a good thing, but I did this at several firms where PowerPoint was closer to an addiction and was an embedded facet of the culture. Quite simply I insisted that every program update, every group or function presentation start with HLI.
 - a. H = Highlights. Show what the team did well, what are the highlights. The real objective there is to say thanks, to spend a bit of time on the positive, to acknowledge that mini-win. It turns into a habit and teams over time start to think in terms of what are we putting in H on the front page. Accomplishment and recognition of accomplishment are simply necessary for a motivational environment.
 - b. L = Lowlights. Here you want to see some stretch, some failure, but most of all you want to see some learning and experimenting. By reviewing this without beating anyone up, maybe even praising the effort and what was learned from a failure, you eliminate the fear and de facto boost innovation. The message quickly goes through the organization/culture that no one got killed for stretch/trying harder and occasionally dropping the ball. This also helps kill one of the most anti-innovation elements in business, which is the "under promise over deliver" malaise.
 - c. I = Innovation. This is simply asking what did you try that was new, what did you grab from phase two and get done in phase one, what serial process did you make parallel, what new method or tool are you using, what did you borrow from prior efforts, etc. The trick is if anyone shows up with a PowerPoint that doesn't lead with HLI you politely cancel the meeting and get them to come back later with that fixed. Over time, quickly, this creates proactive activity inside teams to fill in each of these blanks. Teams start to have early conversations about how they are going to innovate.
5. **Learning Platforms.** It is easy to extend Knowledge Management and Collaboration with an LMS (Learning Management System) or to run them synergistically in tandem. I would also recommend considering massive online open courses (MOOCs) from leading institutions. This does not have to be for just learning content per se, in fact it can be even more useful by finding world-class experts to inform on ways in which learning can be improved, i.e., how we learn. One great example is a free short course done by the head of the Computational Neurobiology Laboratory at the Salk Institute. Interested organizations can apply his world-class brain and expertise on the topic to the critical learning part of their mission. It is free and high impact. Here is just one great example: https://www.coursera.org/learn/learning-how-to-learn/?utm_medium=email&utm_source=other&utm_campaign=opencourse.course_complete.learning-how-to-learn.~opencourse.

course_complete.GdeNrII1EeSROyIACtiVvg.

6. **One Tech Tool.** I firmly believe that technology prowess matters today in any mission you are undertaking. In technology, I believe talent, leadership, motivation, creativity, architecture, and context awareness all matter more than tools. However, in doing tech for 30 years there is one tool that is head and shoulders above the rest, especially as one moves an organization down a collaborative, pragmatic, innovative path. It is Business Process Management. A sub-three-minute video talks about this in some detail and is worth a watch: <http://bit.ly/1O6fbIV>.

Conclusion

The case for innovation is clear. We simply must become more agile and innovative in a pragmatic, results-oriented way.

The case for pragmatic innovation with real impact is complex. Hopefully the experienced-based sections above are helpful. Creating a culture of innovation inside a supporting ecosystem with a modicum of useful tools and the right leadership can lead to great success. Innovation is a pragmatic, broad-based journey, not a fad-centric exercise. Done well, it is the key to being agile and is a concrete force multiplier. It may well be the only sustainable competitive advantage over the next decade or so.

I think humility is key and is generally in undersupply. One of the best things you can do with Silicon Valley is find partners, collaborate, be useful, absorb, learn, and repurpose all that to your own ends. Being great at partnering is important and does not happen by accident.

Lastly, one thing that is inherent in many success stories in Silicon Valley is the idea of Net Transactional Value (NETV). This is about having a deep understanding of what the transactional value of your output is and trying to optimize it. But that is not enough. Net Value means I must subtract from the value the amount of hassle and cost that is required to get this or procure that. The real mission is to maximize the gap of the real net value between transactional value and the cost to do the transaction. The hackneyed example of this gone wrong is the DMV, although in all fairness there was a DMV in western Chicago a decade ago that was the paragon of efficiency and max NETV, so it can be done. I remember finding the supervisor and suggesting he go run United Airlines.

In this vein, one thing you find less of at Silicon Valley firms (at least the small ones) than at say, F100 firms, government agencies, or military procurement wings is unnecessary stuff or processes. These organizations intentionally focus on doing things smartly. Stupid stuff is very quickly eliminated in processes and everyday operations because stupid stuff is a fungus that kills innovation. In large environments, it grows by itself around unattended, undocumented processes and thrives on rules, forms, and neglect. The root cause is often found with those that write the rules or create the forms.

So, having said all that, yes, overcoming the looming set of threats confronting S&T is huge. It is a long hard hill to climb. It is not, however, Sisyphus. I promise you this is worth the climb.

Chapter 16

Strategic Latency, Technology Convergence, and the Importance of the Weapons Mix

Brian Holmes

Further Conceptualizing the Third Offset

This chapter provides a different perspective of the Department of Defense's Defense Innovation Initiative¹ and the Third Offset Strategy.² Because most of my time is spent analyzing emerging technologies³ and the development of future weapon systems,⁴ the unique conceptual importance of strategic latency is highly relevant. Major trends are forcing us to rethink the way we visualize, develop, and apply military technology that include: diverse operational domains;⁵ changes in the global order; a shifting and

1 Chuck Hagel, "The Defense Innovation Initiative" (memorandum, Pentagon, Washington D.C., November 15, 2014). <http://www.defense.gov/Portals/1/Documents/pubs/OSD013411-14.pdf>

2 Bob Work, "The Third US Offset Strategy and its Implications for Partners and Allies" (speech, Willard Hotel, Washington, D.C., January 25, 2015). <https://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/>.

3 Oliver Cann, "These are the top 10 emerging technologies of 2016," *World Economic Forum*, June 23, 2016 accessed October 27, 2017, <https://www.weforum.org/agenda/2016/06/top-10-emerging-technologies-2016/>.

4 "Anthony G. Oettinger School of Science and Technology Intelligence," *National Intelligence University*, accessed October 27, 2017, <http://ni-u.edu/wp/academics/schools/college-of-science-and-technology-intelligence/>

5 David Alexander, "Pentagon to treat cyberspace as 'operational domain'," *Reuters*, July 14, 2011 accessed October 27, 2017, <http://www.reuters.com/article/us-usa-defense-cybersecurity-idUSTR76D5FA20110714>

globalized technology landscape,^{6,7} and the unknowable effects of interdisciplinary scientific convergence.⁸ These trends are complicating the challenge of planning for future wars.

Much of this is captured in Max Boot's seminal book, *War Made New: Weapons, Warriors, and the Making of the Modern World*.⁹ Our recent history also provides important lessons. For example, the "weapons mix" strategy made famous in the 1980s by Dr. Michael Vickers (as depicted in the novel *Charlie Wilson's War*)¹⁰ offers insights into how to exploit foreign platform vulnerabilities and tactics to achieve a strategic goal. We need to build on past military strategies to re-conceptualize future offensive and defensive military weapons development. Such a reconceptualization will fundamentally align with key aspects of the Third Offset Strategy. By understanding the scientific, social, and political forces shaping the Offset Strategy, we can smartly position our military for success, as defined by the attainment of clearly communicated national objectives.

Intersecting Ideas Defined and Explained

The ability to match weapons to targets¹¹ in an effective manner is an age-old problem, particularly when there are known capability gaps¹² along the force continuum.¹³ The utility of each new weapons platform can increase operational flexibility, which becomes incredibly important to consider as operational domains diversify. Familiar conventional domains such as air, land, and sea are increasingly complemented by space, and information/digital. Consequently, the number of future defensive or offensive engagement scenarios for each domain individually, or in concert, are far more complex and interrelated. Domination of each domain becomes harder, and the number of targets higher. For example, emerging operational concepts such as those associated with swarm technologies are bringing further complexity.

6 S. Rajaratnam School of International Studies (RSIS), "Future Landscape Of Global Technology – Analysis," *Eurasia Review*, December 27, 2015, <http://www.eurasiareview.com/27122015-future-landscape-of-global-technology-analysis/>

7 "Homepage," *Office of the Director of National Intelligence*, accessed October 27, 2017, <https://www.dni.gov/index.php/global-trends-home>

8 James Gentile, "Is 'Convergence' the Next Revolution in Science?" *Huffington Post*, December 11, 2013 accessed October 27, 2017, http://www.huffingtonpost.com/james-m-gentile/convergence-science-research_b_4078211.html.

9 Max Boot, *War Made New: Technology, Warfare, and the Course of History, 1500 to Today* (New York: Gotham Books, 2006).

10 Max Boot, *War Made New: Technology, Warfare, and the Course of History, 1500 to Today* (New York: Gotham Books, 2006).

11 Christopher Pernin and Louis Moore, "The Weapons Mix Problem," *RAND Corporation*, accessed Oct 28, 2017, http://www.rand.org/pubs/technical_reports/TR170.html.

12 John Gordon IV et al., "Comparing U.S. Army Systems with Foreign Counterparts," *RAND Corporation*, accessed Oct 28, 2017, http://www.rand.org/pubs/research_reports/RR716.html.

13 "Escalation of Force - Non-Lethal Effects," *Marine Corps Concepts and Programs*, July 10, 2014 accessed Oct 28, 2017, <https://marinecorpsconceptsandprograms.com/programs/fire-support/escalation-force-non-lethal-effects>.

One positive aspect is that younger generations are more attuned to certain emerging technologies if only because of the realistic video games they play, and the unique impact of smart technology and virtual reality simulations. Consequently, two important ideas extracted from the Center for Strategic and Budgetary Assessment's *Toward a New Offset Strategy*¹⁴ are that future power projection will occur in multiple and possibly new domains, and that the application of disruptive technologies will play a key role for all combatants. How we connect these realities with our evolving technical, procurement, and budget priorities is a challenging question to answer.

The idea and implementation behind interdisciplinary scientific “convergence,” often the progenitor for disruptive technology, has been around for centuries, but its execution and impact has accelerated in the information age. These trends have direct consequences for the military. Academic scholars have analyzed the phenomenon of convergence in the context of the technical exchange of mindsets and the cross-pollination of ideas.¹⁵ For example, pioneers like Neil Amundsen,¹⁶ considered the father of modern chemical engineering, had the vision to hire and create a “synergistic, interdisciplinary team that made enormous contributions” to the fields of mathematics, biology, computer science, chemistry, and engineering, paving the way for today’s multidisciplinary approach.

More recently, new acronyms like “NBIC,”¹⁷ which stands for “nanotechnology, biotechnology, information technology, and cognitive science,” describe a new reality of interconnected, multidisciplinary science, both in the discovery phase and in their applications. A good example is human performance research, which represents a smorgasbord of converging technologies that may revolutionize human capabilities upon application. The military implications are staggering. The same is true for autonomous systems, hypersonics, and directed energy weapons, all of which are major factors specifically highlighted in the Third Offset.¹⁸ Decision-making about how to employ these complex and converging mega-technologies requires unprecedented knowledge that is rarely concentrated in one person or even organization.

The notion of “strategic latency,” which describes technologies (as tools) that have significant potential to be strategically transformed by a nation, group or individual for constructive or malevolent purposes, drives home the point that government cannot wait passively

14 Robert Martinage, “Toward a New Offset Strategy—Exploiting U.S. Long-Term Advantages To Restore U.S. Global Power Projection Capability” (Center for Strategic and Budgetary Assessments report, October 27, 2014). <http://csbaonline.org/research/publications/toward-a-new-offset-strategy-exploiting-u-s-long-term-advantages-to-restore/publication>.

15 Dan Berrett, “The Rise of ‘Convergence’ Science,” *Inside Higher ED*, January 5, 2011 accessed Oct 28, 2017, https://www.insidehighered.com/news/2011/01/05/is_convergence_the_new_big_idea_for_health_sciences.

16 “Neal R. Amundson: How he has transformed the scene,” *Minnesota Science & Technology Hall of Fame*, accessed Oct 28, 2017, http://www.msthalloffame.org/neal_amundson.htm.

17 M. Roco and W. Bainbridge, *Converging Technologies for Improving Human Performance* (Dordrecht: Springer Netherlands, 2003), 1-27.

18 http://www.nationaldefensemagazine.org/blog/Documents/Govini_Third%20Offset%20Taxonomy.pdf accessed Oct 28, 2017.

and expect cutting-edge technology to align with its national security priorities. Lawrence Livermore National Laboratory's Expert Advisory Panel in 2016¹⁹ examined how the private sector evaluates and develops disruptive technologies and compared it to the way the government funds, selects, and develops technologies for national security. The private sector, driven by market pressures, is less interested in fundamental research and prefers existing technologies that can be used to disrupt old business models. The government still tries to grow its own technologies through its government lab system or pay established defense contractors to piggyback military applications on established civilian technologies. New models are aimed at filling the gap between these two established pathways.

The Defense Innovation Unit Experimental (DIUx)²⁰ was created to address the fact that the private sector was building and marketing technologies useful to the military more rapidly and efficiently than what could be procured through the burdensome military industrial-acquisition process. The moment one technology hits the shelf, it's practically guaranteed that another one will soon leapfrog its capabilities due to market competition, component improvements, and electronic miniaturization trends. Operationally focused organizations like SOCOM, through modern initiatives like its public-facing intermediary SOFWERX,²¹ and the U.S. intelligence community, through non-profit strategic investor In-Q-Tel (IQT),²² have understood and tried to exploit this environment for years through different mechanisms. Of course, these two activities often serve a relatively small client base compared to the overall modern military force DIUx attempts to integrate with. The historic challenge for the services is the fact that they often need a large supply of tested and proven technologies based on their requirements and force structure, which directly affects the overall budget for them, and the competitive bidding mechanism. Order-of-magnitude scaling affects the cost, as does the diversity of the customer base.

While many debate the probability that initiatives like DIUx will succeed and last over the course of different administrations, defense leadership should instead focus harder on the right way to strengthen and use this initiative to complement and heavily influence the role of the primary U.S. defense contractors, particularly since the 2016 National Defense Authorization Act was passed and reinforced the importance of public-private partnerships. Even legendary Lockheed Martin's Skunk Works®, according to its own origin story,²³ was the result of an "unconventional organizational approach...challenging the current bureaucratic system that stifled innovation and hindered progress" to rapidly engineer and develop platforms to counter new foreign threats. Gone are the days when revolutionary

19 Davis, *Strategic Latency and Warning*, 2016.

20 "Homepage," *Defense Innovation Unit Experimental*, accessed Oct 28, 2017, <https://www.diu.xmil/>.

21 "Welcome to SOFWERX," *SOFWERX*, accessed Oct 28, 2017, <http://www.sofwerx.org/>.

22 "Homepage," *In-Q-Tel, Inc.*, accessed Oct 28, 2017, <https://www.iqt.org/>.

23 "Skunk Works® Origin Story," *Lockheed Martin*, accessed Oct 28, 2017, <http://www.lockheedmartin.com/us/aeronautics/skunkworks/origin.html>.

technologies like nuclear power or the internet are conceived and nurtured within the protective confines of government research labs and released into the wild.

With the strategic latency of cyber technologies fully engaged, the government now turns back to the private sector to manage the offensive and defensive consequences of its own offspring. The weaponization of cyber tools compelled the government to establish new military and civilian agencies to cope with latency. U.S. organizations like Cyber Command, or USCYBERCOM, respond to foreign innovations in the cyber domain. Part of the complexity we face is that nations, groups, and individuals will innovate to achieve their objectives based on different legal and ethical standards, possibly creating new weapon systems that are difficult for us to counter. According to DIUx's director Raj Shah,²⁴ partnering with Silicon Valley and sole-sourcing challenge-based contracts via co-sponsors from the various services is critical to match today's morphing military technology objectives with the appropriate capability.

The military strategist and historian Max Boot,²⁵ who recently served as an advisor to Senator Marco Rubio, described the advancement and disruptive nature of new military technology, such as the advent of chemical agents to break the stalemate of trench warfare in World War I. He perceives military innovation as a forced result of doctrinal loggerheads. Thus, "Revolutions in Military Affairs"²⁶ describes "periods when new technology combined with new tactics reshape the face of battle." Such revolutions occur as a natural function of a competitive battlespace, exemplified by the First Offset when the United States confronted an implacable enemy in the Cold War, the Second Offset that spawned the Revolution in Military Affairs (RMA) in the 1980s, and the Department of Defense's formalization of the Third Offset right now.

The task, however, is greatly complicated in the information age and will be more difficult as competitors like China and Russia²⁷ as well as non-state actors more quickly adjust their doctrine and promote new technological initiatives of their own as near equals. Additionally, since innovative research has become more privatized,²⁸ the likelihood that an emerging technology could compel us to develop additional countermeasures to fielded systems is a very real problem. We've already seen this occur in unmanned aircraft or aerial systems

24 Sydney Freedberg and Colin Clark, "DIUx: Will Carter's Innovation Unit Survive Trump?" *Breaking Defense*, November 16, 2016 accessed Oct 28, 2017,

25 "Experts: Max Boot," *Council on Foreign Relations*, accessed Oct 28, 2017, <http://www.cfr.org/experts/national-security-warfare-terrorism/max-boot/b5641>.

26 Anthony Cordesman, "The Real Revolution in Military Affairs," *Center for Strategic and International Studies*, August 5, 2014 accessed Oct 28, 2017, <https://www.csis.org/analysis/real-revolution-military-affairs>.

27 Guest Author, "Bear, Dragon & Eagle: Russian, Chinese & U.S. Military Strategies," *Center for International Maritime Security*, August 4, 2015 accessed Oct 28, 2017, <http://cimsec.org/chinese-military-strategy-week-comparing-russian-chinese-u-s-military-strategies/17803>.

28 Homepage," *National Science Foundation*, accessed Oct 28, 2017, <https://www.nsf.gov/>.

(UAS), additive manufacturing, and advanced cryptography.^{1,2,3} America's technological advantage is more contested than ever, by more adversaries operating in multiple domains.

These arguments bring us back to the importance and role for DIUx. It's hard to envision a near-term scenario where the U.S. military doesn't require large, uniquely complex platforms for the air, land, and sea domains it occupies, and it's hard to envision customers other than the military legally allowed to build and maintain a submarine or bomber, or the infrastructure required to maintain them.⁴ Raytheon, Boeing, and Lockheed aren't going away, nor is their unique association with the military. The enormity of the global surveillance-and-strike concept requires not only a whole-of-government approach, but an extension of resourcing and outreach far beyond historical examples to reach their technical objectives and mitigate growing operational risk.

The utility of DIUx does not revolve on the acquisition of large hardware, as it does on the soft and small. Simply scan the specifications requested for their Multi Drone Defeat System technology solution request as a prime example.⁵ This is why their approach should succeed if they maintain that focus. Novel technical innovations abound in the private world, particularly in the electronic and materials sector. The Third Offset centers around sensors, automation, and system integrations in multiple domains, particularly digital/information and space—areas that require a constant infusion of latent technical innovation from a diversity of sources.

Before Dr. Michael Vickers became the Assistant Secretary of Defense for Special Operations/Low-Intensity & Interdependent Capabilities, and later Under Secretary for Intelligence⁶ during the Obama administration, he was the CIA paramilitary intelligence officer responsible for conceptualizing the “weapons mix.” To fight the Soviets in Afghanistan, he described the use of a “symphony of different weapons...that would change the balance” by attacking Soviet weaknesses. Despite the seemingly overwhelming complexity of future warfare, we need a baseline from which to apply the appropriate “weapons mix” to specific regional conflicts, including those involving sub- and non-state actors. We need the instruments to field Vickers' symphony whenever and wherever circumstances require. This will require basic underlying technologies to support weapons

1 “UAV or UAS?,” *Unmanned Aerial Vehicle Systems Association*, accessed Oct 28, 2017, https://www.uavs.org/index.php?page=what_is.

2 Michael Lucibella, “Manufacturing Revolution May Mean Trouble for National Security,” *APS News*, April 2015 accessed October 27, 2017, <https://www.aps.org/publications/apsnews/201504/revolution.cfm>.

3 Hugo Zylberberg, “The Return of the Crypto Wars,” *Kennedy School Review*, March 12, 2015, <http://harvardkennedyschoolreview.com/the-return-of-the-crypto-wars/>.

4 “Homepage,” *General Dynamics*, accessed Oct 28, 2017, <http://www.generaldynamics.com/>.

5 “Tap Into a \$100+ Billion Market with Speed,” *Defense Innovation Unit Experimental*, accessed Oct 28, 2017, <https://www.diu.xmil/workwithus/#solution>.

6 Thom Shanker, “A Secret Warrior Leaves the Pentagon as Quietly as He Entered,” *New York Times*, May 1, 2015.

development appropriate to the battlefields of tomorrow, whether they are urban, underground, cyber, space, or hybrid in nature.

One of the main lessons from the Cold War, Offsets One and Two, and the Revolution in Military Affairs is the central role of the government in supporting the basic research and scientific expertise from which the benefits of civilian and military technology are derived. There can be no symphony without fine instruments and skilled musicians to play them. Domain dominance, although more complex, must be achieved through a weapons mix based on the acceptance that there will always be unforeseeable weaknesses in our techno-centric approach, and far more targets, which must be offset by a variety of tools available for the fight in each domain. The “tools” will range in nature from smart adaptations of century-old weaponry—like the semi-automatic pistol, claymore mines, and artillery shells—to more sophisticated, weaponized software bugs and drone swarms acting unconventionally.

It’s highly unlikely a “gold-plated” high-tech solution will ever meet the diversity of our requirements. We must not allow a preoccupation with advanced technologies to undermine strategies that usefully employ old weapons and familiar methods. In fact, this last argument is reinforced in the *Toward a New Offset Strategy* document presented by the DOD. For example, under the global surveillance and strike (GSS) description, the best mix of tools should be “balanced in that it would comprise a mix of low-end and high-end platforms aligned to widely varying threat environments—including advanced A2/AD challenges.”⁷

Regardless of political outcomes, the fundamental concepts driving the Defense Innovation Initiative will remain valid for coping with strategic latency. We should accept that future technologies, which play an integral part in the strategy, will converge over time in unforeseeable ways, and will be transformed and adapted (tactically) by competitors to gain advantage over our tools and strategies. Our adversaries will employ their own mix of technologies designed to exploit our vulnerabilities. Our weapons mix should be adaptable across domains based on the foresight that new weapons have their own technical vulnerabilities, as in the case of cyber and space weapons. In the end, our strategy and tactics will determine whether we can employ technology to provide strategic warning, project power, and defend the nation. Most importantly, we must prevent “a sudden tempest that turns everything upside down.”⁸

7 Martinage, *Toward a New Offset Strategy*, 2014.

8 Boot, *War Made New*, 6, 2006.

Chapter 17

Predicting and Guiding Change in the New Economy of Strategic Latency

Ben Forster

The global economy has changed dramatically, and with it the ability to predict what new technologies will emerge, where, and how they will be used has become increasingly unpredictable. The underlying assumption around strategic latency is that technological emergence does not occur in a vacuum. Macroeconomic considerations help us understand that disruptive security innovations—whether conventional or unconventional weapons—tend to occur within the capital input limitations of nations and in relation to their overarching economic growth objectives. From a purely statist, international-relations-theory perspective, states will seek to build economic power and develop technologies in response to external threats.

A look at the microeconomic ecosystems that surround free market innovation shows a more complicated picture with less economic predictability. Innovative ecosystems that are open to capital investments, an ability to challenge the status quo, intellectual property rights, and free competition fuel the creation of new technologies. The ability of national governments to influence both the pace and direction of disruptive security innovation is decreasing in many respects, leading to a diffusion of agenda-setting power to non-state actors. This is due to both the potent, disruptive potential of technologies being freely developed and also the structure of incentives leading to their development.

This is most readily apparent in the global information economy, and in particular the cybersecurity domain. Platform-based development, crowd-sourced innovation, and other factors that are restructuring the inputs and costs of innovation are the key drivers. At the same time, predicting how states will acquire and utilize technology is difficult to assess with any economic certainty. History has shown that how states decide what to acquire or produce and how to execute production is also not a clean, unitary phenomenon driven by

calculated security or economic interest. Security threats, corruption, and other subnational interests often override seemingly rational calculi, particularly concerning defense-related technology. Likewise, it's not clear that the traditional toolkit of influencing and guiding innovation will work in an increasingly decentralized information economy. As a capital-less economy sets a new precedent for how technologies are developed, closing both the gap between innovating and imitating nations while empowering non-state actors, the national security community will need to find novel ways to harness this process.

Understanding the Innovation Landscape— a Macro Perspective

Strategic latency and strategic disruption have primarily been concerned with security contests between states, and so it's fitting that we begin any discussion of the subject with a look at how national innovation occurs and states direct it. In order to understand how the innovation landscape has changed, it's important to revisit how it has been understood. The use of latent civilian technology in strategically disruptive ways requires several inputs, including technological knowledge, and physical and human capital. Human capital includes knowledge to utilize technologies including worker education and health while physical capital includes machinery and technology. Technological knowledge may include general understanding of factory production processes or proprietary research.⁹

Whether they are state or non-state actors, obtaining these ingredients occurs through one of two ways: the technology can be indigenously produced or acquired through the course of natural market diffusion, including imitation and theft. Economists, including Joseph Schumpeter, Edward Denison, and many others have long held that technological change remains vital to national economic growth.^{10,11} New ideas and technologies improve the efficiency of an economy's capital utilization, resulting in higher national output, greater investment in education, physical and human capital, in turn resulting in new technologies.

The rate at which countries make investments in pioneering innovative, cutting-edge technology becomes important as states reach the limits of their technological frontiers and have exhausted the low-hanging fruit of duplication.¹² States pursue balances of technological imitation and innovation based on capital availability, industrial efficiency, and their proximity to the technological frontier.^{13,14} Of course, utilizing diffused technology—

9 G. Mankiw, *Principles of Economics*, 4th ed. (Mason: Thomson Higher Learning, 2007), 557.

10 P. Menell, "Intellectual Property: General Theories," *Encyclopedia of Law & Economics*, ed. B. Bouckaert and G.D. Geest (Cheltenham, UK: Edward Elgar Publishing, 1999).

11 N. Rosenberg, R. Landau, and D. Mowery, "Introduction," in *Technology and the Wealth of Nations*, ed. N. Rosenberg, R. Landau, and D. Mowery (Stanford: Stanford University Press, 1992), 4.

12 B. Lindsey, Frontier Economics, Forbes, April 25, 2011, <http://www.forbes.com/sites/brinklindsey/2011/04/25/frontier-economics/>.

13 D. Acemoglu, *Localized and Biased Technologies: Atkinson and Stiglitz's New View, Induced Innovations, and Directed Technological Change* (Cambridge: Massachusetts Institute of Technology, 2014).

14 Lindsey, Frontier Economics, 2011.

whether commercial aircraft or toaster ovens—depends on that state’s available capital, including specialized knowledge and training, appropriate management techniques, or basic infrastructure like roads and machinery.¹⁵ A wide range of macroeconomic theories explains why and when technologies developed in one country diffuse to others. Commercial products begin their life in high-income markets, where an abundance of specialized capital and labor, seed financial investment, and early adopters that can provide continuous feedback allow products to be tested before they achieve economies of scale and standardization, after which production moves to lower-income countries to take advantage of cheap labor.¹⁶

Moreover, many economists have noted both a shortening of these product cycles as well as the adoption lag of these technologies between rich and poor countries.¹⁷ In other words, as technologies are developed in high-income countries, the rate at which they are adopted by “imitators” is likely closing. One possibility is that adoption lags are accelerating in certain industries like high tech while not in others. Futurist theories of exponential technological change, such as those of Gordon Moore and Ray Kurzweil, suggest that technological change and computing power are growing at an exponential rate. To this point, intellectual property right (IPR) protection will follow a path that balances the need to duplicate innovative foreign technologies to fuel economic growth in developing countries with the need to protect domestic inventions as national growth slows and domestic innovation becomes necessary.¹⁸

China’s recent economic focus on high-tech technology investments can certainly be explained by these theories. Their transition to a consumer-based economy is a reflection of their gradual move away from a country of solely abundant cheap labor to one of a higher skilled labor force. Commercial investments in things like computing technology and aerospace have spillovers to the development of military technologies like fighter jets, via new capital abundance in the form of machine equipment and a skilled workforce.

The literature on localized technological progress, directed technological change, and induced innovation has unpacked the determinants of innovation even further, examining the correlation between the types of technologies produced in an economy, and the factor supplies they utilize, including prices, workforce wages, and labor supply.¹⁹ Geographic clustering of entrepreneurial circles, including general workforce education, age, local industrial structures that contain labor pools of skilled workers, the strong influx of immigrants, and larger companies that can bleed talent to smaller ones all influence

15 Acemoglu, *Localized and Biased Technologies*, 2014, 11–12.

16 J. Gerber, *International Economics*, 4th ed. (Boston: Pearson Education, 2008), 73–74.

17 D. Comin and M. Mestieri, *The Intensive Margin of Technology Adoption* (Cambridge: Harvard Business School, 2010).

18 Y. Chen and T. Puttitanun, “Intellectual Property Rights and Innovation in Developing Countries,” in *Journal of Development Economics* 78 (2005): 476–477.

19 D. Acemoglu, “When Does Labor Scarcity Encourage Innovation?”, in *Journal of Political Economy* 188, no. 6 (2010): 1040.

innovation.²⁰ In fact, former Cisco CEO John Chambers attributed part of the failure of Wang and Digital Equipment to catch the market shift to PCs because they were both located in Maryland. Bill Gates made similar comments on Microsoft's lethargy in adjusting its products to the Internet because of the company's location in Seattle, not Silicon Valley.²¹

Filling in the Missing Dots—Microeconomic Considerations for Innovation

A cornerstone of what drives innovation is monetization—the ability to transform an idea into profit. Consistent with the earlier discussion on the tendency for economics to “black box” technology, microeconomic models have likewise had difficulty in explaining both why firms pursue innovation and the tangible gains it produces. In large measure, this is due both to the obvious “lack of standardization” in innovation and in determining a definitive threshold on what constitutes a fundamentally novel innovation, either a process or product.²² According to the neo-classical model of the firm, the primary incentive for R&D for the purpose of creating innovation is to maximize profit. Firms take into account the relative costs of these investments, profit potential, competitive differentiation, anticipated market share, and the potential value for customers.²³ Put simply, “...The incentive to innovate is the difference in profit that a firm can earn if it invests in research and development compared to what it would earn if it did not invest.”²⁴

The problem for innovation theories is that firms don't neatly follow this calculus. As economist William Baumol notes, although the economic profits of pursuing new products are often nil for firms, it is the necessity of maintaining a competitive edge and financial survival that drives innovation. It's a phenomenon, Baumol concedes, that is remarkably similar to an arms race (Baumol, 2002, p. 6).²⁵ Firms may go bankrupt in the end, but in a never-ending ladder to avoid the status quo, they have little choice; thus competitive markets drive innovative behavior. Firms are in a constant race to develop new ideas, go-to-market, and outpace the competition to deliver unique value for customers and avoid commoditization, although Joseph Schumpeter challenged this notion, suggesting instead that less than competitive markets drive firms' innovative behavior. Instead, larger firms are able to weather losses and diversify risk.

20 A. Chatterji, E. Glaeser, and W. Kerr, *Clusters of Entrepreneurship and Innovation* (Cambridge: National Bureau of Economic Research, 2013), 2–6, 10–16, <http://www.nber.org/papers/w19013>.

21 J. Chambers, “How We Did It: Cisco's CEO on Staying Ahead of Technology Shifts,” *Harvard Business Review*, May 2015, 37–38.

22 W. Baumol, “Towards Microeconomics of Innovation: Growth Engine Hallmark of Market Economics,” *American Economic Journal* 30, no. 1 (2002): 2.

23 Ibid.

24 R. Gilbert, “Looking for Mr. Schumpeter: Where Are We in the Competition-Innovation Debate?”, in *Innovation Policy and the Economy*, ed. A. Jaffe, J. Lerner, and S. Stern (MIT Press: 2006), 159–215.

25 W. Baumol, “Towards Microeconomics of Innovation,” 2002, 6.

This has been challenged empirically, as many small firms are the most active innovators and “absolute firm size is not necessarily beneficial to innovation”.²⁶ In fact, bureaucratic structures of large firms and risk aversion to changing business processes prohibit larger firms from investing in new innovations. After all, failed product launches in big firms have the propensity to fail publicly; smaller firms have the agility to explore an uncaptured market niche under the radar, while larger companies can eventually capitalize on this through acquisitions.²⁷

There are non-monetary incentives that drive innovation. Former Vice President of Motorola Toby Redshaw admits that much of what drives Silicon Valley innovation is akin to “organized gambling.” Innovation is less about marginal utility investment, though clustered ecosystems where R&D is part of the culture is a key ingredient. According to Redshaw, it’s a fear of falling behind competitors, an ability to accurately forecast where the next market opportunities will be, and the willingness to tolerate failure in an environment where products are developed and sold based on maximizing customer value and “driving out cost and complexity.”²⁸ Markets that are able to weather the rise and fall of firms in this often volatile innovation climate are conducive to innovation. It’s also reflective of the evolving understanding of how humans make boundedly rational decisions. The work of Daniel Kahneman, Amos Tversky, Richard Thaler and other behavioral economists have noted a whole host of innate psychological conditions, heuristics, and biases that make humans act in seemingly irrational ways.

Intellectual property right protection is important for firms at the micro level. A 2009 study of OECD countries found that intellectual property protection universally contributed to high innovation levels in surveyed states. However, while IP protection may encourage foreign inventors to flock, they may not encourage domestic innovation.²⁹ Still many of the most successful companies in Silicon Valley have embraced the ability to test iterations of early-stage products on potential customers before developing product lines and going to market. There’s no way to do that without having intellectual property right protections.

There are also sociocultural elements of innovation. In Asia, businesses are largely organized and reflective of the familial dynasties that have been a cornerstone of capitalistic economic development in the region. According to *The Economist*, giants like Samsung and Hutchinson-Whampoa reflect this dynamic. Family relationships ensure trust and company-wide unity of effort across sectors of the local economy and the world. Combining their ability

26 C. Greenhalgh and M. Rogers, *Innovation, Intellectual Property, and Economic Growth*, 1st ed. (Princeton: Princeton University Press, 2010).

27 S. Hogg, “Why Small Companies Have the Innovation Advantage,” *Entrepreneur*, November 15, 2011.

28 T.E. Redshaw in discussion with the author, August 20, 2016.

29 OECD, *Innovation in Firms: A Microeconomic Perspective* (Paris: OECD Publishing, 2009).

to mobilize resources, coordinate across industries, and ensure organizational stability, they are more likely to take investment risks and capitalize on them.³⁰

Innovating firms must have the freedom to disrupt the status quo, challenge existing technologies and methods of production, and embrace risk-taking. Authoritarian regimes or command economies may inhibit this process and continue their state's reliance on existing technologies.³¹ Israel's innovative culture has been tied to a combination of a strong educational system, government investments, sociocultural family dynamics, a culture of individual risk-taking, and diversity of ideas through immigration. Although many factors are at play, mandatory government service requirements may explain the recent boom in Israeli security innovation.³² The largely empirically discredited "great man theory of innovation" owes the emergence of radical new technologies to ambitious leaders and visionaries—Steve Jobs, Jeff Bezos, Elon Musk, or Thomas Edison. While strong visionary leadership has proven to be instrumental for the likes of Apple or Tesla, the reasons for the success of such men, women, or companies are even more the result of individualist cultures, or where the status quo can be freely challenged and where collaborative product development can occur.^{33,34}

Cybersecurity and the Information Economy—a Roadmap for Where Disruptive Innovation Is Heading

Much of the discussion has looked at innovation from the theoretical lens. The advent of the Internet of Things, crowdsourced innovation, and virtual platforms made possible by cloud computing have significantly reduced the costs for firms to produce goods and greatly revolutionized innovation. The conventional wisdom on effects of capital and labor abundance in driving particular technologies to emerge has become less relevant in an increasingly digitized economy without borders, where industries are amorphous, and everything is "glocalized." In what Jeremy Rifkin calls the zero-marginal-cost society, free software and globally available technological knowledge negate many of the traditional costs associated with production.³⁵ Thus the incentive structures for firms to undertake investments in R&D have changed dramatically.

If scientific discovery is built upon the shoulders of giants—generations of trial and error by thinkers and scientists—then modern giants may well be software-defined networking

30 Brett Ryder, "Asian Values," *The Economist*, April 18, 2015, <http://www.economist.com/news/special-report/21648174-worlds-most-dynamic-region-family-companies-occupy-commanding-heights>.

31 D. Acemoglu, U. Akcigit, and M.A. Celik, *Young, Restless and Creative: Openness to Disruption and Creative Innovations* (Cambridge: National Bureau of Economic Research), 1.

32 G. Shapiro, "What Are the Secrets Behind Israel's Growing Innovative Edge?," *Forbes*, November 7, 2013.

33 A. Schaffer, "Tech's Enduring Great Man Myth," *MIT Technology Review*, August 4, 2015.

34 J. Schrottke and T. Weber, "The End of the Great Man Theory of Innovation," *Bloomberg*, July 11, 2013.

35 J. Rifkin, "Uber and the Zero Marginal Cost Revolution," *Huffington Post*, November 3, 2014, https://www.huffingtonpost.com/jeremy-rifkin/uber-german-court_b_5758422.html.

and crowdsourcing. The opportunities for individual firms to find market niches and bring new ideas to market is accelerating. From NASA to Silicon Valley startups, organizations are turning to crowdsourced innovation, either subcontracting product development to independent consultants or through free open forums, significantly reducing the initial costs of the R&D phase of manufacturing. Sites like SourceForge, Bitbucket, or Github allow individuals to collaborate on building code. Google and Microsoft offer platforms for designers and engineers to work cooperatively across the globe without leaving their home. From YouTube and Coursera to a litany of online universities, free, on-demand knowledge is transforming the way people are educated. Blockchain and Bitcoin, as well as other anonymous currencies enable efficient, autonomous, and often untraceable market interactions.

All of this has flipped many, but certainly not all, traditional economic assumptions where firm clustering and constraints on physical and human capital and technological knowledge were essential ingredients to innovation. And while companies, especially those in high tech, rely on access to pools of human capital to fuel knowledge, the relevance of geographic location to innovation is diminishing. American startups sidestep visa requirements by outsourcing software engineering to teams of coders in Ukraine, Poland, or India. And without the need to keep seats, computers, and rented office space open for these “employees,” the concept of diminishing returns to physical capital is less relevant. Virtual machines and cloud-based software platforms all serve to replace physical capital.

To be sure, geographic clustering and “comparative advantage” in human capital are very much relevant. Central Eastern Europe including Romania, Bulgaria, and Hungary has seen a boom in successful high-tech security startups such as BitDefender, AVG, and ESET, to name a few. This is largely the result of strong national initiatives in STEM education. But

Buyers seek the best price; sellers ply their wares or skills to make the most profit. This scenario is subject to typical market forces, with prices rising when demand is high and falling when it is low. Over time, good products squeeze out bad ones, and high-quality brands can command premium prices. Mergers and acquisitions occur, and deals get made between market participants who know and trust each other. Innovation is constant, and new products thrive or wither depending on the judgment of the market.

the region has not yet achieved the large scale and sustainable boom of Silicon Valley, in large measure because of the lack of an “entrepreneurial ecosystem,” including access to financial investors, mentors, or education in business management, marketing, clients

to test early-stage products, and the other essentials of creating a successful business.³⁶ For this reason many of these early-stage startups have been acquired, or locally gifted programmers have been hired by Western firms. The combination of low economic development and asymmetric investments in science and math education has also turned this region into the global center of cybercrime. Even in a globalized innovation economy, there are still intangible benefits to being an innovator in an entrepreneurial climate.

These same trends appear to be manifesting outside of information technology. The growth of additive manufacturing, including household 3D printing, replaces much of the capital needed to produce everything from heart valves to firearm receivers. While additive manufacturing loses the economies of scale of mass production, requiring fewer parts reduces the costs and labor intensity of an initial build, and it allows increased customization—a feature that’s particularly concerning for strategic disruption. It also means that the era of phased product development will likely slowly disappear as new generations of any given product can be instantly designed and shipped to customers.

This is a cornerstone of the software world, where incremental product innovations like software releases can be instantly pushed to devices and services. The modular design and ease of construction in additive manufacturing means an inherent blurring of industry lines—a company can easily pivot between producing commercial items one day and defense equipment the next, since the same assembly lines and production processes can be used.³⁷ The proliferation of computer-aided design files (CAD), schematics, and designs provides the technological knowledge needed to use this physical capital. While an individual can readily produce conventional weapons like firearms, we may be far from unconventional technologies like nuclear weapons, where some key components are still tightly controlled from export.³⁸

But this new market behavior’s effect on strategic latency is most readily apparent in the cybersecurity domain, where the incentives for developing disruptive technology have changed. The black and frequently gray market for cyberweapons includes a litany of products and services. Some of these include initial access tools like exploit kits and “zero-day” vulnerabilities that can be used to gain access to computers or networks; nation-state-grade polymorphic malware which evades signature-based detection and behavioral recognition; service-based hacking or denial-of-service attacks; infrastructure for launching attacks including compromised web pages, secure virtual private networks,

36 B. Szabo, “How Central Eastern Europe is Transforming From Outsourcing to a Real Tech Hub,” *Forbes*, October 2, 2013, <https://www.forbes.com/sites/ciocentral/2013/10/02/how-central-eastern-europe-is-transforming-from-outsourcing-to-a-real-tech-hub/#36acbe221297>.

37 R. D’Aveni, “The 3D Printing Revolution,” *Harvard Business Review*, May 2015, 44.

38 A. Nelson, “The Truth About 3D Printing and Nuclear Proliferation,” *War on the Rocks*, December 14, 2015, <https://warontherocks.com/2015/12/the-truth-about-3-d-printing-and-nuclear-proliferation/>.

and encryption.³⁹ Moreover, these cyberweapons trade under normal market principles. As reported in 2014 by the RAND corporation:⁴⁰

With anonymous freelancers and organized collectives alike able to specialize according to their own comparative advantage, you have the makings of a highly efficient market. The risks for operating in this entrepreneurial environment are offset by increasingly sophisticated anonymization tools like Tor and unbreakable encryption. But not all of this market operates in the dark. Private and publicly traded companies, some of whom also conveniently sell anti-zero-day solutions, deal in an unregulated market of finding, buying, and selling vulnerabilities in commercial software in everything from Google Chrome to Windows operating systems. Firms operating in this ethical gray zone sell primarily to governments and law enforcement agencies and are paid in hundreds of thousands of dollars.⁴¹

By commercial market-economy standards, buying and selling exploit kits or security vulnerabilities in baby monitors, websites, and web browsers would not appear innovatively disruptive. In fact, these dynamics resemble characteristics of commercially disruptive technology. Clayton Christensen, Tom Bartman, and colleagues at Harvard Business School use a handful of criteria in assessing the disruptive potential of an innovation: the product opens the given market to customers who were pushed out by pricing; delivers a continually improving experience at a low price to customers; and opens the market segment to new “value networks” or the means of consumption.

Indeed we see many disruptive characteristics in these black and gray cyberweapons markets—low prices enable new entrants like “script kiddies” and hacktivists to launch damaging attacks with little or no technical knowledge; new supply chains and value networks have emerged in the form of often anonymous intermediaries, freelance developers, and brokers who can independently develop and sell to a satisfied customer base: governments and criminals. Attack methods that were once only available to the most advanced nation-states are now available for purchase by non-state actors.

In large measure this stems from the ability to monetize research and development. Decades ago there was little incentive for private researchers to spend countless hours poring over code in the hope of identifying obscure system vulnerabilities a software manufacturer may have missed—so called “zero days.” For one, systems weren’t as interconnected as they are in today’s Internet of Things, so the risks, and therefore payoffs for finding vulnerabilities, were inherently lower. Governments with teams of

39 National Security Research Division, *Markets for Cybercrime Tools and Stolen Data*, by L. Ablon, M. Libicki, and A. Golay (Santa Monica: RAND, 2014), 10, 34.

40 Ibid., 1.

41 A. Greenberg, “Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six Figure Fees,” *Forbes*, March 21, 2012, <https://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/#882a89d1f745>.

data scientists, mathematicians, and computer programmers could afford to identify these vulnerabilities, effectively at a financial loss, but they weren't highly targeted. But as computing technology proliferated and became widely commercialized, the ability to monetize these attacks has become more apparent. With this the incentives for private innovation changed drastically and, in apparent irony, are now bought by those same teams of government researchers. This is also partly reflected in the cost of production drop of what were once considered nation-state-grade cyberweapons.

According to security researchers, ten years ago the cost of producing Stuxnet⁴² was, by some estimates, somewhere in the range of hundreds of millions of dollars and required dozens of computer scientists. Similar malware can now be produced with close to a dozen specialists in the range of only \$10,000 in cost.⁴³ All of this is facilitated by a new market that obeys few of our classical views on innovation.

While it might be a stretch to consider malware development as truly innovative, on par with the cell phone or atom bomb, as more information becomes digitized, and more industries embrace IoT as a means of optimizing processes, the disruptive potential of these latent technologies increases dramatically. As Ron Lehman notes in the chapter on "Sputnik-like events," the tendency to react to new technologies in ways that may ultimately prove detrimental to our strategic edge is particularly relevant in a new innovation economy with new and more fluid market dynamics, and one that produces technology with greater weaponized disruptive potential, and has less stability and predictability. Cyberweapons to include malware, exploit kits, and vulnerabilities give an asymmetric advantage to state and non-state actors alike. A Syrian group's planting of a false story on an Associated Press Twitter feed caused stock markets to plummet, resulting in billions of dollars in market losses.⁴⁴ Cyberattacks targeting operations technology like SCADA systems and Programmable Logic Controllers (PLCs) have resulted in severe physical damage to industrial systems in Iran and Germany.

And predicting how these tools are used is even more difficult in an information age when everything can be weaponized. The gray market that has emerged is driven by various groups, including nation-states with geopolitical objectives, hacktivists with purely political ambitions, criminal groups bent on financial return, or terrorists. Each of these actors faces unique motivations, the entirety of which cannot be captured by a single theory alone.

42 Stuxnet malware disabled Iranian nuclear centrifuges in 2010. Its use marked the first time a cyberweapon had been able to cause severe damage to physical operations' technology systems.

43 P. Paganini, "Cost of conducting APT campaigns is dramatically dropping," Security Affairs, 2014, <http://securityaffairs.co/wordpress/22056/cyber-crime/apt-cost-dramatically-dropping.html>.

44 M. Fisher, "Syrian Hackers Claim AP Hack That Tipped Stock Market by \$36 Billion. Is It Terrorism?" *Washington Post*, April 23, 2013.

Lessons for the National Security Community—How Do We Predict, Manage, and Influence the Emergence of Strategically Latent Technologies?

From a practical perspective, given the myriad of factors and uncertainty over economic drivers of innovation, how can states—and particularly the national security community—encourage, shape, and contain this new form of technological innovation? The relationship between government and rest of the national economy is captured in the neo-institutionalist perspective on what Marina Ranga and Henry Etzkowitz term “triple helix systems.” While the concept has been around since the 1990s, it expands upon thinking of innovation economies as a purely one-to-one relationship between industry and government to a triadic relationship that incorporates universities as well.⁴⁵ Under statist configurations of this model, the national government plays the “leading role [in] driving academia and industry,” while simultaneously “limiting their capacity to initiate and develop innovative transformations.” These include authoritarian or command economies like China, Russia, and countries of the former Soviet Union.

By contrast, in laissez-faire systems such as the U.S., private industry is the primary driver of innovation while government and university R&D produce those technologies which private firms would not.⁴⁶ Ranga and Etzkowitz posit that a “balanced configuration” offers the best environment conducive to innovation. Here, the “university and other knowledge institutions act in partnership with industry and government and even take the lead in joint initiatives.” This fosters both economy-wide spillover effects and the mutual support of these institutions, which allows faster, higher payoff innovation through greater risk taking.⁴⁷

The developmental state model—pioneered in Japan and popularized in the developing world including China, Korea, India, and Taiwan—is an example of a command-economy approach to innovation. Under these systems the national government plays a more hands-on role in acquiring foreign technology, providing domestic businesses access to cheap capital, and carefully regulating the entry of foreign investment and technology “often with the goal of promoting positive spillovers into other industrial sectors,” cross ownership, and vertical integration within large industries.^{48,49} According to the McKinsey Global Institute, China’s rapid growth has been largely the result of capital accumulation, and in

45 Triple Helix Research Group, “The Triple Helix Concept,” *Stanford University*, 2013, https://triplehelix.stanford.edu/3helix_concept.

46 M. Ranga and H. Etzkowitz, “Triple Helix Systems: An Analytical Framework for Innovation Policy and Practice in the Knowledge Society,” *Industry and Higher Education*, 27, no. 3 (2013): 239–240.

47 Ibid.: 257.

48 Department of Government, *An Analysis of the Economic and Security Motives Behind Foreign Technology Theft: A Comparative Case Study in the Defense Industry*, by B. Forster (London: London School of Economics and Political Science, 2014).

49 National Research Council, *Conflict and Cooperation in National Competition for High-Technology Industry* (Washington, D.C.: National Academy Press, 1996), 25.

order to reach sustained long-run growth it will need to innovate.⁵⁰ Government-sponsored investments play a large role in this.

The lesson for China—learned during the Great Leap forward—was the limit of a command economy and that technological and capital development cannot exceed a region or state’s natural capacities. The country’s special economic zones (SEZs), which relax foreign trade and investment restrictions, were a move away from aspects of a centrally managed command economy. Today, China’s state-owned venture capital fund, Zhongguancun Development Group (ZDG), invests in international incubation centers to allow early-stage startups access to China’s market. Japan’s experience in the 1980s provides a prime example of successful directed investment. Its economy was organized around catching up with foreign competitors by maximizing technological diffusion between sectors of the economy, industries, and suppliers to a degree not matched by Western economic models (Samuels, 1994).⁵¹ When Japan sought to indigenously co-develop the FS-X, a spinoff of the F-16, it was because it “...pushes all the right industrial buttons—new materials, advanced technology, national prestige and fat contracts.”^{52,53}

At the same time, examples abound where states engaged in production of defense technology that served no seemingly rational economic calculus. At the time Pakistan began its nuclear weapons program in the 1970s and 80s, it had one of the lowest GDPs in the world, stagnant growth, and a dearth of capital. Its ability to create highly enriched uranium (HEU) and weapons-grade plutonium was the result of technological imitation and diffusion: a combination of foreign technology theft from developed countries, obtaining dual-use technology from clandestine trade with Europe, and direct assistance from China.⁵⁴ Nowhere in this story were the latest management techniques, intellectual property rights, or entrepreneurial clustering—this technological development was covertly isolated from the rest of the economy with few, if any, positive spillovers to civilian industries. More than anything Pakistan’s nuclear weapons program was a direct result of national will and the existential threat of a nuclear-armed India. President Zulfikar Ali Bhutto said at the time: “If India builds the bomb, we will eat grass or leaves, even go hungry, but we will get one of our own.”⁵⁵

50 E. Roth, J. Seong, and J. Woetzel, “Gauging the Strength of Chinese Innovation,” *McKinsey Quarterly*, October 2015.

51 R. Samuels, “Pathways of Technological Diffusion in Japan,” *MIT Sloan Management Review* 35, no. 3 (1994), <http://sloanreview.mit.edu/article/pathways-of-technological-diffusion-in-japan/>.

52 Department of Government, *An Analysis of the Economic and Security Motives Behind Foreign Technology Theft*, by B. Forster (2014).

53 K. Szymkowiak, “Profit is the Biggest Motivator: New Weapons Production Highlights Growth of Japan’s Defense Industry,” *Japan Economic Journal*, June 14, 1986: 7.

54 P. Kerr and M. Nikitin, *Pakistan’s Nuclear Weapons* (Washington, D.C.: Congressional Research Service, 2016), 3, <https://www.fas.org/sgp/crs/nuke/RL34248.pdf>.

55 Nuclear Threat Initiative, *Pakistan*, 2016, accessed June 18, 2016, <http://www.nti.org/learn/countries/pakistan/nuclear/>.

In part this is a reflection of the way states make their investment decisions. National and sub-national agencies are rational agents that assess their respective environments, and act accordingly to maximize budgets and lobby for state resources, a phenomenon captured in theoretical models of rent seeking, public choice, and organizational sociology.^{56,57} This is to say that while the issue of strategic latency is often viewed from an international-relations-theory perspective, the reality of how states determine security investments is often not economically rational, and states are not unitary agents. This is reflected in the “paradox” of China’s authoritarian economic and policy planning instituted in the mid-1990s. National level policies and investment strategies developed in Beijing are conformed to provincial level needs—either by national level intent or due to rent seeking—so that economic decisions include collusion amongst organizations in an effort to balance competing resource demands, power, and political wills within government institutions.

Hence even nationally mandated investments in technology may result in practically different outcomes. While rent seeking is hardly unique to command economies or authoritarian states, it is certainly more pronounced in these economies and even more so when dealing with defense technology investments. It’s no surprise that states pursue defense technology development when “they perceive heightened threats to their security,”⁵⁸ but when these threats are perceived to be non-existential, such as in times of relative peace, the influences of ideology and political alliance are better guides to where and how states will choose to invest and innovate in technology.

From an innovation perspective, China’s relaxing of once-strict investment regulations in parts of the country is a reflection of understanding that increasing the rate at which innovation can occur requires establishing a durable environment that can withstand the trial and error of innovation cycles. Command economies can produce one-off disruptive technologies, and are useful in facilitating economic catchup to more technologically advanced countries—through intellectual property theft and government-induced interindustry technological diffusion—but they lower the rate at which new technology and ideas can be generated.

The U.S. approach to shaping and guiding national security innovation has certainly paid dividends. DARPA and In-Q-Tel provide early-stage startup funding as well as mechanisms for testing early iterations of product design. National lab and university partnerships—such as Lawrence Livermore National Laboratory and University of California Berkeley—provide an important mechanism for transfer of ideas from public to private. Research partnerships allow for a robust development of human capital and innovation clustering.

56 Rent seeking is the process of lobbying for state resources, diverting productivity, effort, and resources away from utility maximizing activities in order to capture state controlled financial resources. As economist Robert Tollison notes, it is the “... idea that transfers are converted into social costs when individuals expend real resources and efforts to capture them.” See R. Tollison, “The Economic Theory of Rent Seeking,” *Public Choice* 152 (2012): 73–74, doi:10.1007/s11127-011-9852-5.

57 X. Zhou, “The Institutional Logic of Collusion Among Local Governments in China,” *Modern China* 36, no. 1 (2010): 53.

58 Arroyo Center, *Military Expenditures and Economic Growth*, by J. Castillo et al (Santa Monica: RAND), xii–xiii.

One of the challenges for the national labs has been a siloing of innovation developed from broader commercialization. The Department of Energy's 2016–2017 Technology Transfer Execution plan is a promising step toward fueling private-sector competitiveness with public sector R&D. This has been the modus operandi for developmental state economies like China, which have a “cozy” relationship between private firms, government agencies, and public research institutions, where the necessity of economic catchup with the West means doing anything to move technology from private to public (and vice versa). In the European Union and Israel, early-stage startup capital investments by the government and collaborative entrepreneurship events are successfully fostering innovation hubs.⁵⁹

How else can government influence this new innovation climate? According to Peter Howitt, “...economic policies with respect to trade, competition, education, taxes and intellectual property can influence the rate of innovation by affecting the private costs and benefits of doing R&D.”⁶⁰ Acemoglu & Finkelstein's 2006 study of the medical sector showed that increases in labor prices via government regulation are shown to increase the adoption of new technologies, suggesting that policies that raise capital-labor ratios in heavily regulated industries may spur innovation.⁶¹ Applied to the defense industry, this might include tax cuts for specific areas of research and development in the defense industrial base, relaxing of foreign labor restrictions—including easing the availability of work visas—foreign investment, seed investment capital for companies producing critical technologies, or tax increases in other industries to offset cuts in others.

There are significant challenges to these approaches. First, neither of the United States' two most successful innovation hubs—Silicon Valley or Route 128—could be considered a result of intentional government planning, although research institutions and companies in both clusters have certainly benefited from government subsidies.⁶² The positive effects of government controls on innovation are consistently difficult to measure: while strict government measures have prohibited the full entry of companies like Uber into France, less stringent regulation and high demand have outpaced similar restrictions in the U.S.⁶³ Hence it might be difficult, if not impossible, to pinpoint an economic model that explains why, when, and how strategically disruptive technologies arise.

59 B. Szabo, “How Central Eastern Europe is Transforming From Outsourcing to a Real Tech Hub,” *Forbes*, October 2, 2013, <https://www.forbes.com/sites/ciocentral/2013/10/02/how-central-eastern-europe-is-transforming-from-outsourcing-to-a-real-tech-hub/#36acbe221297>.

60 P. Howitt, “Endogenous Growth,” in *The New Palgrave Dictionary of Economics*, ed. S. Durlauf and L. Blume (New York: Palgrave Macmillan, 2008), 1.

61 D. Acemoglu and A. Finkelstein, *Input and Technology Choices in Regulated Industries: Evidence from the Healthcare Sector* (Cambridge: National Bureau of Economic Research, 2006), accessed September 2015, <http://www.nber.org/papers/w12254>.

62 A. Chatterji, E. Glaeser, and W. Kerr, *Clusters of Entrepreneurship and Innovation* (Cambridge: National Bureau of Economic Research, 2013), 22, <http://www.nber.org/papers/w19013>.

63 P. Coy, *The Bloomberg Innovation Index* (2015), accessed July 7, 2016, <http://www.bloomberg.com/graphics/2015-innovative-countries/>.

But if Israel's rise to prominence in the cybersecurity industry offers any insight, it is that a combination of external security threats, a permissive entrepreneurial culture and government investment in science and education can produce "surprising" and rapidly growing technological innovations.⁶⁴ This suggests that external threats are a major factor in the pursuit of technology, and in this case it is expected that not all such technological adoption or pursuit will be economically sound. When threats are low, we are more likely to see development of technologies that satisfy domestic political, ideological, and/or economic needs.⁶⁵

The picture becomes more complicated in the largely unregulated and poorly understood information (cyber) economy, where the greatest rate of strategically disruptive innovation is occurring. It's not clear how any of the conventional economic tools of spurring innovation apply to this new economy of disruptive innovation. Tax incentives mean little in a globally decentralized network where new comparative advantages emerge. For example, national investments in STEM education coupled with intended or unintended restrictions on economic incentives to innovate—intellectual property protection, political stability, immigration restrictions, or taxes—may result in brain drain to other countries.⁶⁶ Intellectual property right enforcement is difficult, if not impossible: who owns the property and what laws apply? How can enforcement be carried out?

In China and Russia, with regards to cyberspace, the solution has been covert coopting and partnerships with independent hackers or collectives by state intelligence agencies. The FBI's recent indictment of Russian FSB agents and freelance hackers for breaking into Yahoo is telling of this connection, and of how using freelancers as proxies can have unintended consequences. Much like the use of privateers by imperial navies during the 17th century, writs of endorsement can serve as a valuable projection of force where the government cannot maintain a sustained presence. And in the case of both China and Russia, this has been shown to be an effective and, for the most part, controllable tool. But while states use non-state actors for operational purposes, it's not clear there has been any control over cyberweapons development or containing this innovation in any positive way. In what is effectively a tragedy-of-the-commons dilemma, states' participation in these innovation markets for short-term security gains fuels market incentives that may end up undermining their own national security through uncontrolled proliferation.

It's also indicative of the decentralized way states make investment decisions. In absence of comprehensive national or international policies that govern this largely covert market, it's likely that individual agencies make unilateral decisions to participate to the detriment

64 P. Suci, "Why Israel Dominates in Cyber Security," *Fortune*, September 1, 2015, <http://fortune.com/2015/09/01/why-israel-dominates-in-cyber-security/>.

65 G. Whitten and L. Williams, "Buttery Guns and Welfare Hawks: The Politics of Defense Spending in Advanced Industrial Democracies," *American Journal of Political Science* 55, no. 1 (2011): 117–134.

66 C. Stokes, "The Trump Effect: the US is Heading for a Tech Brain Drain," February 24, 2017, <https://venturebeat.com/2017/02/24/the-trump-effect-the-u-s-is-heading-for-a-tech-brain-drain/>.

of long-term national security interests. This is an economic and policy precedent that will set the tone for future markets that emerge around technologies like biohacking. It took decades after the first commercial computers were invented for hackers to take an interest in breaking into them. Once this occurred (in 1990s–2000s) it took almost another ten years for signature-based antivirus to lose its relevance (hackers were bypassing it).

As industrial manufacturing and the Internet of Things become increasingly interconnected to increase production efficiency, the market for disruptive innovation will shift again. As product cycles shorten, computing power improves through advances in machine learning, and the adoption lag between countries—the time until commercial products developed in one place saturate the global marketplace—shrinks, this innovation is likely to happen at an increasingly rapid pace.

As former General Stanley McChrystal noted: “It takes a network to defeat a network.” It certainly takes a network to innovate like one. The private-sector solution for much of this innovation has been to co-opt this human capital. Charlie Miller and Chris Valasek, who famously hacked a Jeep Cherokee, were hired by Uber. Google has similarly hired teams of formerly freelance hackers to find bugs and vulnerabilities in their products. The government has been slow to adopt this approach. While the Department of Defense recently hosted a “Hack the Pentagon” bug bounty program, the participants went through intensive background investigations, which has historically discouraged many researchers.

Clearly it’s not feasible to open the floodgates on federal hiring. But the U.S. government needs a new approach to guiding—not controlling—the inevitable innovation that’s occurring, and it needs to find it fast. A key lesson from behavioral economics and psychology is that humans will always act in their own interest. Understanding the financial and non-monetary incentives that now guide independent innovation, we must understand that this cannot be choked—nor should we want it to be. Policymakers’ responsibility should be to guide this innovation responsibly. Improved grassroots education in schools, coding, and basic internet literacy are much needed and would be instrumental in fostering the right human capital for guiding this new market innovation.

This new model of decentralized innovation serves as a potential model for understanding other forms of potentially disruptive latent technology. A key lesson for issues of strategic latency is to watch the market incentives. Where actors can successfully monetize research and development efforts, expect not only existing technology, but innovation to proliferate. How actors use this technology is another question entirely.

Conclusion: Can Economics Predict When and Where Strategically Disruptive Technologies Emerge?

This chapter began with a consideration of the macro and microeconomic factors that drive innovation in countries. It’s looked at how innovation has been understood in the theoretical sense and how it’s evolved in the information age to produce novel,

unpredictable, and more potent technologies. A macro perspective has traced the emergence of new technologies by virtue of how their respective factor inputs are influenced, where countries have greater labor or capital inflows that support local factors of production, free trade, higher development levels, and a balance of imitation and intellectual property rights protection. Thus, historically, disruptive technologies tend to emerge in countries with more of these inputs while developing countries tend to imitate in an effort to catch up economically.

A more micro perspective has shown that “creatively destructive” ecosystems that permit trial and error and open competition fuel innovation. At the same time there are intangible microeconomic incentives for innovation that states must foster in order to produce greater rates of novel technologies. Although there are clear microeconomic incentives for firms to innovate, the literature suggests that these will be realized, perhaps unsurprisingly, in states with political stability, balanced IPR protection, and a culture of supporting “creative construction.”

In many ways though, this paradigm is shifting. In an increasingly globalized world where physical capital is being replaced by digital ecosystems and platform-based disruption, geography, and hence state-centric approaches to predicting the emergence of disruptive technologies, is less relevant. In Central Europe, a disruptive system of high-tech cybersecurity startups has emerged in countries with low levels of economic development and national infrastructure. This is largely a result of government investments in STEM education.

At the same time, history has shown that nationally directed investments in strategically disruptive technologies are difficult to predict by any economic calculus. This is because they may be covert in nature, driven by overwhelming political forces, and may have highly limited spillovers beyond a handful of industries that hold political value. In cases where strategic international competition, external threats, or realpolitik are at play, we would do better to use theories of international relations rather than economic rationality to determine where and what types of technologies will emerge.

This is especially true in countries like China where balance-of-power shifts between national-, state-, and provincial-level government decision-making means that national-level economic policies and investments are in constant flux as they respond to each level's preferred outcomes. Rational subnational units invest and behave in a value-maximizing way, but certainly not in unison.¹ This is apparent with defense spending which, whether in war or peace, is driven by a combination of internal rent seeking and external threats that are difficult to predict with economic theory.

When we overlay the realities of a changing economy with how states actually make investment decisions, it's apparent that the new disruptive technology landscape requires

1 X. Zhou, “The Institutional Logic of Collusion Among Local Governments in China,” *Modern China* 36, no. 1 (2010).

new mechanisms for guiding and influencing it. The lesson from the defense industry and command economies is that nationally directed investments sometimes work and many times don't. In an economy that is increasingly behaving more like a decentralized network, the national security community must also behave more like a network. As Guy Kawasaki notes, successful innovation comes from listening to your customer—and letting them show you new ways to use your product.

Chapter 18

Closing Thoughts: Humanity, Machines and Power

Zachary Davis and Michael Nacht

A confluence of mega-trends is shaping the political-military-social context within which technology is taking its course. Shared perspectives on these trends can be found in other studies, such as the CIA's Global Trends and other future forecasts.² Areas of agreement include: the acceleration of scientific discovery, the speed of business, the difficulty of tracking R&D in multiple fields and the complexities created by multi-disciplinary convergence, the inability of governments to keep pace with these trends—much less make timely decisions about them—the implications for future warfare, and the benefits that humankind is reaping from technological progress. There is also broad agreement on the potential for technology to do great harm. At the core of these macro-level trends is the human spirit, expressed through individual and collective actions. Excessive focus on technology, we found, risks overlooking the human impetus that creates and uses these tools.

Our Strategic Latency Group noted that sovereignty and the role of states in shaping the global commons is changing, although we did not endorse the idea that current trends in globalization are hastening the dispatch of nation-states to the dustbin of history. Although technology is empowering individuals and groups, states remain the central actors in matters of war and peace, despite the difficulties governments face in controlling technology and its harmful effects. For the foreseeable future, national governments will be responsible for protecting their populations from technology threats. This fact reinforces the importance of S&T intelligence to provide strategic warning and the value of recent efforts to energize defense procurement processes.

² Office of the Director of National Intelligence, *Global Trends, Paradox of Progress*, <https://www.dni.gov/index.php/global-trends-home>; The Atlantic Council, *Our World Transformed: Geopolitical Shocks and Risks*, <http://www.atlanticcouncil.org/publications/reports/our-world-transformed-geopolitical-shocks-and-risks>; Center for New American Security, *Game Changers: Disruptive Technology and US Defense Strategy*, <https://www.cnas.org/publications/reports/game-changers-disruptive-technology-and-u-s-defense-strategy>.

The Red section of the book examines the analytic challenge governments face when trying to understand foreign technology threats. The White section looks at how technology is changing the overall security landscape. The Blue section assesses how the U.S. government goes about acquiring technology for its national security needs.

To what extent is technology driving the forces of change, as opposed to channeling or facilitating them? Our group was divided on possible causal relationships between global mega-trends and technology

You can design and create, and build the most wonderful place in the world. But it takes people to make the dream a reality.

—Walt Disney

drivers behind those trends. Perhaps predictably, technologists within the group tended to place higher causal influence on technologies, social scientists were uncomfortable about speculating due to a lack of data (but speculated nonetheless), and our private-sector colleagues were firmly grounded in business-oriented pragmatism. However, there was broad recognition that classical concepts of war and peace, and the ability to distinguish between them, are being challenged, in part due to technology.

“Hybrid” and “gray zone” conflicts may not have clear beginnings or endings, and the identities of actors and their interests are often unknown. Distinctions between offense and defense have become similarly murky as borders lose their coherence as physical and symbolic barriers, and definitions of ownership and identity slip the bonds of established thought. Technology may not be single-handedly leading the way to the future, but few would argue that it’s not one of the chief drivers of change.

Technology is simultaneously enhancing and corroding traditional levers of state power. Basic concepts of international politics such as “hard” and “soft” power, economic leverage, and traditional diplomacy are increasingly dependent on technological means. Everyone must compete with contending “narratives” backed by unconventional instruments of power. Public discourse is especially susceptible to global media. Official statements about everything from bomb damage estimates to measures of economic growth are increasingly contested, with no single voice viewed as authoritative. In the sciences, seemingly ingrained concepts such as peer review and evidentiary process have been called into question, less by religious orthodoxy of the type that challenged Copernicus and Galileo, but more by political factions who find it useful to portray science and technology as representing elitist proclivities. The legitimacy of science itself has fallen victim to postmodern interpretations, even while the fruits of scientific research are eagerly embraced by global markets and consumers.

Who can be trusted to explain the complexity of quantum computers or gene sequencing and their implications for national and international security? Wes Spain’s chapter shows how technology threats can be exaggerated and marketed to advance budgets and careers, further undermining public confidence in official assessments. The provocative essay by Daniel Tapia-Jimenez turns deconstructivist ideas on their head to offer an actor-network

perspective on technology and national security. These authors show us new ways to think about strategic latency by questioning basic assumptions while at the same time respecting the corpus of knowledge that has been assembled over the course of generations.

Changes in the way people view science and technology reflect the decentralization of power from the states and institutions that have defined world order to a newly emerging ecosystem of rising actors. Paul Bracken highlights this point in his chapter, arguing that the old order cannot accommodate the power shifts that technology is facilitating. In this new environment, international norms of behavior, especially those intended to manage the global commons, are increasingly difficult to maintain and perpetuate. Even established norms against nuclear proliferation and chemical weapons use face daunting futures. Global norms for newer technologies in the realms of nano, bio, cyber and space sciences may be even harder to establish and maintain as the great powers that championed global rules become less willing and able to enforce them.

The international relations scholar Hedley Bull coined the term “anarchical society” to describe the controlled chaos of the Cold War global order.³ The next iteration of world order appears to be even more anarchic, less governed, and massively complex, with more diverse centers of concentrated power less inclined to promote and enforce system-wide rules. With technology being increasingly accessible to more competing groups and individuals, James Canton, the author of *Future Smart*,⁴ warns that individuals and organizations that do not embrace strategic latency will be overtaken by events, lacking the tools required to compete for economic, political, military, and cultural advantage. Viewing world politics through the lens of strategic latency, S&T represents a distinctive form of power. This book is an effort to define the contours of S&T power and contextualize it within the current international security landscape.

Within that landscape, longstanding norms of ethics that guide scientific research, including prohibitions against the use of human and animal subjects, intellectual property rights, peer review, and scientific methods, may not be universally shared by newcomers vying for competitive advantage. The chapter by James Giordano and his team about neurobiological research in China illustrates some of these disconcerting trends. The potential application of properly and improperly derived scientific knowledge for military purposes follows from a broader breakdown of shared values of acceptable behavior, including anachronistic prohibitions on biological “weapons.”

How can the old system of multilateral treaties and technology control lists withstand the onslaught of innovation from individuals and groups armed with state-like R&D capabilities? Jennifer Snow argues that engagement with the outliers who are exploring the cutting edges beyond the bounds of governmental authority is our best option. For Snow, the

3 Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (New York: Columbia University Press, 1977).

4 James Canton, *Future Smart: Managing the Game Changing Trends That Will Transform Your World* (Philadelphia, PA: Da Capo Press, 2015).

formation of self-regulating communities provides an emergency alarm system—a canary in a coal mine—that will call attention to immoral and dangerous research within the hacker/maker/DIY movements. Will such decentralized and democratized entities enforce familiar governing principles for ethics and morality in S&T, or form new understandings of what is permissible?

The Strategic Latency Group debated but came to no conclusions about the role of cyber-connectivity and new media in redefining the

Men have become the tools of their tools.

—Henry David Thoreau

security architecture of the world. While developments in the cyber world over the last decade illustrate the core concept of strategic latency, we were divided on the significance of the threats posed by state and non-state cyber machinations. Some view the Internet of Things and the potential predictive power of big data as revolutionary and strategic, while others in the group view them as incremental and tactical in nature. This was surprising in light of real-world developments in “fake news,” hostile political influence operations, and the pandemic of cyber hacking that took place throughout the course of the Latency Project. Our hesitance to venture definitive assessments might be explained by Zhou Enlai’s perhaps misunderstood response to Henry Kissinger’s query about the merits of the French Revolution: “It’s too soon to tell.”

We are in the early days of understanding the political effects of cyber-connectivity, but the evidence of strategic effects is growing in case studies of the Arab Spring, the Color Revolutions, and Russian meddling in the elections of 2016–17. Nevertheless, while recognizing the growing influence of networked actors in politics, we did not concur with the view that global social networks have fundamentally redefined power alignments, as some have argued.⁵ Our definition of strategic would require such social networks to directly challenge the hard power capabilities of the primary actors within the state-centric structure. It is not clear that the erosion of state power that has been achieved by cyber-based actors will necessarily harken an historic realignment of the international system.

Many of the same qualifications apply to the revolutionary effects of artificial intelligence on security affairs. Our group was divided on whether AI qualifies as a true strategic game changer. While nobody disputes the proposition that knowledge is power, we differed on the significance of the insights and control mechanisms made possible through AI, machine learning, and big data. While several authors aligned themselves with the view that AI and related developments should rank near the top of the all-time greatest hits of strategic latency, others were not persuaded that the reliable data streams required for predictive capability or operational reliability are currently available. Nevertheless, we found consensus in the major theme of convergence in which AI is combined with

⁵ Ann Marie Slaughter, *The Chess Board and the Web: Strategies of Connection in a Networked World* (Hartford: Yale University Press, 2017). Another perspective along these lines is expressed by Ayesha and Parag Khanna in their *Hybrid Reality*, referenced in the introduction.

other technologies to form new capabilities that are widely applicable to national security problems. For example, the combination of AI-controlled swarms of autonomous vehicles armed with unconventional weapons might provide unprecedented battlefield advantages, but still might not match the destructive power of the atomic bomb, as Joseph Pilat argues in his chapter.

With the erosion of state power, hopes for global governance of cyberspace appear to have been overtaken by individual, group, commercial, and national desires to use these tools without restraint. Jen Snow may be right that nations need expert help from white- and gray-hat hackers to navigate these uncharted territories, including the dark web and its environs. Several group members cited the role of witting and unwitting technological proxies in the cyber realm as a particularly fertile research area, especially regarding their employment by state actors. Contractors, NGOs, hackers, and corporate entities are all competing to advance their multi-faceted interests in cyberspace. How do we measure the net effects of groups like Anonymous, Kaspersky Labs, or ISIS on national and international security? Measuring strategic latency and its effects remains high on our priority research list.

The chapter by Davis and Nacht on terrorist technology innovation offers a tentative conclusion that internet communications may be a force multiplier for terrorists, but don't qualify yet as a true game changer. In terms of strategic effects, innovations in simple mine warfare were reinvented as improvised explosive devices that have proved a vexing counter to U.S. technological superiority. This point is aptly elaborated by David Chu, who reminds us that new is not always better. Old, familiar technologies can be strategic when aligned against the enemy's weaknesses. Chu argues the same holds true for U.S. defense policy today, when so many influential thinkers advocate a full embrace of the latest and greatest technologies, many of which have inherent strategic vulnerabilities, such as reliance on GPS, the internet, or global supply chains that can be disrupted. In many cases we may be trading one set of dangers for another. New is not always better for Blue, or necessarily more threatening for Red. Innovative countermeasures are often effective.

With respect to the future of warfare, we are well situated at Lawrence Livermore National Laboratory to gain insight into recent developments in robotics, 3D printing, unmanned vehicles, drone swarms, missile defense, space, lasers, advanced materials, cyber, and other defense technologies. As a nuclear weapons lab, we are committed to the deterrence mission and exploring ways to prevent adversaries from challenging our deterrence posture. Joseph Pilat's chapter reminds us of the enduring priority of this mission, which will not be superseded by other forms of military conflict. One trend in this arena involves the effort to design an integrated suite of defense technologies to enhance deterrence. Sometimes referred to as "cross domain" deterrence⁶ or "integrated strategic deterrence," it is a renewed effort to combine an optimal mix of conventional, defensive, and nuclear

6 Center for Global Security Research, "3rd Annual Cross-Domain Deterrence Seminar: Towards Integrated Strategic Deterrence" (summary report, Lawrence Livermore National Laboratory, November 15–17, 2016). https://cgsr-dev.llnl.gov/content/assets/docs/CDD_Report_Nov_2016_FINAL.pdf.

capabilities designed to persuade aggressors against attacking vital U.S. interests. The growing emphasis on space and cyber assets figures prominently in this emerging calculus, and thus involves many aspects of strategic latency.

Another dimension of deterrence receiving renewed attention is the role of U.S. allies in extended deterrence partnerships.⁷ Any thoughts that nuclear weapons were declining as tools of state power have been sidelined by renewed investments in nuclear arsenals by Russia, China, India, Pakistan, and North Korea. This doubling down on nuclear weapons triggered the need to reassure allies such as Japan, South Korea, and NATO, who are concerned about being the target of nuclear intimidation, of America's ongoing commitment to extended deterrence. One sign of that commitment is the modernization of aging Cold War weapons and infrastructure to incorporate new technologies. Modernization could also reduce costs by replacing aging Cold War production methods with more efficient, automated systems, as in other industries. Such modernization has been held in check partly by hopes that restraint by the U.S. would inspire other countries to exercise a similar de-emphasis of nuclear weapons. Unfortunately, there is no evidence that this has worked, and leaves America facing tough choices about right-sizing its nuclear enterprise, from its R&D base to the weapon production infrastructure, command and control systems, and replacement of vintage delivery platforms that constitute the strategic triad. As much as technology is changing security around the world, nuclear deterrence and the prevention of nuclear war merits special status as the original poster child for strategic latency.

Beyond deterrence, how will warfighters of the future be equipped to prevail in circumstances in which the enemy may be indistinguishable from non-combatants, may inhabit urban mega-cities, and may not abide by recognized rules of conduct in warfare? U.S. Special Operations Command (SOCOM) has taken the lead in defining so-called "hybrid" or "gray zone" conflicts.⁸ The wars of the future may be radically different than those of the past, and will require updated intelligence, organization, and technologies to fight and win. New operational concepts and decision-making processes are needed to develop and employ the drone swarms, unmanned vehicles, robotics, space assets, cyber tools, and other new weapons that are being imagined as part of the Third Offset.⁹

The complexity that comes with these new forms of warfare will be added to—but not replace—the already challenging circumstances in which we find ourselves. Traditional armies fighting with tanks and terrorists wielding AK-47s are not going away as strategic latency produces new means of conflict. Our strategy must discriminate between the complex threats of today and apply appropriate means to defeat them. As Ron Lehman shows in his chapter about the lessons of Sputnik and the American response, a robust

7 Brad Roberts, *The Case for Nuclear Weapons in the 21st Century* (Stanford CA: Stanford University Press, 2016).

8 United States Special Operations Command, "The Gray Zone" (white paper, September 9, 2015).

9 Bob Work, "The Third US Offset Strategy and its Implications for Partners and Allies" (speech, Willard Hotel, Washington, D.C., January 25, 2015). <https://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/>.

R&D base supported by a strong economy provides the means from which to craft calibrated military strength. The best defense against foreign strategic latency is a deep wellspring of homegrown strategic latency that can be harvested in times of need.

The essays in the Blue section focus on US efforts to develop and procure the most appropriate technologies for future warfare, including intelligence needs. Former officials Frank Gac, Timothy Grayson and Joe Keogh take stock of government innovations intended to speed acquisition of advanced technologies. Their chapter provides an assessment of what innovations have worked well and which have fallen short. Lisa Owens Davis shows how the national laboratories can fill a gap between pure research pursued by academic institutions and profit-oriented defense contractors. Together, these chapters offer ideas about how to focus and shorten the procurement labyrinth. Economist Ben Forster echoes David Chu's warning about the hidden costs of cutting-edge technologies that may make sense from an innovation and market perspective, but often carry unanticipated consequences for the government. Similarly, Blanken and Lepore show how rational game-theoretic solutions to defense technology requirements can backfire and leave warfighters with inadequate or ill-suited weapon systems. Their model reminds us that all countries have access to global technology markets, making it extremely difficult for one state to maintain technological superiority for long.

Brian Holmes takes a broad strategic perspective that advocates a calculated mix of weapons that are custom-fitted to specific objectives. He sees the current DOD procurement experiments such as DIUx and SOFWERX as a step in the right direction of matching specific technologies to concrete military objectives. Toby Redshaw, however, counsels caution for those who embrace private-sector ethos and business practices as a means to satisfy government defense needs. He agrees with Holmes on the need for targeted outcomes but advocates limited, incremental and accountable business innovations to protect taxpayers from the type of failures that are integral to the private tech sector. One theme on which we all agree is the need for new models of public-private partnerships in defense technology.

Future warfare undoubtedly holds many surprises, some of which may qualify as having strategic effects. Strategic surprise is a certainty. Our group considered various unconventional scenarios involving the use of novel weapons and tactics by states, groups, individuals, proxies, and commercial entities. Free to speculate, we conjured a wicked brew of sinister drone swarms, AI-guided cyber bots, laser beams, incapacitating agents, pervasive surveillance, neural messaging, and space weapons, employed to produce a variety of dystopian futures. With global norms in retreat and access to advanced S&T growing, more actors could be increasingly willing to contemplate the unthinkable, including mass casualties. It is not hard to imagine an abundance of terrible innovations capable of great harm, some of which might actually come to pass. How should the U.S. deter and defend against such eventualities?

None of the troubling scenarios we imagined would occur, however, without identifiable human beings driving events. From the initial spark of innovation that produces a tool,

through the harnessing of latent potential for peace or war, latency is about people. The overarching theme of this book is the inescapable human element in creating and actualizing strategic latency. To understand Red capability, follow the people. The secret to the White section is strategy, doctrine, and politics. Blue is about organization, economics, and process. At every stage, the independent variable is people, with all of their quirks, beliefs, foibles, prejudices, and unpredictability. Strategic latency is a marriage between human and machine, only comprehensible through deep knowledge of both sides of the union.

Author Biographies

Jacob Andriola

Jacob Andriola is a J.D. Candidate at American University's Washington College of Law focusing on intellectual property and international law. He has a B.A in philosophy from The College of New Jersey with a specialization in law and ethics. Currently, he serves as an intern with the Legal Services Corporation and a research associate with the Neuroethics Studies Program of the Pellegrino Center for Clinical Bioethics of Georgetown University Medical Center, Washington, DC.

Rebecca Balebako

Rebecca Balebako is an information scientist at the RAND Corporation. Balebako is interested in technology and policy, and how our digital lives and actions transform society. Her research includes communicating the privacy and security risks of technology to consumers and understanding the roles and risks of new technologies. Her work is at the intersection of computer science, machine learning, human decision-making, and behavioral economics. Before her doctoral studies, she was a software engineer and product manager at startups and universities for over a decade. She has a Ph.D. in engineering and public policy from Carnegie Mellon University, an MLA in software engineering from Harvard University, and a BA in mathematics from Mount Holyoke College.

Leo Blanken

Leo Blanken joined the Defense Analysis Department at the Naval Postgraduate School in the summer of 2008. He received a BA from the University of San Francisco, an MA from Columbia University, and a Ph.D. in political science from the University of California at Davis. His dissertation on patterns of imperial expansion received the best dissertation award from the Western Political Science Association, and has been published by the University of Chicago Press as *Rational Empires: Institutional Incentives and Imperial Expansion*. He also has a co-edited book on Georgetown University Press entitled *Assessing War: The Challenge of Measuring Success and Failure*.

His current research explores the impact of agent incentives within the dynamics of force structure planning, strategy, intelligence, and assessment in emerging conflict environments. Leo is a USA Boxing certified trainer and helps kids learn the basics of boxing by volunteering at Pacific Coast Boxing in Pacific Grove, CA. He also collects and DJs rare soul and funk records from the 1960s and 1970s. He is part of the Soul Lotto crew of DJs based in England, and some of his sets can be accessed at www.soulotto.com.

Paul Bracken

Professor Bracken is professor of management and political science at Yale University. He is the author of *The Second Nuclear Age*, *Managing Strategic Surprise*, *Fire in the East*,

The Command and Control of Nuclear Forces and many other books and articles. Bracken is included in Princeton Review's current book on "The Best 300 Professors" in the United States.

Professor Bracken often leads business war games for companies and governments facing complex new environments. He has led games on the future of the European asset management industry, U.S. financial services regulation, and corporate strategies for technological competition with China. His undergraduate degree is from Columbia University, in engineering, and he has a Ph.D. from Yale University in operations research.

James Canton

Dr. James Canton is a renowned global futurist, social scientist, keynote presenter, author, and visionary business advisor. He is the author of *The Extreme Future: The Top Trends That Will Reshape the World in the 21st Century*, Dutton 2006, and *Technofutures: How Leading-Edge Innovations Will Transform Business in the 21st Century*, Next Millennium Press, 2004.

Dr. Canton is CEO and Chairman of the Institute for Global Futures, a leading think tank he founded in 1990 that advises business and government on future trends. He advises the Global Fortune 1000 on trends in innovation, financial services, health care, population, life sciences, energy, security, workforce, climate change, and globalization. From a broad range of industries, clients include: IBM, BP, Intel, Philips, General Electric, Hewlett Packard, Boeing, FedEx, and Proctor & Gamble. He is a Senior Fellow at the Center for Research in Innovation at Northwestern's Kellogg School of Management and on the advisory board of the Corporate Eco Forum. He has advised three White House Administrations, the National Science Foundation, and MIT's Media Lab, Europe.

A frequent guest of the media, Dr. Canton is a commentator on CNN. He was named "the Digital Guru" by CNN and "Dr. Future" by Yahoo. Dr. Canton's media coverage has included CNBC, Fox, PBS, ABC, *Fortune*, *The Wall Street Journal*, *The Economist*, *Bloomberg Report*, *The New York Times*, *US News and World Report*, *CEO*, and *CIO* and *CFO* Magazines. His Global Futurist blog is followed by a world-wide audience. Dr. Canton serves as co-chairman of the Futures and Forecasting Track at Singularity University, which is educating a new generation of leaders to use advanced technologies to transform the planet for the better.

Celeste Chen

Celeste Chen is a Master's Candidate at the McCourt School of Public Policy at Georgetown University. Through her roles at the Department of Education, Department of Commerce, and the Embassy of Australia, she has explored different intersections of emerging technology, foreign policy, and academic research. She is currently a 2017 Presidential Management Fellows Program Finalist, and she possesses a Bachelor of Science degree in neurobiology and studio art from Georgetown University.

David Chu

David Chu serves as President of the Institute for Defense Analyses. IDA is a non-profit corporation operating in the public interest. Its three federally funded research and development centers provide objective analyses of national security issues and related national challenges, particularly those requiring extraordinary scientific and technical expertise.

As president, Dr. Chu directs the activities of more than 1,000 scientists and technologists. Together, they conduct and support research requested by federal agencies involved in advancing national security and advising on science and technology issues.

Dr. Chu served in the Department of Defense as Under Secretary of Defense for Personnel and Readiness from 2001–2009, and earlier as Assistant Secretary of Defense and Director for Program Analysis and Evaluation from 1981–1993. From 1978–1981 he was the Assistant Director of the Congressional Budget Office for National Security and International Affairs.

Dr. Chu served in the U. S. Army from 1968–1970. He was an economist with the RAND Corporation from 1970–1978, director of RAND’s Washington Office from 1994–1998, and vice president for its Army Research Division from 1998–2001. He earned his doctorate in economics, as well as a bachelor of arts in economics and mathematics, from Yale University.

Dr. Chu is a member of the Defense Science Board and a Fellow of the National Academy of Public Administration. He is a recipient of the Department of Defense Medal for Distinguished Public Service with Gold Palm, the Department of Veterans Affairs Meritorious Service Award, the Department of the Army Distinguished Civilian Service Award, the Department of the Navy Distinguished Public Service Award, and the National Academy of Public Administration’s National Public Service Award.

Cameron Colquhoun

As one of the UK’s leading voices on 21st century intelligence and cyber security, Cameron Colquhoun recently arrived at RAND from London, as the inaugural Fulbright Commission Cyber Award winner. Cameron spent a decade working in GCHQ (the UK’s NSA) on counter-terrorism and cybersecurity, was embedded with SOCOM and JSOC in Iraq during 2008, and wrote detailed strategic assessments for the UK Cabinet Office and government ministers on terrorism and geopolitics. He co-wrote an analytical thinking training package that was subsequently put forward by the NSA to President Obama, as a series of remedial steps to address analytical shortfalls following the attempted attack over Detroit in 2010. Since leaving the public sector, Cameron founded an ethical Open Source Intelligence business, Neon Century—a consultancy that uses open data analytics to address risk questions in the cyber, geopolitical, and commercial space—and has worked closely with some of the world’s biggest companies on their cyber threats. Cameron has featured on BBC News,

the Daily Telegraph, *WIRED Magazine*, and was named one of London's most promising young entrepreneurs by an influential financial services publication. Cameron holds an undergraduate degree in International Relations, and a First Class Masters' degree in Middle East Security.

Zachary S. Davis

Dr. Zachary Davis is Senior Fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory and a Research Professor at the Naval Postgraduate School in Monterey, California where he teaches courses on counterproliferation. He has broad experience in intelligence and national security policy and has held senior positions in the executive and legislative branches of the U.S. government. His regional focus is South Asia.

Davis began his career at the Congressional Research Service at the Library of Congress and has served in the State Department, the Arms Control and Disarmament Agency, Congressional committee staffs, and the National Security Council. In 2006–2007, he was Senior Advisor at the National Counter Proliferation Center, in the office of the Director of National Intelligence. He is the author of numerous government studies and reports on technical and regional proliferation issues. He currently leads a project on the national security implications of emerging and advanced technologies at LLNL and supports US Special Operations Command on the development of counterproliferation education programs.

Davis's scholarly publications include articles in *Orbis*, *Asian Survey*, *Arms Control Today*, *Security Studies*, *The American Interest*, and chapters in numerous edited volumes. He was editor of the widely read 1993 book *The Proliferation Puzzle: Why States Proliferate and What Results*. His edited book on the 2002 South Asia crisis was published by Palgrave Macmillan in 2014. His new book, *Strategic Latency: Red, White and Blue*, will be published this year. Davis holds a doctorate and a masters degree in international relations from the University of Virginia and earned his undergraduate degree from UC Santa Cruz.

Lisa Owens Davis

Lisa Owens Davis founded Owens Davis Consulting in 2014 to provide clients with expertise gained from her career working with U.S. government agencies on issues related to weapons of mass destruction proliferation, verification, global illicit networks, intelligence analytics, government business development, and strategic planning.

At Lawrence Livermore National Laboratory Lisa served as the Intelligence Program Director in the Office of Strategic Outcomes where she was responsible for the development and execution of multi-year, strategic development plans for the Laboratory. Prior to that she was Program Leader in LLNL's Global Security Directorate managing and executing intelligence analysis and operations support to programs countering national security threats. She has served multiple tours in Washington, D.C. including at the CIA, the Department of State, and the Department of Energy.

Lisa has received awards for her work from LLNL, the Central Intelligence Agency, and the Department of State. She completed the LLNL Leadership Institute with the University of California Berkeley's Haas School of Management. She was a Presidential Management Fellow and worked at the International Atomic Energy Agency in Vienna. Proficient in three foreign languages and fluent in Spanish, Lisa taught English in Czechoslovakia and Spain. She received her MA in International Policy from the Monterey Institute of International Studies and earned her BA in Spanish from University of California, Santa Barbara.

Frank Gac

Dr. Frank D. Gac retired in 2014, after an exciting and productive 38-year career with the Los Alamos National Laboratory. During that time he served as an Executive Advisor to the Principal Associate Director for Global Security; led the Ceramic Science & Technology and International Research, Analysis, and Technology Groups; and was on Intergovernmental Personal (IPA) assignments with the Central Intelligence Agency and the Office of the Director of National Intelligence. He is currently a Guest Scientist with Los Alamos and a Consultant to the Lawrence Livermore National Laboratory Center for Global Security Research. His B.S. and M.S. are in Ceramic Engineering from the University of Illinois and University of Missouri–Rolla, respectively, and his Ph.D. is in Materials Science & Engineering from the University of Washington.

Ben Forster

Ben Forster is a solutions manager for a Silicon Valley cyber security firm where he supports global marketing across critical infrastructure and industry. Previously he was a management consultant for the Office of the Under Secretary of Defense for Policy where he supported the Deputy Director, Defense Technology Security Administration on the Security Cooperation Reform Task Force. He subsequently consulted for the Defense Security Cooperation Agency where he helped manage international civilian advisor operations. He holds a masters in global politics from the London School of Economics and Political Science, and a bachelors from Claremont McKenna College.

James Giordano

James Giordano is Chief Scientist, Office of the Senior Vice President for Research of Georgetown University, and Professor in the Departments of Neurology and Biochemistry. He is Chief of the Neuroethics Studies Program of the Pellegrino Center for Clinical Bioethics, and Co-director of the O'Neill-Pellegrino Program in Brain Science and Global Health Law and Policy at the Georgetown University Medical Center, Washington DC. Professor Giordano is Senior Science Advisory Fellow to the Strategic Multilayer Assessment Group of the Pentagon, and serves as an appointed member of the Neuroethics, Legal and Social Issues Advisory Panel of the Defense Advanced Research Projects Agency (DARPA) working primarily upon neuroethical and legal aspects of neuromodulatory approaches employed in the Systems Based Neurotechnology for Emerging Therapies (SUBNETS) and Restoring Active Memory (RAM) Programs.

A neuroscientist and neuroethicist with over 25 years' experience in basic and translational research upon neural mechanisms of decision-making and neuropsychiatric processes, his current work focuses upon neuroethical and legal issues arising in and from the use of advanced neurotechnologies in medicine, public life, and national security, intelligence, and defense. He is the author of over 230 publications and seven books in neuroscience and neuroethics, and 11 governmental whitepapers on bioscience, biotechnology, and biosecurity. Professor Giordano was awarded a Ph.D. in biological psychology from the City University of New York; was NIEHS post-doctoral fellow in neurotoxicology and neuropathology at the Johns Hopkins University; APA Visiting Fellow in advanced neuroimaging at Harvard Medical School/Massachusetts General Hospital; and completed post-graduate training in bioethics and health policy at the Neiswanger Institute of Loyola University, Chicago.

Tim Grayson

Dr. Timothy Grayson is founder and president of Fortitude Mission Research LLC. He specializes in strategy and technology analysis related to security and intelligence for both government agencies and the private sector. He has also served on the board of advisors of several small businesses in these sectors. Prior to founding Fortitude, Dr. Grayson served as a senior executive in several large and small defense companies and in the U.S. federal government. He holds a Ph.D. in Physics from the University of Rochester where he specialized in quantum optics and a B.S. in Physics from the University of Dayton with minors in mathematics and computer science.

Brian Holmes

Dr. Brian Holmes is the Associate Dean of the Anthony G. Oettinger School of Science and Technology Intelligence at the National Intelligence University in Washington, D.C. He is a former research scientist, naval officer, and intelligence analyst.

Joseph Keogh

Dr. Keogh, a Chemist and Senior Executive with the U.S. Government, retired in 2009 after a rewarding 32 years of service in intelligence, focusing on novel advancements and uses of science and technology. A former Captain in the U.S. Army, he earned his B.S. from Drexel University and his Ph.D. from the University of Colorado at Boulder, both in Chemistry. In 1990–91 Dr. Keogh was a Presidential Exchange Fellow with the Bush Administration. In that role he was responsible for helping to catalyze industry-government exchange of best practices and building networks for improved understanding between government and industry executives. He was also awarded recognition in National Security Studies from the Institute of World Politics. Dr. Keogh is a pioneer in applying systems architecture to solving complex national security problems. For the past eight years he has been applying his talents at the executive level to private industry.

Ron Lehman

Ron Lehman is Counselor at Lawrence Livermore National Laboratory, Chair of the Defense Department Threat Reduction Advisory Committee, and Board Chair of the International Science and Technology Center. Ron was Director of the U.S. Arms Control and Disarmament Agency from 1989–1993 when START I, START II, the Chemical Weapons Convention, the Conventional Forces in Europe Treaty, Open Skies, and other historic agreements were concluded. Ron served in DOD as Assistant Secretary for International Security Policy, in the State Department as Ambassador and U.S. Chief Negotiator on Strategic Offensive Arms, in the White House as Deputy Assistant to the President for National Security Affairs, and on the National Security Council staff. Ron was on the professional staff of the Senate Armed Services Committee, taught at Georgetown University, was a post-doctoral fellow at the Hoover Institution, and served in Vietnam with the US Army.

Jason Lepore

Jason Lepore is an Associate Professor in the Economics Department of the Orfalea College of Business at California Polytechnic State University. He has published articles on topics in game theory and industrial organization in prestigious outlets such as *Journal of Economic Theory*, *Journal of Mathematical Economics*, and *International Journal of Industrial Organization*. He also does research using game theoretic reasoning to analyze military planning and technology published in outlets such as *Defence and Peace Economics* and *Defense Analysis*. Jason was a co-editor of the book *Assessing War: The Challenge of Measuring Success and Failure* (Georgetown University Press, 2015) and is currently working on a book about the interaction between military strategy and defense planning.

Michael Nacht

Michael Nacht holds the Thomas and Alison Schneider Chair in Public Policy. From 1998–2008 he was Aaron Wildavsky Dean of the Goldman School. He is a specialist in U.S. national security policy; science, technology, and public policy; and management strategies for complex organizations. He is the author or co-author of five books and more than eighty articles and book chapters on nuclear weapons policy; regional security issues affecting Russia and China, the Middle East, and East Asia; cyber and space policy; counter-terrorism and homeland security; international education; and public management.

Nacht served as Assistant Secretary of Defense for Global Strategic Affairs (2009–2010), after unanimous U.S. Senate confirmation, for which he received the Distinguished Public Service Award, the Department's highest civilian honor. Previously, he was Assistant Director for Strategic and Eurasian Affairs of the U.S. Arms Control and Disarmament Agency (1994–97), during which time he participated in five Presidential summits, four with Russian President Yeltsin and one with Chinese President Jiang Zemin. He is currently chair of the Policy Focus Area for the Nuclear Science and Security Consortium led by the UC Berkeley Department of Nuclear Engineering.

Nacht holds a BS in Aeronautics and Astronautics and an MS in Operations Research from New York University, an MS in Statistics from Case Western Reserve University, an MA in Political Science from the New School for Social Research, and a Ph.D. in Political Science from Columbia University.

Osonde Osoba

Osonde Osoba (pronounced “oh-shOwn-day aw-shAw-bah”) is an associate engineer at the RAND Corporation and a professor at the Pardee RAND Graduate School. He has a background in the design and optimization of machine-learning algorithms. He has applied his expertise to diverse policy topics such as epidemiology, defense acquisition, and science and technology policy. His more recent focus has been on data privacy and accountability in algorithmic systems and artificial intelligence. Prior to joining RAND, he was a researcher at the University of Southern California (USC). His research there focused on improving the speed and robustness of popular statistical algorithms like the expectation-maximization (EM) and backpropagation algorithms used in applications like automatic speech recognition. He also made contributions on the robustness and accuracy of approximate Bayesian inference schemes. Osoba received his Ph.D. in electrical engineering from USC and a BS in electrical and computer engineering from University of Rochester.

Joseph F. Pilat

Joseph F. Pilat is a Program Manager in the Office of National Security and International Studies at the Los Alamos National Laboratory and a Global Fellow at the Woodrow Wilson International Center for Scholars where he co-directs the Nonproliferation Forum. He served as Representative of the Secretary of Defense to the Fourth Review Conference of the Nuclear Non-Proliferation Treaty (NPT), and as senior adviser to the U.S. Delegation at the 1995 NPT Review and Extension Conference. Dr. Pilat also served as representative of the Secretary of Defense to the Open Skies negotiations. He has held positions in the Pentagon and the Congressional Research Service, and has taught at Cornell University, Georgetown University, and the College of William and Mary. He is the co-editor of the *Handbook of Nuclear Proliferation and Policy* (Routledge, 2015) and the co-author of *The Politics of Weapons Inspections* (Stanford University Press, 2017).

Toby Edwardo Redshaw

Toby Redshaw is a global business transformation leader who has driven P&L and business process/performance improvements across multiple industries. He is known for helping firms deliver competitive advantage through innovative, real-world IT-centric strategy and speed-of-execution in high growth, high service, and high technology environments. In addition to CIO leadership, Toby’s business and operational expertise includes hands-on M&A, acquisition integration, multi-billion dollar procurement, risk and regulatory, eCommerce/marketing leadership, diversity, and venture capital/Silicon Valley experience. He works at the nexus of pragmatism and innovation.

Toby is currently SVP of Digital Ecosystems for Verizon at the HQ in Basking Ridge, NJ. He was previously the Global CIO at American Express and at Aviva PLC, a UK-headquartered \$85 billion revenue insurer with \$800 billion in assets under management. Prior to that he spent six years at Motorola where he simultaneously had product, marketing, strategy, and technology responsibilities in addition to being executive chairman of a portfolio company and the first Chief Procurement Officer. He helped found and run a global start up based in Silicon Valley, China, London, and Ohio. He started his career as one of the first employees on the international side of FedEx where he had a 17-year career in business and IT.

Jennifer Snow

Major Jennifer Snow is the Donovan Group Innovation Officer for the U.S. Special Operations Command, Donovan Group Futures Plans and Strategy and SOFWERX Team. She serves as the military representative for technology outreach and engagement to bridge the gap between government and various technology communities to improve collaboration and communications, and identify smart solutions to wicked problems and the development of future smart technology policy.

Major Snow entered the Air Force in November 2002 as a graduate of the U.S. Officer Training School at Maxwell AFB in Montgomery, Alabama. She began her professional career as a member of Air Force Special Operations Command, served as an Air Education and Training Command intelligence instructor supervisor and was selected to be one of General Keith B. Alexander's Junior Officer Cryptologic Career Program Interns at the National Security Agency. Prior to her current assignment, Major Snow was a graduate student at the Naval Postgraduate School, where she studied emerging disruptive technologies and focused on a class of fast-moving emerging technologies she calls "Radical Leveling Technologies," as an area of concern to National Security. Her work was presented to National Security Council staff at the White House. Her efforts focus on examining Radical Leveling Technologies through the lens of 3D printing and seek to address the broad implications of these technologies as well as the need to leverage the expertise, access, and capacity of the community of users and technology drivers to find innovative policy solutions while still enabling technology for good.

Wes Spain

Wes Spain is Senior Fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory. He has broad experience in intelligence and national security, leading programs and activities in intelligence analysis, technology development, and business and program development, as well as intelligence and military teams overseas. Before joining LLNL, Wes served with Central Intelligence Agency and the United States Army. He holds an M.A. in international relations and a B.S. in political science.

Daniel Tapia-Jimenez

Daniel Tapia-Jimenez is a Ph.D. Candidate at University of California, Davis. His dissertation explores how technology affects international cooperation and competition following

developments and incidences related to agricultural biotechnology and cybersecurity technology. In so doing it aims to refine a general framework to understand emerging technologies. His broader research agenda focuses on ways to understand and anticipate technological impacts in international relations. The aim of this research is to better inform researchers and policymakers as to technology's impacts. He has interned at the Center for Global Security Research at Lawrence Livermore National Laboratory. He holds a B.A. in political science and international studies from Dominican University of California, and an M.A. in political science from University of California, Davis.

Bill Welser

William (Bill) Welser IV is the director of the Engineering and Applied Sciences (EAS) Research Department at the RAND Corporation, a professor at Pardee RAND Graduate School, and co-director of RAND's Impact Lab. As director of the EAS Research Department, he is responsible for roughly 200 world-class professional research staff. Welser maintains a deep personal research portfolio focused on the challenges related to technology design, adoption, and complexity. His current efforts involve privacy, artificial intelligence, industrial ecosystems, commercial drones, and cryptography. His published research has informed policy decision-makers and the public on topics such as space debris mitigation and remediation; military force posture; integration of women into combat positions; vulnerabilities and capabilities of space systems; maintenance and sustainment of stealth aircraft; and medical logistics support to US military and embassy personnel around the globe. His design of a cryptographic solution for avoiding collisions in space was developed into working prototypes via the DARPA PROCEED program. His research has been published via media outlets *Scientific American*, *Foreign Affairs*, *Time*, and *BusinessWeek* as well as various newspapers, podcasts, and websites.

Prior to RAND, Bill served in the USAF as an acquisition officer and engineer responsible for program management, design of next-generation technologies, systems engineering, and procurement and production of advanced technologies. His military service included time spent at the Space and Missile Systems Center and the Electronic Systems Center. Bill received his B.S. in chemical engineering from University of Virginia, his M.B.A. from Boston College, and his M.S. in finance from Boston College.

This work was performed under the auspices of the U.S. Department of Energy
by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.



The mission of the Center for Global Security Research is to catalyze broader national and international thinking about the requirements of effective deterrence, assurance, and strategic stability in a changed and changing security environment.

To learn more please visit our website: cgsr.llnl.gov

